N° 3054

# ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

DIX-SEPTIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 8 juillet 2026.

# RAPPORT

FAIT

AU NOM DE LA COMMISSION D'ENQUÊTE *sur les* **dépendances structurelles** *et les* **vulnérabilités systémiques** *dans le* **secteur** *du* **numérique** *et les* **risques** *pour l'***indépendance** *de la* **France***,*

Président

M. PHILIPPE LATOMBE

Rapporteure

MME CYRIELLE CHATELAIN

Députés

**TOME I**

**RAPPORT**

Voir les numéros : **2245** et **2369**.

*La commission d'enquête sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France, est composée de :* M. Philippe Latombe, *président* ; Mme Cyrielle Chatelain, *rapporteure* ; M. Édouard Bénard ; M. Nicolas Bonnet ; M. Éric Bothorel ; M. Jérôme Buisson ; Mme Sophia Chikirou ; Mme Virginie Duby-Muller ; M. Thomas Gassilloud ; M. Philippe Gosselin ; M. Sacha Houlié ; M. Arnaud Le Gall ; M. Aurélien Lopez-Liguori *(jusqu'au 25 avril 2026)* ; M. Paul Midy ; Mme Laure Miller ; Mme Josy Poueyto ; M. Stéphane Rambaud ; Mme Isabelle Rauch ; Mme Sophie-Laurence Roy ; M. Alexandre Sabatou ; M. Arnaud Saint-Martin ; M. Emeric Salmon ; M. Hervé Saulignac ; M. Thierry Sother ; M. Aurélien Taché ; M. Vincent Thiébaut ; Mme Mélanie Thomin.

**SOMMAIRE**

___

Pages

## AVANT-PROPOS DU PRÉSIDENT

Il est des sujets qui exigent davantage que le débat politique ordinaire. Parce qu'ils engagent l'intérêt général, interrogent l'efficacité de l'action publique ou mettent en lumière les attentes de nos concitoyens, ils appellent une démarche fondée sur l'écoute, l'exigence des faits et la recherche patiente de solutions. Les commissions d'enquête parlementaires répondent à cette ambition.

Par les pouvoirs d'investigation qui leur sont confiés, par la publicité de leurs travaux et par l'indépendance de leurs analyses, elles constituent l'une des expressions les plus abouties de la mission de contrôle du Parlement. Elles permettent de dépasser les impressions, les approximations ou les controverses pour établir les faits, comprendre les responsabilités et proposer des évolutions utiles à l'action publique.

Mais la véritable singularité d'une commission d'enquête réside sans doute dans sa méthode. Elle rassemble des parlementaires issus d'horizons politiques différents, parfois opposés, qui acceptent de soumettre leurs convictions à l'épreuve des faits. Les divergences ne disparaissent pas : elles nourrissent au contraire le débat.

Dans le contexte turbulent que connaît actuellement l'Assemblée nationale où, dans une sorte de réflexe pavlovien de rejet, les désaccords sont trop souvent exacerbés, il me semble essentiel de le rappeler. Toutefois, l'exercice impose à chacun une même discipline : écouter avant de conclure, vérifier avant d'affirmer, confronter les analyses avant de formuler des recommandations.

Alors que la vie publique est souvent perçue à travers le prisme de la confrontation permanente, cette démarche transpartisane revêt une portée particulière. Elle rappelle qu'au-delà des alternances et des clivages, il existe un espace où les représentants de la Nation peuvent travailler ensemble, dans le respect de leurs différences, pour servir un objectif commun. Ce n'est pas l'effacement des sensibilités politiques qui fait la force d'une commission d'enquête, c'est leur capacité à produire, par le dialogue et la rigueur, une compréhension partagée des enjeux.

Le présent rapport sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France est le résultat de cette exigence collective. Les auditions, les déplacements, les contributions écrites et les nombreux échanges qui ont rythmé les travaux de la commission ont permis de faire émerger des constats solides et, chaque fois que cela a été possible, des recommandations largement partagées. Là où des désaccords subsistent, ils sont assumés avec transparence ; là où un consensus a pu être trouvé, ce dernier témoigne de la force du travail parlementaire, lorsqu'il s'affranchit des réflexes partisans.

À l'heure où les Français attendent de nos institutions qu'elles démontrent leur capacité d'écoute, d'évaluation et de proposition, les commissions d'enquête

rappellent que le Parlement n'est pas seulement le lieu de la confrontation démocratique : il est aussi celui de la recherche de la vérité, du contrôle de l'action publique et de la construction de solutions durables.

C'est dans cet esprit qu'a été élaboré ce rapport. Puissent ses constats nourrir le débat public, éclairer les décisions à venir et contribuer, par-delà les appartenances politiques, au renforcement de la confiance entre les citoyens et leurs institutions.

Puisse-t-il contribuer à cette ambition, en offrant aux pouvoirs publics, aux acteurs concernés et à l'ensemble de nos concitoyens les éléments nécessaires à une meilleure compréhension des enjeux et à l'amélioration de l'action publique, sur le sujet majeur que constituent les dépendances structurelles et les vulnérabilités systémiques de notre pays dans le secteur du numérique

Mon principal regret reste sans doute qu'il ait fallu attendre l'ère MAGA pour qu'un plus grand nombre de politiques et de groupes parlementaires s'intéresse aux dépendances structurelles et aux vulnérabilités systémiques de la France dans le secteur du numérique, ainsi qu'aux risques pour l'indépendance et la souveraineté de notre pays.

Les dépendances sont là, depuis fort longtemps, et il est tout à fait regrettable que nous ayons vécu tant d'années, notamment dans une naïve confusion qui consiste à penser qu'un allié est un ami. Les manières brutales de l'actuel occupant de la Maison Blanche auront au moins eu l'avantage de provoquer un électrochoc que j'espère salutaire, et suivi de mesures rapides et efficaces. Le présent rapport ambitionne d'ailleurs, par ses préconisations, d'y contribuer.

Voilà plus de six ans que je tente d'alerter sur ce sujet, comme rapporteur de la mission d'information sur la souveraineté numérique nationale et européenne, en 2021, ou comme président de la commission spéciale chargée d'examiner le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, l'an dernier. Je me suis senti peu entendu, peu suivi et trop souvent cantonné au rôle frustrant de Cassandre. Avec cette différence majeure que celle-ci n'avait à alerter que sur un seul cheval de Troie, alors que nous devons faire face à une multitude de vulnérabilités : fournisseurs américains de cloud, systèmes d'exploitation étrangers, nombreux composants électroniques asiatiques, infrastructures internet mondiales… Et cette liste n'est sans doute pas exhaustive. Le tout dans un contexte mondialisé où la cyberguerre bat son plein.

En 2021, dans le rapport de la mission d'information sur la souveraineté numérique nationale et européenne, j'écrivais : « La construction d'une souveraineté numérique nationale et européenne doit être le fil rouge des décisions politiques mises en œuvre dans la décennie à venir. Il s'agit en effet d'un impératif absolu. Sans cette boussole, le risque est grand de voir les capacités d'action des individus, des entreprises et des États se réduire progressivement, faute de maîtriser le " nouveau monde " numérique, alors que de nouveaux acteurs, publics et privés,

se sont emparés de leviers d'influence pour servir leurs propres intérêts ». Force est de constater que, cinq ans plus tard, nous n'avons pas vraiment progressé.

D'aucuns s'étonneront que la commission d'enquête ne se soit pas intéressée à la cybersécurité et aux failles des entités nationales, publiques et privées. Ce n'est pas un oubli mais la conviction, peut-être illusoire, que ce texte essentiel allait être rapidement mené à son terme et qu'il n'était pas nécessaire que la commission l'abordât. La menace d'une action menée par la Commission européenne contre la France, devant la CJUE, avant la fin de l'année, et le risque d'une amende devraient sans doute permettre d'espérer l'inscription rapide de ce texte, voté à l'unanimité en commission spéciale, à l'ordre du jour de la séance.

Qu'il me soit enfin permis de regretter que cette commission d'enquête n'ait pas connu un intérêt médiatique à la hauteur des enjeux abordés. Dans un monde entièrement numérisé, la conquête de notre autonomie stratégique est un enjeu vital pour l'avenir de notre économie, l'amélioration de notre compétitivité, la création d'emploi et le bien-être de nos compatriotes. Cela passe par la réduction de nos dépendances et de nos vulnérabilités et nécessite une prise de conscience collective. Il en va de nos libertés individuelles et collectives. Les vidéos des auditions permettront, je l'espère, à tous ceux qui souhaitent s'informer, de combler ce manque de médiatisation.

Je tiens tout particulièrement à remercier la rapporteure, Mme Cyrielle Chatelain, et les membres du bureau, pour la qualité de nos échanges et leur volonté d'un travail transpartisan de qualité.

Longue vie à ce rapport et à ses préconisations, qui arrivent à point nommé pour nourrir l'examen tant attendu en séance du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, ainsi que celui du projet de loi de finances pour 2027 !

# INTRODUCTION

## POURQUOI UNE COMMISSION D'ENQUÊTE ? LES GAFAM À L'ÈRE MAGA

### A. UN CHOIX MARQUÉ PAR LE CONTEXTE GÉOPOLITIQUE INTERNATIONAL

En 2019, une commission d'enquête sur la souveraineté numérique du Sénat dressait d'ores et déjà le constat suivant : *« Aujourd'hui, il faut défendre notre modèle de société et nos valeurs : l'Homme n'est pas une somme de données à exploiter. Le cyberespace, loin de l'utopie égalitaire de ses débuts, est devenu un lieu d'affrontement mondial, où s'exercent luttes d'influence, conflits d'intérêts et logiques sociales et économiques antagonistes. La révolution numérique et la maîtrise des données ont fait émerger des acteurs économiques capables de rivaliser avec les États. Dans ce contexte, et face à de redoutables concurrents, comment conserver une capacité autonome d'appréciation, de décision et d'action ? »* (1).

En 2021, un rapport de M. Philippe Latombe, président de la présente commission d'enquête, concluait : « *la construction d'une souveraineté numérique nationale et européenne doit être le fil rouge des décisions politiques mises en œuvre dans la décennie à venir. Il s'agit en effet d'un impératif absolu. Sans cette boussole, le risque est grand de voir les capacités d'action des individus, des entreprises et des États se réduire progressivement, faute de maîtriser le " nouveau monde " numérique, alors que de nouveaux acteurs, publics et privés, se sont emparés de leviers d'influence pour servir leurs propres intérêts.* » (2)

Ces diagnostics convergeaient déjà pour souligner la criticité du sujet et la nécessité de reconquérir une souveraineté numérique pour s'extraire des dépendances à des acteurs étatiques ou privés.

En réalité, ces dépendances sont la résultante de plusieurs décennies durant lesquelles cinq géants ont constitué des empires industriels et se sont profondément implanté en Europe. Google, Apple, Amazon, Meta et Microsoft détiennent ou maîtrisent une très grande partie de l'infrastructure et des services numériques qui constituent notre quotidien. Les dépendances qu'ils ont créées étaient jusqu'à présent silencieuses, et ne menaçaient pas directement le fonctionnement de notre pays.

---

*(1) Gérard Longuet,* Le devoir de souveraineté numérique, *rapport d'enquête, octobre 2019* https://www.senat.fr/notice-rapport/2019/r19-007-1-notice.html

*(2) Philippe Latombe,* Rapport d'information sur le thème « Bâtir et promouvoir une souveraineté numérique nationale et européenne », *juin 2021*

https://www.assemblee-nationale.fr/dyn/15/rapports/souvnum/l15b4299-t1_rapport-information.pdf

Elles sont désormais un levier de menaces supplémentaire, au même titre que les ressources énergétiques importées ou les droits de douane. Si le groupe Écologiste et social a pris l'initiative de la création de la commission d'enquête, c'est en raison du contexte géopolitique. Le second mandat de Donald Trump à la présidence des États-Unis d'Amérique, commencé en janvier 2025, marque 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 conférences internationales de lutte contre le dérèglement climatique – est fortement remis en cause.

La stratégie de sécurité nationale américaine, publiée début décembre sous l'égide du nouveau président, dénigre nos règlementations environnementales, désigne l'Union européenne comme ennemi de la liberté et recherche l'alignement des valeurs européennes sur celles des MAGA *(Make America Great Again* – mouvement politique partisan de Donald Trump). Pour atteindre ces objectifs, l'actuel président des États-Unis s'appuie sur une puissance stratégique, partiellement constituée des outils numériques américains.

Au contexte géopolitique s'ajoute le déploiement à grande échelle de l'intelligence artificielle générative, comportant tout à la fois des opportunités, mais aussi d'importantes menaces. Cette technologie est aujourd'hui portée par des acteurs américains, au premier rang desquels on retrouve ces cinq géants, et d'autres comme Open AI en cours de constitution à vitesse accélérée – sans toutefois négliger l'importance prise par les acteurs chinois dans ce domaine.

Enfin, plusieurs dirigeants de grandes entreprises du numérique sont devenus aujourd'hui bien plus des acteurs politiques que des acteurs économiques. Elon Musk a soutenu Donald Trump dans son accession à la Maison Blanche et a sciemment déployé une intelligence artificielle générative comportant des biais antisémites. S'agissant de la société Palantir, son fondateur, Peter Thiel, affirme depuis 2009 que liberté et démocratie ne sont plus compatibles tandis qu'Alex Karp, son PDG actuel, a publié sur X le 18 avril 2026 un manifeste pour une *République technologique*. Ce manifeste plaide pour une nouvelle ère de dissuasion fondée sur l'IA, dénonce les politiques d'inclusion, le pluralisme et plaide pour une hiérarchie entre les cultures.

Cette situation rend nécessaire l'examen des dépendances systémiques des citoyens, des administrations et des acteurs économiques aux technologies numériques. 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. Quelles sont les dépendances critiques qui peuvent affecter le fonctionnement de notre pays ? Comment y remédier ? Telles sont les deux questions qui ont guidé les travaux de la commission d'enquête.

## B. TYPOLOGIE DES VULNÉRABILITÉS DANS LE SECTEUR DU NUMÉRIQUE

Les dépendances structurelles dans le secteur du numérique peuvent être rassemblées en six grandes catégories de vulnérabilité.

### 1. Ingérences et diffusion de fake news : une vulnérabilité démocratique

Le débat public est marqué par l'organisation d'opérations d'ingérence informationnelle dans l'objectif de manipuler l'opinion par la diffusion de contenus inexacts ou trompeurs. Les acteurs menant ce type d'attaques voient leurs **moyens décuplés avec l'utilisation de l'intelligence artificielle**, laquelle permet de mener des actions plus crédibles dans des volumes beaucoup plus importants. L'utilisation généralisée de l'intelligence artificielle comme vecteur d'information crée également un risque de diffusion de fausses informations par « empoisonnement de contenu ». Dans son rapport « Défis et opportunités de l'intelligence artificielle dans la lutte contre les manipulations d'information » [(1)], Viginum [(2)] indiquait ainsi : « *la diffusion massive des outils génératifs interroge (…) fait craindre une élévation structurelle du niveau de menace liée aux ingérences numériques étrangères, avec le risque d'une altération de la perception de la réalité par les citoyens* ».

Au-delà des opérations d'ingérence organisées, la qualité de l'information et du débat public est aujourd'hui fortement affectée par les algorithmes utilisés par les réseaux sociaux. Lors de son audition devant la commission d'enquête, M. David Chavalarias, directeur de recherche au CNRS (Centre national de la recherche scientifique), présentait les résultats des recherches académiques réalisées sur l'impact des algorithmes dans le débat public [(3)] : « *Les résultats d'une étude très récente, menée notamment par Germain Gauthier, ont été publiés le mois dernier dans Nature. Aux États-Unis, des individus qui n'utilisaient pas l'algorithme standard de X y ont été exposés pendant sept semaines. Bien que la période soit assez courte, elle a suffi pour que 5 à 7 % d'entre eux en moyenne changent d'opinion à l'égard de Zelensky ou portent un jugement différent sur le caractère justifié ou non des procès contre Trump ou certaines idées conservatrices.*

« *Cette mesure empirique montre donc qu'un algorithme peut faire changer d'opinion 5 à 7 % des électeurs en moyenne et jusqu'à 15 % des électeurs indépendants, qui, aux États-Unis, peuvent voter pour les Républicains ou les Démocrates en fonction des sujets ou des élections. Avec X, vous avez un média qui a la main sur 32 millions d'utilisateurs réguliers et peut influencer 15 % des*

---

*(1) Viginum,* Défis et opportunités de l'intelligence artificielle dans la lutte contre les manipulations de l'information, *février 2025*
https://www.sgdsn.gouv.fr/files/files/Publications/20250207_NP_SGDSN_VIGINUM_Rapport%20menace%20informationnelle%20IA_VF.pdf

*(2) Service de vigilance et de protection contre les ingérences numériques étrangères.*

*(3) Table ronde du 10 mars 2026.*

*indécis* [1]*, ce qui correspond à peu près à l'écart entre Kamala Harris et Donald Trump dans le vote populaire* ».

Les ingérences informationnelles et les algorithmes structurant la diffusion d'information sur les réseaux sociaux constituent un risque systémique, dans la mesure où ils peuvent porter atteinte au fonctionnement politique des institutions, à l'intégrité du vote et, plus généralement, à la diffusion de la connaissance.

### 2. Les attaques cyber : l'exploitation des failles techniques des administrations et des entreprises

Les attaques cyber constituent la menace la plus visible à laquelle exposent les vulnérabilités induites par le numérique. Le panorama de la cybermenace, édité chaque année par l'Agence nationale de la sécurité des systèmes d'information (Anssi) [2] en dresse un tableau synthétique. Les menaces cyber couvrent **l'organisation d'attaques envers des cibles avec comme premier objectif un motif économique (rançons).** À ce titre, les PME/TPE/ETI sont la catégorie d'entités la plus affectée (37 %), devant les collectivités territoriales (17 %). Les menaces cyber constituent ainsi un coût économique potentiel pour les entités ciblées ou leurs utilisateurs et usagers directs ou indirects. Les attaques à des fins d'espionnage poursuivent également un motif économique, en lien direct avec l'identité des victimes visées.

Les menaces **peuvent également revêtir des objectifs plus politiques**, comme en témoigne la recrudescence des attaques lors des Jeux olympiques et paralympiques de Paris en 2024. Elles prennent la forme principalement de raids sur les sites internet (dites attaques par DDoS, déni de service distribué), et plus rarement de sabotage d'installations industrielles.

Durant les quelques mois où se déroulait la commission d'enquête, plusieurs cas de fuites de données majeures liées à des cyberattaques ont eu lieu, telles que celles ayant visé l'opérateur de tiers payant Almery [3] ou le portail de l'Agence nationale des titres sécurisés (ANTS) [4]. Ces nombreuses fuites démontrent l'importance du sujet ainsi que la régularité et la diversité des cyberattaques.

---

*(1) L'effet sur les indécis serait, en réalité, de 10 %, avec un intervalle de confiance à 95 % de [0,4 % ; 19,6 %], selon la rectification apportée par M. David Chavalarias à l'issue de son audition. Comme il l'a précisé, cela signifie qu'il y aurait 75 % de chances que le fil d'actualité de X fasse changer d'opinion d'au moins 2 % des électeurs indépendants aux États-Unis.*

*(2) Anssi,* Panorama de la cybermenace 2025, *mars 2026*

*https://www.cert.ssi.gouv.fr/uploads/CERTFR-2026-CTI-002.pdf*

*(3)Communiqué de presse, Almerys, mai 2026*

*https://static1.squarespace.com/static/59522b05e4fcb5c94e48e42c/t/6a184915e23c031798d8edc0/1779976469837/Communiqu%C3%A9+de+presse+almerys+du+25+mai+2026.pdf*

*(4) Communication de l'Agence nationale des titres sécurisés, avril 2026 https://ants.gouv.fr/toute-l-actualite/incident-de-securite-relatif-au-portail-antsgouvfr*

### 3. L'évolution des usages : de plus en plus de données à stocker et à protéger

Avec le recours aux technologies numériques, les personnes comme les entreprises ou les administrations publiques confient l'ensemble de leurs données à des acteurs tiers. Historiquement, ces données étaient stockées sur nos propres machines : ordinateur pour les particuliers, serveurs internes pour les entreprises. Face à la multiplication des outils numériques et au développement des plateformes, l'ensemble des acteurs, publics comme privés, **recourent de façon croissante au cloud** pour l'hébergement de leurs données et le fonctionnement de leurs applications. Les données sont désormais hébergées sur des serveurs distants, stockées dans des centres de données, et l'information circule via des réseaux télécoms.

Cette situation désormais établie génère trois problématiques :

– **La légalité du stockage et du traitement des données opérés** : pour les particuliers, le consentement est-il recueilli de façon valide et proportionnée, selon les règles en vigueur ? Pour les entreprises, la protection de leurs données commerciales et de leur propriété intellectuelle est-elle assurée ? L'Europe a été pionnière sur le terrain de la protection des données personnelles avec l'adoption du Règlement général sur la protection des données (RGPD), entré en application en 2018, qui venait renforcer et compléter la loi « Informatique et libertés » de 1978.

– La seconde est **l'extraterritorialité du droit**. Le fait d'être soumis à un droit extra-européen revêt une importance particulière au regard de la place prise par les acteurs extra-européens dans le secteur du numérique : Google, Meta, Amazon, Microsoft. Le Clarifying Lawful Overseas Use of Data Act (Cloud Act) de 2018 permet aux autorités américaines disposant d'un mandat ou d'une autorisation du juge dans le cadre d'une enquête criminelle d'exiger d'une entreprise américaine qu'elle fournisse les données stockées sur ses serveurs, y compris lorsque ces données ne sont pas hébergées aux États-Unis. Le Foreign Intelligence Surveillance Act (Fisa) vise plus particulièrement les particuliers en autorisant la collecte de données sur des personnes ou entités non américaines à des fins de sécurité nationale. Si ce texte date de 1978, il a été amendé en 2008 pour introduire la section 702, permettant la surveillance des communications électroniques de ressortissants étrangers en dehors du territoire américain, les fournisseurs de services relevant des juridictions américaines étant contraints d'apporter leur assistance. Ainsi, en confiant leurs données à des acteurs extra-européens, **les citoyens et entreprises risquent de ne plus être protégés par les législations française ou européenne, celles-ci pouvant *de facto* entrer en contradiction avec la législation** de l'État de domiciliation de l'entité contrôlant les données.

– Enfin, la captation des données représente également un **risque pour les entreprises et les administrations** : espionnage industriel ou diplomatique, atteintes aux dirigeants, utilisation de la donnée à des fins économiques.

### 4. « Si c'est gratuit, c'est toi le produit » ! – Quand le profit prime sur les libertés individuelles et la santé des personnes

Le fonctionnement des systèmes numériques s'est progressivement concentré autour d'acteurs privés dominateurs, qui agrègent autour d'eux de très nombreux acteurs. Cette architecture entraîne plusieurs risques. D'une part, en maîtrisant un large spectre de l'information, ces multinationales du numérique acquièrent une connaissance très fine des individus, des entreprises et des administrations. Cette connaissance est vendue au plus offrant pour développer de la publicité ciblée. D'autre part, les informations détenues sont diffusées et circulent entre de très nombreux acteurs, rendant impossible le contrôle de l'utilisation qui en est faite. Les exemples d'utilisations non souhaitées ou malveillantes sont ainsi nombreux.

Lors de son audition devant la commission d'enquête, Mme Katia Roux, chargée de plaidoyer au sein de l'association Amnesty International a présenté les conclusions des travaux menés depuis plusieurs années par l'ONG [(1)] : « *L'ensemble de ces recherches met en évidence l'existence d'un modèle économique commun, fondé sur un profilage intrusif, une collecte massive de données personnelles et le recours à la publicité ciblée, qui constitue le moteur du fonctionnement de ces plateformes. Ce schéma se retrouve de manière constante puisque les plateformes cherchent en permanence à accroître la quantité de données collectées afin d'élaborer des profils toujours plus précis, destinés à être commercialisés auprès des annonceurs, tandis qu'elles recourent, dans le même temps, à des algorithmes sophistiqués pour déduire des centres d'intérêt, voire des indicateurs de bien-être, comme c'est le cas de TikTok. L'objectif poursuivi consiste à personnaliser les contenus, à maintenir les utilisateurs en ligne le plus longtemps possible et à remporter cette guerre de l'attention, souvent au détriment des droits humains.* »

Les impacts pour les particuliers sont nombreux : violation de leur vie privée, exposition à des contenus nocifs pour la santé, développement d'algorithmes addictifs pour augmenter le temps de présence sur le réseau.

### 5. Le verrouillage des utilisateurs : une pratique au cœur des stratégies des fournisseurs de logiciels

Aux fondements de l'économie numérique se trouve la notion d'effets de réseau : plus une solution ou une infrastructure est utilisée, plus elle rend service à son utilisateur, plus elle agrège de nouveaux participants, verrouille les usages et renforce sa domination.

L'utilisation de logiciels et de services numériques entraîne généralement des situations de dépendance aux solutions propriétaires (*vendor lock-in*) pour des raisons commerciales. Les fournisseurs de ces logiciels conçoivent des architectures

*(1) Table ronde, ouverte à la presse, réunissant des associations sur le thème de la protection des données personnelles, le 25 mars 2026.*

qui rendent difficile la migration vers une autre solution, ce afin de pouvoir vendre des services de maintenance et des prestations complémentaires de développement dans la durée. Tant pour les acteurs économiques que pour les particuliers, le changement de système est coûteux et requiert du temps et des efforts, avec parfois le risque de perte d'informations en cas de transfert.

La dépendance à un vendeur peut avoir des conséquences dommageables, qui peuvent aller de l'augmentation unilatérale des prix de fourniture à la rupture du service lorsque ce vendeur n'est plus en mesure d'assurer la continuité de sa solution (incident de service, faillite) ou bien ne le souhaite plus (choix stratégique de l'entreprise ou décision des autorités).

Le risque de dépendance augmente dans un secteur où le marché se partage entre quelques grands acteurs économiques. La notion de *gate keepers* (mal traduite en « contrôleurs d'accès ») a été introduite par la Commission européenne dans le Digital Market Act (DMA) [(1)], pour matérialiser juridiquement l'existence d'entreprises ayant le contrôle d'infrastructures digitales qui constituent le socle du fonctionnement économique et social des États membres.

Ces acteurs ne sont pas simplement des contrôleurs d'accès : non seulement ils définissent les modalités d'accès, mais ils sont propriétaires et seuls gestionnaires d'une infrastructure dont dépendent les acteurs économiques et les citoyens. Ils peuvent ainsi décider d'obliger leurs utilisateurs à accepter des conditions d'utilisation de leurs données, promouvoir des services additionnels en favorisant leurs produits au détriment de ceux de leurs compétiteurs, accroître unilatéralement les tarifs d'accès ou encore ne pas permettre la récupération des données de leurs utilisateurs en cas de sortie.

### 6. Les vulnérabilités liées aux infrastructures et aux composants clés

L'ensemble des services digitaux reposent sur l'existence d'une infrastructure physique : les data centers (centres de données) et les réseaux télécoms. Le nombre et la taille de ces infrastructures physiques augmentent en raison de l'usage grandissant des services numériques, et ce mouvement s'accélère du fait de la course à l'intelligence artificielle. Le fonctionnement de ces infrastructures est la condition nécessaire au bon fonctionnement des services numériques, sur lesquels reposent aujourd'hui de nombreux services vitaux.

*(1) Règlement 2022/1925 du Parlement européen et du Conseil relatif aux marchés contestables et équitables dans le secteur numérique (DMA), entré en vigueur le 1er novembre 2022, applicable depuis le 2 mai 2023.*

La construction et le maintien des infrastructures sont eux-mêmes dépendants de l'approvisionnements en composants clés. Comme l'indique un rapport de l'Institut de relations internationales et stratégiques (Iris) [(1)], « *La production de composants électroniques s'est largement délocalisée des États-Unis et de l'Europe vers les pays d'Asie, d'abord le Japon puis la Corée du Sud, Taïwan et enfin la Chine. Au début des années 1990, les pays européens représentaient 40 %, les États-Unis 37 % et le Japon 20 % de la production mondiale. Au début des années 2000, ces trois régions représentaient au total 37 % de la production mondiale. La part des États-Unis est passée à 12 % et celle de l'Europe à 7 % alors que la Chine représente désormais 18 % de l'offre mondiale (…) En ce qui concerne les échanges internationaux, plus de la moitié des exportations (55 %) sont assurées par trois pays asiatiques (Chine, Taïwan, Corée). Pour ce qui concerne les composants spécifiques au développement de l'Intelligence artificielle, la concentration est encore plus forte puisqu'ils sont produits dans deux pays : la Corée avec Samsung et surtout Taïwan avec TSM* ».

La dépendance aux composants-clés de l'industrie numérique s'est généralisée au cours des deux dernières années avec l'affaiblissement de la capacité industrielle européenne.

**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 | |

## C. LE PÉRIMÈTRE DE LA COMMISSION D'ENQUÊTE

L'objet de la commission d'enquête était d'examiner les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France. La proposition de résolution n° 2245 du

*(1) M. Philippe Barbet*, « *Les composants électroniques au cœur de la rivalité technologique entre la Chine et les États-Unis* », Observatoire géopolitique du numérique et des technologies émergentes », *janvier 2026* https://www.iris-france.org/wp-content/uploads/2026/01/ObsNumerique_2026_01_rivalite-USA-Chine_Note_FR.pdf

groupe Écologiste et social [1] listait plusieurs axes d'études conduisant à embrasser un champ très large de problématiques. Ainsi que le relevait le rapport de M. Philippe Latombe lors de l'examen de la recevabilité de la proposition de résolution [2], « *l'exposé des motifs de la proposition de résolution évoque à la fois les cyberattaques d'ampleur menées par des acteurs privés, les actes d'ingérence et les outils de surveillance de masse déployés par des États hostiles, les stratégies développées par les grandes entreprises du numérique et les enjeux liés à la législation européenne du numérique (…). Il importera donc, pour une telle commission d'enquête, de veiller à cadrer au mieux ses travaux (…)* ».

Au regard des moyens d'action dont disposait la commission d'enquête et du temps imparti de six mois, la rapporteure a dû faire des choix. La présente section vise à les présenter les choix s'agissant des objectifs poursuivis par la commission d'enquête et des sujets traités.

Pour répondre au contexte particulier, **la rapporteure s'est ainsi concentrée sur les dépendances et vulnérabilités qui sont au cœur du modèle mis en place par les acteurs américains,** à travers les deux sujets suivants :

**– La mise en place de systèmes massifs de stockage et de traitement des données des personnes et des entreprises, comprenant le cloud et les infrastructures physiques le soutenant (data centers).** Le cloud est un sujet structurant, dans la mesure où il sous-tend désormais le fonctionnement de l'ensemble des applications informatiques, y compris l'intelligence artificielle. Les entreprises fournissant les services et les infrastructures de cloud ont ainsi la maîtrise d'une couche essentielle de l'économie.

**– Les vulnérabilités créées par le monopole de certains acteurs sur des briques logicielles essentielles au fonctionnement de notre économie et le contrôle de plateformes structurantes.** Les acteurs dominants du domaine du numérique ont conquis des positions fortes sur leur marché cœur (le moteur de recherche pour Google, les systèmes d'exploitation pour Microsoft, etc.) et évoluent désormais vers une intégration horizontale (extension de leurs services à l'ensemble des secteurs) et verticale (prises de position sur le segment des infrastructures et des logiciels). Ils bénéficient de leur positionnement historique pour développer des services additionnels touchant l'ensemble des secteurs économiques, venant ainsi diminuer l'espace économique des acteurs classiques. Au cœur de cette domination, la maîtrise de la donnée, qui leur permet d'améliorer leur offre technologique.

---

*(1)* https://www.assemblee-nationale.fr/dyn/17/textes/l17b2245_proposition-resolution#

*(2)* https://www.assemblee-nationale.fr/dyn/17/rapports/cion_lois/l17b2369_rapport-fond#

Dans cet espace économique au croisement de la donnée utilisateurs et du logiciel, trois entreprises ont un fort poids économique :

– **Amazon**, opérateur de la plateforme mondiale de livraisons à domicile, mais également leader mondial des services cloud avec sa filiale Amazon Web Services (AWS) ;

– **Microsoft**, fournisseur du principal système d'exploitation des ordinateurs du monde entier et de la suite bureautique associée Microsoft 365, fournisseur de cloud à travers Microsoft Azure ;

– **Google**, opérateur du moteur de recherche du même nom, dominant le domaine de la publicité en ligne, et fournissant également des services de cloud via sa filiale Google Cloud Services.

Les trois groupes internationaux sont rassemblés sous le terme d'*hyperscalers*, qui restitue bien la spécificité conférée par leur contrôle d'une grande partie des couches indispensables au fonctionnement d'internet.

Fournissant des infrastructures essentielles, ces trois entreprises doivent faire l'objet d'une régulation spécifique. Or, **leur localisation à l'extérieur des frontières européennes crée justement une faille dans la capacité de la puissance publique à les contrôler**. Ce point a fait l'objet d'une attention particulière de la part de la commission d'enquête : dans quelle mesure les droits français et européen sont-ils capables d'assurer une régulation effective des pratiques des acteurs propriétaires des infrastructures numériques essentielles ?

À l'inverse, les sujets suivants n'ont pas été traités par la commission d'enquête :

– la cybersécurité. La préservation de la cybersécurité est bien sûr fondamentale et requiert la mise en œuvre de mesures de protection très fortes, avec le soutien de la puissance publique. Toutefois, elle n'emporte pas nécessairement d'enjeux systémiques et aurait nécessité des investigations spécifiques ;

– les ingérences informationnelles : ce thème, étroitement lié aux enjeux diplomatiques, touche à des thématiques qui vont au-delà de la sphère numérique. Il a de plus fait l'objet d'un traitement récent par la commission des affaires étrangères de l'Assemblée nationale [(1)] ;

– les infrastructures matérielles autres que les data centers (puces, câbles sous-marins).

**L'analyse de ces trois sujets aurait fait ressortir d'autres dépendances et vulnérabilités à des grandes puissances internationales : à la Chine dans le**

---

*(1) M. Alain David et Mme Laetitia Saint-Paul, rapport d'information sur l'irruption de l'intelligence artificielle dans les ingérences étrangères, janvier 2025.* https://www.assemblee-nationale.fr/dyn/17/dossiers/irruption_intelligence_artificielle_dans_ingerences_etrangeres

**domaine de l'approvisionnement en matériel, à la Russie s'agissant des menaces de cybersécurité et d'ingérences informationnelles. La commission d'enquête ne disposait pas du temps suffisant pour couvrir l'ensemble de ces thématiques.**

## UNE ANALYSE INÉDITE : DES LOGICIELS DÉPLOYÉS DANS LES MINISTÈRES AUX EFFETS SYSTÉMIQUES DE L'INTELLIGENCE ARTIFICIELLE

### A. LES ADMINISTRATIONS PUBLIQUES ET LES ENTREPRISES D'INTÉRÊT VITAL : UNE IMPORTANCE QUI JUSTIFIAIT UN TRAITEMENT PARTICULIER

#### 1. Objectifs

Une analyse par cercles concentriques permet de pondérer l'importance des risques selon le statut et le rôle des entités menacées. Trois niveaux peuvent ainsi être distingués.

– Les **administrations** doivent être soumises à des règles de protection particulières du fait de leur rôle au service de l'ensemble des concitoyens, des services qu'elles fournissent, mais également de leur manipulation de données confidentielles à des fins opérationnelles (exemples : services des impôts, données de santé, etc.).

En raison du temps de travail limité dont elle disposait et de sa concomitance avec les élections municipales, la commission n'a pas traité de manière approfondie la situation des collectivités territoriales. Certaines données, provenant de la centrale d'achat publique Ugap (Union des groupements d'achats publics), sont présentées dans le rapport, mais elles ne sont pas exhaustives. Les collectivités territoriales étant un acteur majeur de la souveraineté numérique, ce sujet mériterait un traitement à part entière.

– De par leur taille critique ou leur rôle dans l'exploitation d'un service, **les entreprises ou secteurs clés** prennent une place spécifique dans l'économie française tant leur défaillance pourrait revêtir des conséquences importantes. Ce peut être des entreprises industrielles, bancaires, des médias, etc. Les réglementations européennes et françaises créent d'ores et déjà des obligations spécifiques aux entités économiques essentielles, comme par exemple les directives NIS 1 et NIS 2 (*Network and Information Security*), cette dernière étant en cours de transposition par **le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité – dont la poursuite de l'examen est fortement attendue par le Parlement**. Parmi cette catégorie, les **opérateurs d'importance vitale (OIV)** sont ceux dont la sauvegarde est essentielle à la préservation de la souveraineté du pays (défense nationale, intérieur, etc.) ou dont la fragilisation aurait des conséquences immédiates et massives (exemple : gestionnaires de réseaux d'infrastructures, etc.). Les grandes entreprises, même non chargées de missions essentielles, sont également des acteurs dont les difficultés

peuvent avoir des répercussions à grande échelle, quel que soit le secteur considéré : grande distribution, agro-alimentaire, industrie, construction, assurance, etc.

– Enfin, **l'économie générale** est constituée de l'ensemble du tissu économique, formé des TPE, PME et ETI, ainsi que des particuliers. Ces acteurs ne disposent pas de moyens spécifiques (direction des services d'information, etc.) pour se doter d'outils informatiques propres, ou ne peuvent se tourner vers des solutions plus coûteuses.

Dans un contexte géopolitique marqué par la hausse des menaces américaines, la dépendance des administrations et des entreprises ou secteurs clés à des solutions logicielles et cloud non européennes fait courir le risque de paralysie de systèmes critiques. L'objectif est de mesurer ces dépendances et d'examiner dans quelle mesure des solutions françaises/européennes peuvent constituer des alternatives, et à quelles conditions (compétitivité, performance, etc.).

Pour le périmètre des acteurs retenus (cf. paragraphe suivant), la rapporteure a défini les objectifs suivants :

– Disposer d'un **panorama le plus complet possible et chiffré des achats logiciels et services cloud** des administrations et des services clés.

– Déterminer dans quelle mesure des stratégies techniques et contractuelles sont mises en œuvre pour **assurer la résilience des systèmes d'information, des services et la protection des données.** Chaque ministère, chaque service public est-il en mesure de continuer à fonctionner sous la menace d'un retrait unilatéral de technologies américaines ?

– Comprendre la place des acteurs et de l'emploi français dans la fourniture des services informatiques à la sphère publique et le rôle de la commande publique et privée dans l'accompagnement de la structuration d'une filière numérique française.

### 2. Plan de travail

Le degré de détail des investigations menées par la commission d'enquête a été adapté en fonction des structures concernées.

Au regard de leur importance, mais également du rôle conféré à l'Assemblée nationale de contrôle de l'action du Gouvernement, une approche systématique a été suivie pour les administrations d'État. Les autres acteurs publics ont été intégrés dans l'analyse, mais sans vocation d'exhaustivité, selon les modalités décrites ci-dessous.

**SOLLICITATIONS DE LA COMMISSION D'ENQUÊTE PAR TYPE D'ACTEUR PUBLIC**

| Acteur public | Modalités de sollicitation |
|---|---|
| Administrations d'État | Questionnaire à destination des administrations (voir liste en annexe)<br>Auditions des directions des systèmes d'information (DSI) (1)<br>Questionnaire à destination de la direction interministérielle du numérique (Dinum) |
| Administration hospitalière | Questionnaire à destination de l'AP-HP (Assistance publique-Hôpitaux de Paris) |
| Collectivités territoriales | Non traité en raison du temps d'enquête limité et de la concomitance avec les élections municipales |
| Grands instituts de recherche publics | Table ronde réunissant des DSI d'organismes de recherche (2) |
| Opérateurs d'importance vitale | Questionnaire à destination d'une sélection d'entreprises publiques opérant un service critique d'importance vitale (voir liste en annexe) |
| Transverse | Table ronde réunissant les centrales d'achat publiques (3)<br>Questionnaire à destination de l'Ugap |

Enfin, le secteur bancaire, et plus particulièrement la question des moyens de paiement, a fait l'objet d'une étude de cas, dans la mesure où ce secteur est géré par des opérateurs privés, sous supervision de la puissance publique.

## B. LES DÉPENDANCES SYSTÉMIQUES : UNE APPROCHE GLOBALE

### 1. Objectifs

Le second axe d'analyse consiste à évaluer les dépendances systémiques engendrées par la concentration de pouvoirs dans les mains de quelques acteurs de taille mondiale.

Fortes de leur position économique dominante, les Gafam génèrent des gains qui leur permettent d'accroître une avance technologique déjà très importante et d'assoir leur position dans le marché des services numériques. En 2025, Microsoft a dégagé 160 milliards de dollars de revenus de ses activités, Google 165 milliards, Amazon 140 milliards et Meta 60 milliards. Ensemble, les quatre sociétés prévoient d'investir plus de 650 milliards en 2026 dans l'IA (4). Elles disposent de l'accès aux meilleures ressources humaines, techniques et financières et suivent des rythmes de développement très rapides.

Cette captation de valeur génère les revenus permettant d'accroître leur domination technologique, grâce à des investissements colossaux dans les infrastructures clés, en particulier les data centers.

---

*(1) Auditions des 9 avril et 7 mai 2026.*

*(2) Audition du 1er avril 2026.*

*(3) Audition du 9 avril 2026.*

*(4) M. Arnaud Leparmentier, « IA : la folle course des géants américains de la tech »,* Le Monde*, 7 février 2026* https://www.lemonde.fr/economie/article/2026/02/07/intelligence-artificielle-la-folle-course-des-geants-de-la-tech_6665758_3234.html

Dans un secteur en voie d'accélération, **les années à venir sont cruciales pour endiguer le renforcement de positions dominantes qui accentueront encore la dépendance aux solutions et infrastructures extra-européennes.**

La rapporteure a défini les objectifs suivants :

– Expliquer pourquoi les produits développés par les firmes américaines se sont imposés et continuent d'évincer du marché leurs alternatives européennes. Pourquoi ces dernières n'ont-elles pas émergé ? Quels sont les freins, réels et imaginaires ? Comment éviter de bâtir de nouvelles dominations ou d'en prolonger de certaines avec le déploiement rapide de l'intelligence artificielle générative ?

– **Décrire l'usage de la donnée personnelle à des fins de monétisation**, en identifiant les risques pour la protection de la vie privée. En novembre 2025, la Commission européenne a publié une proposition de règlement omnibus numérique, qui modifie des régulations structurantes et historiques comme le RGPD, le règlement sur l'intelligence artificielle (Artificial Intelligence Act – AI Act) et le règlement sur les données (Data Act). La commission présente ces modifications comme une simplification des lois numériques de l'Union européenne à des fins de compétitivité, alors que de nombreux acteurs considèrent qu'elles constituent une déréglementation défavorable aux citoyens et à la filière numérique européenne. Cet omnibus digital est-il positif pour les Européens ou bien est-il imposé par des acteurs dont l'intérêt est d'affaiblir la protection des données personnelles afin d'accroître leur monétisation ?

– **Comprendre les prises de position des acteurs mondiaux sur les infrastructures vitales**, en prenant comme cas d'étude les data centers. Le Président de la République a annoncé 109 milliards d'euros d'investissements privés lors du Sommet pour l'action sur l'intelligence artificielle qui s'est tenu à Paris en février 2025. La politique gouvernementale est aujourd'hui très clairement favorable au déploiement des capacités de data centers sur notre territoire. Quelles sont les conséquences d'une telle politique ? L'implantation de data centers est-elle effectivement un outil de réduction de nos dépendances, et à quelles conditions ? Dans quelle mesure un tel déploiement profiterait-il réellement aux acteurs économiques français en leur permettant de regagner une place dans l'écosystème numérique ?

### 2. Plan de travail

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

– autorités indépendantes : Commission nationale de l'informatique et des libertés (Cnil) et Autorité de la concurrence ;

– opérateurs économiques de l'État : Caisse des dépôts, Banque publique d'investissement ;

– chercheurs, journalistes et experts dans le domaine du numérique et de la protection des données personnelles ;

– associations de protection du droit à la propriété des données personnelles ;

– représentants d'entreprises du numérique et du monde économique ;

– anciens dirigeants politiques.

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

Enfin, le sujet des data centers a fait l'objet d'un traitement particulier, à travers l'envoi de questionnaires à l'administration.

*
* *

La spécificité du travail de la commission d'enquête tient au fait d'avoir conduit ces deux analyses en parallèle. Des travaux avaient été menés séparément sur chacun des deux axes. Dans un rapport datant de septembre 2025, la Cour des comptes avait ainsi examiné les enjeux de souveraineté des systèmes d'information civils de l'État (1). De la même manière, le Sénat, dans sa commission d'enquête sur les coûts et les modalités effectifs de la commande publique et la mesure de leur effet d'entraînement sur l'économie française de juillet 2025 (2), avait traité des enjeux de la souveraineté numérique dans la commande publique, toutes administrations confondues. D'autres rapports ont pu analyser l'ampleur du phénomène des dépendances numériques au niveau de l'ensemble de l'économie.

Le travail de la commission d'enquête, combinant une approche précise et ciblée sur les administrations et un examen plus général du fonctionnement du secteur du numérique, a ainsi permis de dégager une analyse globale du phénomène et des moyens d'action qui dépassent des diagnostics secteur par secteur.

Restituant les échanges avec les acteurs confrontés chaque jour à la réalité de la situation, le présent rapport explore en profondeur les dimensions techniques, juridiques et économiques des dépendances et vulnérabilités aux géants de la tech américains que nous avons laissé se construire au fil des dernières décennies.

---

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

*(2) M. Dany Watteebled, rapporteur de la commission d'enquête du Sénat sur les coûts et les modalités effectifs de la commande publique et la mesure de leur effet d'entraînement sur l'économie française, « L'urgence d'agir pour éviter la sortie de route : Piloter la commande publique au service de la souveraineté économique », juillet 2025.*

*https://www.senat.fr/travaux-parlementaires/structures-temporaires/commissions-denquete/commission-denquete-sur-les-couts-et-les-modalites-effectifs-de-la-commande-publique-et-la-mesure-de-leur-effet-dentrainement-sur-leconomie-francaise.html*

# PREMIÈRE PARTIE : LE DIAGNOSTIC

## CHAPITRE 1 – MICROSOFT, VMWARE, ORACLE, CES TROIS LOGICIELS QUI NOUS GOUVERNENT – LES DÉPENDANCES DES ADMINISTRATIONS AUX SOLUTIONS AMÉRICAINES

Étape incontournable dans l'analyse des vulnérabilités induites par le numérique, l'examen des dépendances de l'État aux solutions extra-européennes a constitué le premier objectif de la commission d'enquête. Dans quelle mesure le recours à des logiciels et services fournis par les Gafam fait-il peser une menace sur le fonctionnement de nos services publics, y compris les plus critiques d'entre eux ?

Les analyses développées dans le présent chapitre s'appuient sur les informations collectées par la rapporteure auprès des administrations par le biais de questionnaires – dont le modèle est reproduit en annexe n° 2. Les données recueillies portent sur les éléments suivants :

– pour les logiciels remplissant des fonctions support (bureautique, systèmes d'exploitation, gestion de bases de données, etc.) : des informations concernant le fournisseur et sa nationalité d'origine ainsi que le montant annuel des dépenses de licences ;

– pour les logiciels métiers : le type de logiciel (développé spécifiquement pour les besoins du ministère ou à façon), les modalités de développement (externe ou interne), le degré de criticité et le degré de dépendance à la solution choisie ; il est à noter que la commission s'en est tenue, sur ce point, aux dépendances de premier rang, et n'a pas pu étudier en détail les solutions technologiques sur lesquelles reposent ces logiciels métiers (hors logiciels support décrits ci-dessus) ;

– pour les solutions cloud : la liste des contrats cloud signés ;

– pour les solutions IA : la liste des contrats signés et les fonctionnalités.

Ces données sont complétées de réponses écrites détaillant les stratégies mises en œuvre par chacune des directions numériques des ministères. Enfin, certains directeurs des systèmes d'information ont été auditionnés par la commission d'enquête.

## A. LES APPLICATIONS MÉTIERS : LE RECOURS PRINCIPALEMENT À DES FOURNISSEURS FRANÇAIS, DES VULNÉRABILITÉS DANS CERTAINS MINISTÈRES

### 1. Données sources

Les constats suivants reposent sur les données recueillies auprès des ministères sollicités. Elles portent sur un total de 466 applications métiers recensées : il ne s'agit pas d'un recensement exhaustif. Si certaines administrations ont transmis la liste de l'ensemble de leur parc applicatif, d'autres ont communiqué une sélection des applications métiers qu'elles jugeaient pertinentes au regard de l'objectif de la commission d'enquête.

Pour certains critères, les données sont insuffisamment renseignées (mentions « NC » pour « non communiqué » ou cases vides).

Néanmoins, les informations collectées sont cohérentes avec les réponses écrites transmises par ailleurs, et peuvent donc être considérées comme fiables pour fournir une vision de la situation du parc applicatif des administrations.

### 2. Modes de développement des applications métiers : la prédominance des logiciels spécifiques

Les applications métiers sont constituées d'une combinaison de solutions développées pour les besoins propres des ministères et de produits achetés sur étagères. S'agissant des solutions à façon, les développements sont réalisés par des entreprises de services numériques, ou bien pilotées en interne, le cas échéant avec l'appui de prestataires intégrés aux équipes de développement. Les proportions de chacune des catégories d'application varient selon les administrations et les effectifs dont elles disposent pour les tâches de développement.

Les questionnaires envoyés aux administrations ont permis de collecter des informations sur :

– la répartition des logiciels entre progiciels sur étagères et applications « à façon », développées spécifiquement pour les besoins de l'utilisateur ;

– la répartition des développements entre développements externes, développements internes et développements assurés par une équipe interne avec des renforts externes (externe/interne).

Les chiffres recueillis auprès des administrations montrent que :

– les logiciels spécifiques représentent deux tiers du total (303 sur un total de 466), contre seulement 30 % pour les logiciels sur étagères ;

– les développements réalisés par des sociétés externes représentent 57 % du total (266 développements externes sur 466), les développements pilotés par des

équipes projets internes mais avec un appui externe concernent 25 % des cas (116 projets), les développements internes représentant une minorité (11 %, soit 33 projets) (1).

### 3. Dépendances à des fournisseurs extra-européens

Une première source de vulnérabilités a été identifiée à travers l'analyse comparée des stratégies d'internalisation/externalisation menées par les différentes administrations. Le second facteur est le recours à des fournisseurs extra-européens pour des applications critiques. Sur ce dernier point, la détection des vulnérabilités est menée en étudiant de manière combinée plusieurs critères :

– le pays d'origine du fournisseur ;

– la capacité à substituer une solution par une autre, immédiatement ou selon un horizon de temps défini ;

– la criticité de l'application. Ici, sont retenues deux catégories, en cohérence avec celles retenues dans la doctrine Cloud au centre (2) : les « 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 les « applications dont le défaut est susceptible d'engendrer l'interruption de l'exercice d'une mission de service public essentielle ». Ces deux catégories sont appelées respectivement « catégorie 1 » et « catégorie 2 » dans les développements suivants – sachant qu'une même application peut appartenir aux deux catégories à la fois ;

– les coûts de développement engagés pour la réalisation de l'application ou les coûts de licences payés annuellement ;

– la maîtrise des codes sources ou le recours à des solutions open source.

Les deux tableaux suivants illustrent la nationalité des fournisseurs pour les applications critiques (catégorie 1 à gauche et catégorie 2 à droite). Il ressort de l'analyse que pour ces applications :

– les fournisseurs français sont très majoritaires, avec respectivement 69 % et 83 % du total ;

– les États-Unis sont le deuxième pays fournisseur, avec sept applications pour la catégorie 1 (dont une application non substituable et une application substituable à un horizon compris entre un et trois ans) et douze applications pour la catégorie 2 (dont une non substituable et trois à un horizon compris entre un et trois ans).

---

*(1) Le complément à 100 % est constitué des projets pour lesquels aucune information n'est disponible sur ce critère.*

*(2) Pour une présentation détaillée de la doctrine Cloud au centre, voir chapitre 1, C., 1.*

**DÉPENDANCES PAR PAYS POUR LES APPLICATIONS CRITIQUES**

| Pays | **Nombre d'applications Catégorie 1** | **Nombre d'applications Catégorie 2** |
|---|---|---|
| **Allemagne** | **7** | **8** |
| En cours | 1 | 1 |
| Non | 1 | 1 |
| 5 ans | | 1 |
| NC | 5 | 5 |
| **Canada** | **1** | **2** |
| Non | | 1 |
| NC | 1 | 1 |
| **Chine** | **5** | **5** |
| NC | 5 | 5 |
| **Corée** | **3** | **3** |
| NC | 3 | 3 |
| **États-Unis** | **7** | **12** |
| 1 an – 3 ans | 1 | 3 |
| En cours | 1 | 1 |
| Oui – délai non connu | | 1 |
| Oui - immédiate | | 1 |
| Non | 1 | 1 |
| NC | 4 | 5 |
| **France** | **81** | **228** |
| < 1 an | 3 | 3 |
| 1 an – 3 ans | 5 | 8 |
| 3 ans – 5 ans | 4 | 5 |
| 5 ans | 2 | 2 |
| À l'étude | 4 | 5 |
| En cours | 8 | 9 |
| Non | 23 | 144 |
| Oui – délai non connu | | 1 |
| Oui – immédiate | 6 | 7 |
| NC | 26 | 44 |
| **Japon** | **3** | **3** |
| NC | 3 | 3 |
| **Pays-Bas** | **1** | **3** |
| Non | 1 | 2 |
| NC | | 1 |
| **Royaume-Uni** | **2** | **3** |
| Non | 1 | 2 |
| NC | 1 | 1 |
| **Suède** | **6** | **6** |
| 1 an – 3 ans | 1 | 1 |
| NC | 5 | 5 |
| **Suisse** | **2** | **2** |
| 5 ans | 2 | 2 |
| **Total** | **118** | **275** |

*Source : réponses aux questionnaires de la rapporteure.*

Lecture : les catégories sont définies ainsi :

- En cours : Substitution en cours de mise en œuvre
- À l'étude : substitution à l'étude
- Oui – immédiate / Oui – délai non connu : substitution immédiate possible / substitution possible mais sous un délai inconnu
- Non : pas de substitution identifiée
- 1 an – 3 ans / 3 ans – 5 ans / 5 ans : substitution réalisée à l'horizon 1 an – 3 ans / 3 ans – 5 ans / supérieure à 5 ans
- NC : information non communiquée

Les deux tableaux suivants fournissent une vision de la nationalité des fournisseurs pour les applications dont le coût de développement a été supérieur à 1 million d'euros ou dont les frais de licences ou de maintien en conditions opérationnelles sont supérieurs à 1 million par an. Ce paramètre constitue un indicateur complémentaire du degré d'importance de l'application en termes de flux gérés et de nombre d'utilisateurs. Les tableaux ci-dessous montrent que, pour ces applications, les dépendances sont limitées.

**DÉPENDANCES PAR PAYS POUR LES APPLICATIONS AU COÛT DE DÉVELOPPEMENT OU AU COÛT DE FONCTIONNEMENT ANNUEL SUPÉRIEUR À 1 MILLION D'EUROS**

| Pays | Applications - Coûts de développement > 1 M€ | Applications - Coûts annuels > 1 M€ |
|---|---|---|
| **Allemagne** | | **3** |
| En cours | | 1 |
| Non | | 1 |
| NC | | 1 |
| **Canada** | **1** | |
| Non | 1 | |
| **États-Unis** | **1** | **2** |
| 1 an – 3 ans | 0 | 1 |
| Oui – délai non connu | 1 | |
| NC | | 1 |
| **France** | **38** | **22** |
| 1 an – 3 ans | 1 | 1 |
| 3 ans – 5 ans | 4 | |
| 5 ans | | 2 |
| À l'étude | 2 | 1 |
| En cours | 1 | 2 |
| Non | 28 | 12 |
| Oui – immédiate | 1 | 1 |
| NC | 1 | 3 |
| Pays-Bas | | **1** |
| Non | | 1 |
| NC | | |
| Royaume-Uni | | **1** |
| Non | | 1 |
| Suisse | **2** | **2** |
| 5 ans | 2 | 2 |
| Total | **42** | **31** |

*Source : réponses aux questionnaires de la rapporteure.*

Le tableau ci-dessous recense les applications dont les coûts de développement ou d'exploitation sont supérieurs à un million d'euros, et dont le pays d'origine du fournisseur n'est pas la France.

**APPLICATIONS CRITIQUES DÉVELOPPÉES PAR DES FOURNISSEURS ÉTRANGERS DONT LES COÛTS DE DÉVELOPPEMENT OU D'EXPLOITATION SONT SUPÉRIEURS À 1 MILLION D'EUROS**

| Administration | Nom de l'application | Objet | Nom du fournisseur | Pays d'origine |
|---|---|---|---|---|
| AP-HP | Orbis | Orbis est la solution principale du SI Hospitalier de l'AP-HP, au cœur de la gestion du patient et de la production des soins.<br>La solution Orbis est déployée par module sur l'ensemble des établissements AP-HP : se rapporter au plan de déploiement pour le détail des déploiements réalisés. L'application Orbis, dans le portefeuille des applications, décrit le fonctionnel et le technique transverse et commun à tous les modules. | Dedalus | Allemagne |
| AP-HP | Glims | L'application Glims est un système de gestion de laboratoires (SGL) qui permet d'organiser et d'automatiser l'ensemble des processus du laboratoire (pré-analytique, analytique et post-analytique), de l'enregistrement de la demande des services cliniques au rendu des résultats en passant par la récupération des résultats fournis par les automates. Il permet de garantir un service de qualité au prescripteur et au patient en intégrant notamment la prescription connectée (transmission des données de prescription depuis Orbis). | Clinysis | États-Unis |
| AP-HP | Picture archiving communication | Outil de stockage et d'archivage des examens d'imagerie médicale à l'AP-HP. Cela représente environ 42 M d'examens archivés et accessibles en temps réel par les médecins et autres utilisateurs. L'AP-HP produit environ 2,7 M d'examens par an pour 1,2 M de comptes rendus de radiologie. | Philips | Pays-Bas |
| DGGN | CSI-OPS | Application de gestion des sollicitations et des interventions. Elle vise à faciliter et optimiser l'engagement des personnels et des moyens de la GN, auprès des usagers. | Techwan | Suisse |
| DGGN | BDSP OPS (GSI) | BDSP OPS a pour finalité la gestion des sollicitations des usagers et des interventions. Il s'agit d'un SI majeur pour la GN (12 millions de fiches produites par an, plus de 3 millions d'interventions suivis, environ 4-5000 utilisateurs en temps réel). | Techwan | Suisse |
| Justice (DGAP) | Saphir | Fourniture des équipements de surveillance électronique | AUEM | Royaume-Uni |
| Ministères économiques et financiers (MEF) | CHORUS | Gestion des déplacements temporaires (ordres de mission, états de frais, changements de résidence) (SAP Concur) - Gestion des dépenses, comptabilités budgétaire et comptable, recettes non fiscales (SAP) | SAP | Allemagne |

Enfin, s'agissant des stratégies techniques et contractuelles mises en œuvre par les administrations pour se prémunir de la dépendance aux fournisseurs, le tableau suivant précise le nombre d'applications pour lesquelles chaque administration est propriétaire des codes sources (en ligne) et les applications qui sont développées en open source (en colonne). Par exemple, la Caisse nationale des allocations familiales (Cnaf) ne dispose pas du code source pour les huit applications recensées, contrairement à la Caisse nationale de l'assurance maladie (Cnam) pour les 102 applications renseignées. Les deux administrations ayant le plus recours à des applications open source sont la gendarmerie nationale (sept applications) et le ministère de l'agriculture, de l'agro-alimentaire et de la souveraineté alimentaire.

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).

**PROPRIÉTÉ DES CODES SOURCES ET USAGE DE L'OPEN SOURCE DANS LES APPLICATIONS MÉTIERS DES ADMINISTRATIONS**

| Ministère | Open source : Non | Open source : Oui | Total |
|---|---|---|---|
| **AP-HP** | **9** | **1** | **10** |
| Non propriétaire | 1 | | 1 |
| Propriétaire | 8 | 1 | 9 |
| **CNAF** | **8** | | **8** |
| Non propriétaire | 8 | | 8 |
| Propriétaire | | | |
| **CNAM** | **102** | | **102** |
| Non propriétaire | | | |
| Propriétaire | 102 | | 102 |
| **Culture** | **7** | **3** | **10** |
| Non propriétaire | 5 | 1 | 6 |
| Propriétaire | 2 | 2 | 4 |
| **DGESIP (1)** | **2** | **1** | **3** |
| Non propriétaire | | | |
| Propriétaire | 2 | 1 | 3 |
| **DGGN (2)** | **25** | **7** | **32** |
| Non propriétaire | 9 | 1 | 10 |
| Propriétaire | 16 | 6 | 22 |
| **DGPN (3)** | **18** | **1** | **19** |
| Non propriétaire | 1 | 1 | 2 |
| Propriétaire | 17 | | 17 |
| **Éducation nationale** | **4** | **1** | **5** |
| Non propriétaire | 3 | | 3 |
| Propriétaire | 1 | 1 | 2 |
| **France Travail** | **1** | | **1** |
| Non propriétaire | | | |
| Propriétaire | 1 | | 1 |
| **Justice** | **73** | | **73** |
| Non propriétaire | 54 | | 54 |
| Propriétaire | 19 | | 19 |
| **Agriculture** | **8** | **30** | **38** |
| Non propriétaire | 4 | | 4 |
| Propriétaire | 4 | 30 | 34 |
| **Europe et affaires étrangères** | **63** | **3** | **66** |
| Non propriétaire | 22 | 2 | 24 |
| Propriétaire | 41 | 1 | 42 |
| **Ministères économiques et financiers** | **13** | **1** | **14** |
| Non propriétaire | 3 | | 3 |
| Propriétaire | 10 | 1 | 11 |
| **Ministères sociaux** | **17** | | **17** |
| Non propriétaire | 16 | | 16 |
| Propriétaire | 1 | | 1 |
| **Transition écologique (MTE)** | | 19 | 19 |
| Non propriétaire | | | |
| Propriétaire | | 19 | 19 |
| **Total** | **350** | **67** | **417** |
| Non propriétaire | 126 | 5 | 131 |
| Propriétaire | 224 | 62 | 286 |

*Source : réponses aux questionnaires de la rapporteure.*

*(1) direction générale de l'enseignement supérieur et de l'insertion professionnelle.*

*(2) direction générale de la gendarmerie nationale.*

*(3) direction générale de la police nationale.*

## B. LOGICIELS SUPPORTS : LA DÉPENDANCE À TROIS ACTEURS AMÉRICAINS, MICROSOFT, ORACLE ET VMWARE

Si les situations sont assez variables entre les ministères pour les applications métiers, les dépendances critiques identifiées pour les logiciels supports sont les mêmes dans l'ensemble des administrations. Seules celles ayant d'ores et déjà lancé des plans de basculement vers des solutions de substitution open source sont en mesure de limiter leurs vulnérabilités.

### 1. Dépendance généralisée aux outils Microsoft : systèmes d'exploitation et suite bureautique Office 365

La dépendance aux outils Microsoft est profondément ancrée dans les systèmes d'information des administrations. À l'exception de la gendarmerie nationale, qui a généralisé le recours à des solutions open source (voir *infra*), l'ensemble des administrations interrogées sont concernées.

Cette dépendance tire parti de deux facteurs :

– l'habitude créée auprès des utilisateurs des produits. Selon le ministère de l'Europe et des affaires étrangères : « *l'impact auprès des utilisateurs métier [de la sortie des produits Microsoft] est élevé. La faisabilité technique est en cours de vérification mais les premiers indicateurs sont positifs. En revanche, le risque de rejet des utilisateurs importants. De plus, une sortie totale n'est pas possible au regard de la nécessité d'assurer une continuité de service sur certains services numériques et logiciels d'accessibilité* ».

– l'interconnexion des outils Microsoft avec l'ensemble des applicatifs développés autour. Ainsi que l'indiquent les ministères sociaux : « *La sortie de Windows pour les postes de travail paraît peu réaliste à date, aucune solution actuelle sur étagère n'offrant la maturité fonctionnelle nécessaire pour garantir la continuité de service et le niveau de productivité des agents des ministères, dans un contexte notamment de très forte pression et de réduction des effectifs. Il est difficile d'envisager une sortie de Windows à court terme en raison de son rôle central dans les environnements de travail, tant pour les postes utilisateurs que pour de nombreux outils métiers et dispositifs périphériques. Le système d'exploitation est aujourd'hui profondément intégré à l'écosystème métier et applicatif, aux mécanismes de sécurité, aux annuaires et aux chaînes de support, rendant toute substitution brutale risquée pour la continuité de service. D'autant que le SI des MSO [maladies à signalement obligatoire] souffre encore de fragilités structurelles (obsolescence, sécurité) non réglées. Une telle évolution supposerait enfin des investissements importants en adaptation logicielle, en formation et en accompagnement des usages, qui ne peuvent être conduits que dans une trajectoire de moyen à long terme ».* Le constat rejoint celui formulé par le Commissariat à l'énergie atomique et aux énergies alternatives (CEA) : *« Nous ne parviendrons pas à remplacer l'ensemble des suites commerciales. Microsoft, par exemple, est très profondément ancré dans nos systèmes d'information, au-delà de ce que l'on voit*

*comme le système d'exploitation ou la suite Office ; il pilote aussi la gestion de nos identités avec Active Directory ou la gestion de nos parcs de PC et de serveurs. Nous essayons tous d'aller vers l'open source là où c'est possible, mais ce n'est pas possible partout* » [(1)].

– la nécessité d'inscrire dans le temps long le processus de basculement des outils propriétaires vers le logiciel libre ; ce point sera développé dans la suite du rapport.

### 2. Dépendance structurelle aux outils Oracle (gestion des bases de données) et VMWare (virtualisation) et dans une moindre mesure IBM et Red Hat

Outre les outils déployés par Microsoft, les principales dépendances identifiées concernent les solutions Oracle et VMWare, communes à la plupart des entités interrogées. IBM et Red Hat sont également cités par plusieurs d'entre elles.

Les solutions concernées ont la particularité d'être fortement intégrées aux systèmes d'information (SI), ce qui rend la transition vers des alternatives difficile. Ainsi que l'indique le ministère de la justice : « *Le fonctionnement* [des] *logiciels métier peut reposer sur des briques logiciels et des infrastructures, pour partie soumises à des dépendances. Les principales vulnérabilités en matière de dépendance sont les éditeurs pour les systèmes d'exploitation et couches middleware, notamment VMWare, Oracle, Windows. Pour ces dépendances, les schémas de résilience doivent être travaillés sur plusieurs années. Des substitutions peuvent être envisagées pour certaines d'entre elles sur un délai de moyen terme. Pour d'autres (par exemple, le système d'information Windows sur les ordinateurs), un remplacement dans ce délai devrait faire l'objet d'une étude de faisabilité spécifique* ***et nécessiterait des ressources (agents publics et ressources budgétaires) complémentaires dans le cadre d'un arbitrage interministériel*** ».

L'Assistance Publique-Hôpitaux de Paris (AP-HP) indique que « *globalement, nous disposons plutôt de logiciels métiers français ou européens, assez compétitifs en termes de coût – notamment poussés par la concurrence – mais parfois immatures en termes de produit ou d'innovation. À l'inverse, les solutions d'infrastructure et de sécurité, nécessaires pour porter ces solutions métier, sont quasi exclusivement américaines et israéliennes (…). Pour les logiciels support, (…) nous avons clairement identifié les principaux éditeurs non européens avec lesquels nous avons une dépendance technologique que nous jugeons excessive. Nous avons identifié des actions prioritaires (ex : systèmes de gestion de bases de données, virtualisation, sauvegardes, outils collaboratifs, etc.) et entamé des projets de réduction de cette dépendance, plus ou moins avancés – avec un faible appui financier externe de ces initiatives* ».

*(1) Audition de M. Baptiste Grigy, directeur des systèmes d'information du Commissariat à l'énergie atomique et aux énergies alternatives (CEA) ;*

**La Cnam** a réalisé en 2025 un premier état des lieux des dépendances à des solutions propriétaires critiques. « *Les constats ont été les suivants :*

« *– 85 % des dépenses logicielles sont réparties entre 8 fournisseurs dont 7 sont américains*

« *– 80 % de nos applications cœur de métier utilisent des solutions étrangères telles que Oracle, Broadcom, RedHat, IBM, Microsoft...*

« *À la suite de ce premier état des lieux, plusieurs actions ont été identifiées dont celle prioritaire portant sur la finalisation de la cartographie des dépendances associée à une mesure pragmatique et pondérée de la dépendance* ».

La **Caisse nationale d'assurance vieillesse** (**Cnav)** a lancé des actions de réduction des dépendances qui visent à se désengager de la plateforme IBM d'ici 2031, à réduire le nombre de bases de données opérées sous Oracle et à rechercher des solutions alternatives à VMWare pour la virtualisation.

Les actions menées par **le ministère de l'éducation nationale** sont très similaires : « *il s'agit principalement de faire évoluer les architectures techniques des produits en service, pour beaucoup conçus entre 2000 et 2010, pour réduire la dépendance aux éditeurs des composants techniques sélectionnés à l'époque comme les serveurs d'application (Oracle) et serveurs de bases de données (Oracle, IBM). La voie poursuivie par le ministère consiste à substituer progressivement ces composants par des équivalents open source (Tomcat, PostgreSQL). Des crédits sont programmés en 2026 sur ce sujet et une trajectoire pluriannuelle est engagée relativement aux technologies Oracle et IBM.*

« *(...) La solution de virtualisation VMware n'est pas substituable à court terme car son usage est extensif. Son périmètre fonctionnel est bien supérieur à celui communément entendu de la virtualisation et sous-tend un véritable cloud privé dont les effectifs d'administration sont une fraction de ceux communément nécessaires pour des solutions alternatives comme Openstack. Des expérimentations sont en cours pour substituer une partie des services d'infrastructure avec la solution Proxmox. La transition visée par le ministère s'inscrit dans la conteneurisation progressive de son SI, technologie pour laquelle le ministère a réalisé des investissements importants en technologie et en formation. Kubernetes, la technologie phare dans ce domaine, sous-tend la nouvelle application nationale de gestion de la scolarité du 1er degré, équipant en cible l'ensemble des 42 000 écoles publiques du territoire national. Cette application est en déploiement progressif jusqu'à sa généralisation à l'automne 2026, et se substitue à une application équivalente basées sur les technologies Oracle et IBM.*

« *Les bases de données et les serveurs d'application Oracle ne sont pas substituables à 3 ans. Au-delà des réécritures applicatives, qui sont des opportunités évidentes de substitution technologiques mais limitées à des cycles de vie applicatifs assez longs, des expérimentations d'adaptation des applications existantes ont été menées sur plusieurs cas conduisant parfois à des instabilités*

*applicatives. Par ailleurs, dans un contexte de ressources très contraint, les travaux techniques d'adaptation des applications souffrent systématiquement de la concurrence des besoins métiers et de leur traduction en évolutions fonctionnelles, régulièrement sous l'injonction de réformes ou politiques publiques d'urgence ».*

Enfin, s'agissant des **ministères économiques et financiers**, le constat est là encore identique : « *Il n'y a pas aujourd'hui de cartographie des dépendances formalisées à l'échelle des Ministères Économiques et financiers, mais un certain nombre d'aspects critiques des dépendances ont pu faire l'objet de travaux spécifiques ponctuels ou portés sur des périodes plus longues : logiciel de gestion de base de données Oracle, logiciel statistique SAS, logiciel de virtualisation VMWARE* ». Ainsi que l'expliquait Tomasz Blanc, chef du service des systèmes d'information de la direction générale des finances publiques (DGFIP), lors de son audition devant la commission d'enquête : « *Compte tenu de l'ancienneté de notre système, des dépendances extra-européennes subsistent, que nous nous efforçons de maîtriser et de réduire. Nos principales dépendances concernent les infrastructures matérielles, avec IBM et Oracle, quasi exclusivement produites en Asie et aux États-Unis à défaut de solutions européennes complètes. Nous activons toutefois les leviers de la concurrence dans l'acquisition des matériels et des marchés afin de maîtriser au mieux ces dépendances. S'agissant d'IBM, notre dépendance est héritée des années quatre-vingt, à l'image des serveurs IBM Z, qui supportent encore nos applications historiques de calcul de l'impôt ou d'échanges bancaires. Bien que fiables et performants, ces systèmes sont coûteux (4,5 millions d'euros en 2025) et en sortir s'avère complexe. La migration d'applications écrites en Cobol (Common Business-Oriented Language) vers des logiciels libres exige en effet des projets longs et des tests rigoureux, comme l'illustre la refonte progressive de la paie des fonctionnaires d'État. Cette complexité structurelle limite d'ailleurs notre capacité de négociation contractuelle. Quant à Oracle, sur lequel s'appuient encore de nombreuses applications, notre dépendance date du début de l'ère web, époque où cet éditeur s'imposait pour la fiabilité des bases de données. Oracle, qui représente 8,5 millions d'euros annuels, équipe notamment la déclaration en ligne des revenus et la comptabilité locale. Là encore, la richesse fonctionnelle de ces outils rend leur remplacement long et onéreux* ».

En guise de synthèse, le tableau ci-dessous recense, pour chaque administration, l'utilisation de solutions fournies par les cinq principaux fournisseurs de logiciels extra-européens.

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

| | Microsoft | Oracle | VM Ware | IBM | Red Hat |
|---|---|---|---|---|---|
| Ministères sociaux | X | | X | | |
| MAASA (1) | 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 | X | X | | |
| Edu Nat | X | X | X | X | X |
| Gend nat | X | | | | |
| Justice | X | X | X | | X |
| MEAE (2) | X | | X | | |
| Intérieur - DGPN | X | X | X | | |
| France Travail | X | | X | | |

*Source : réponses aux questionnaires de la rapporteure.*

Les éléments recueillis auprès des administrations font ainsi apparaître une dépendance critique aux solutions proposées par quatre acteurs américains. Microsoft en premier lieu, dont les solutions de bureautique et de systèmes d'exploitation, sont déployées sur la quasi-totalité des postes de travail. Oracle, VMWare et IBM fournissent des logiciels qui sont complètement intégrés aux applicatifs des administrations, et dont la sortie requiert des travaux très profonds de rénovation des systèmes d'information. Pour l'ensemble de ces solutions, des alternatives existent, comme le prouve le cas de la gnationale, mais des transitions ne sont envisageables que sur un temps de plusieurs années.

### 3. État du déploiement des solutions open source au sein des administrations : l'exemple à suivre de la gendarmerie nationale, les 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. « *Dès le début des années 2000, la gendarmerie nationale a opéré un virage numérique stratégique en privilégiant la normalisation et l'indépendance vis-à-vis des éditeurs en ayant recours aux logiciels libres. Il s'agissait d'optimiser l'interopérabilité, rationaliser la maintenance et garantir une sécurité, une performance et une fiabilité optimales des SI.*

« *En outre, l'utilisation des logiciels en* open source *permet de ne pas subir l'obsolescence programmée des solutions offertes par les éditeurs. L'intégralité de*

*(1) ministère de l'agriculture, de l'agro-alimentaire et de la souveraineté alimentaire.*

*(2) ministère de l'Europe et des affaires étrangères.*

*la gestion du poste de travail gendarmerie est réalisée en interne afin de répondre aux objectifs de maîtrise technique, industrielle, des données et des coûts. Des équipes dédiées sont chargées de l'architecture logicielle du poste (choix du système d'exploitation et de sa configuration, choix des applicatifs installés, sécurisation du poste de travail) et peuvent s'appuyer sur des équipes de support de proximité pour le déploiement et l'assistance utilisateurs de 1er niveau.*

« *Cette stratégie d'internalisation se retrouve en particulier :*

« *– pour les outils bureautiques, avec un recours quasi général à Libre Office. 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 équipés ;*

« *– pour les messageries individuelles, organiques (boîtes d'unité) et spécifiques (boîtes fonctionnelles partagées pour des besoins particuliers), toutes reposent intégralement sur des logiciels libres (suppression des tous derniers comptes Outlook début 2024) ;*

« *– pour un outil de coédition et de partage de fichiers nommé Partage NG, utilisé par 106 000 personnels de la police et la gendarmerie, que l'ANFSI opère et héberge en interne en se basant sur l'outil libre Nextcloud ;*

« *– pour une solution de gestion électronique de documents (GED), basée sur l'outil libre Nuxeo, avec une offre socle en cours de construction qui servira en premier lieu au répertoire des actes administratifs et des décisions, et au Mémorial (documentation de référence de la gendarmerie).*

« *Elle comprend également les fonctionnalités comme l'authentification, le chiffrement de la communication, le stockage réseau partagé, les fonctionnalités d'inventaire et de suivi du parc.* »

Le déploiement de solutions maîtrisées en interne s'étend jusqu'au parc de smartphones, pour lequel les terminaux et les systèmes d'exploitation sont aussi spécifiés par l'Agence du numérique des forces de sécurité intérieure (Anfsi).

« *Concernant le smartphone NEO, l'ANFSI gère l'intégralité du parc en interne : le système d'exploitation est conçu en partenariat avec l'OSIIC (Opérateur des systèmes d'information interministériels classifiés) dépendant du SGDSN à partir d'une version d'Android, souche libre, qui est spécialement sécurisée. Le magasin d'applications est géré en interne et chaque application passe par un process d'audit avant d'être mise à disposition des utilisateurs. Comme pour le poste de travail Gendarmerie, l'ANFSI maîtrise également tout l'écosystème autour du smartphone.* »

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**. Toutes les directions ne sont pas concernées, mais celles qui le sont rassemblent la majorité des agents, en particulier la DGFIP.

« *Essentiellement pour des raisons de coûts (mais également de stratégie de souveraineté), certaines directions des [Ministères économiques et financiers] (DGFIP, DGDDI, Insee notamment) ont opté pour LibreOffice comme outil bureautique standard sur le poste de leurs agents, tout en maintenant un déploiement ponctuel de la suite bureautique Microsoft Office en " client lourd " en parallèle, rendu nécessaire pour échanger des documents de manière compatible avec certains partenaires extérieurs, en particulier la commission européenne. Les autres directions (administration centrale, DGCCRF, DG Trésor) ont préféré les solutions MS Office propriétaires à la demande de leurs agents, très centrés dans leurs activités d'état-major sur l'outil bureautique. L'accès à ces outils Microsoft se faisait sur la base d'achats de licences, maintenues en conditions de sécurité par l'éditeur sur une période de 10 ans (cas de MS Office 2013). Le changement de politique tarifaire de l'éditeur (durée de maintenance réduite à 5 ans pour MS Office 2021 notamment) a conduit à poser la question d'une bascule vers un mode de redevance annuelle pour lisser l'augmentation liée au changement de modèle financier, tout en maintenant une protection satisfaisante en matière de sécurité.* »

Concernant les dépendances au système d'exploitation Windows ainsi qu'aux produits Oracle, IBM et VMWare, « *Le logiciel libre constitue le pilier central de [la démarche engagée par la DGFIP]. Depuis les années 2000, l'émergence de solutions matures (telles que Linux pour les systèmes d'exploitation ou PostgreSQL pour les bases de données) offre des performances comparables aux produits propriétaires. Pour pallier l'absence de support éditeur, nous avons structuré dès 2005 un marché de support devenu interministériel s'appuyant sur des entreprises françaises spécialisées. Cette approche nous garantit une expertise de haut niveau et une correction réactive des bogues, pour un coût nettement inférieur aux licences classiques. Les résultats concrets valident ce choix puisque depuis 2010, la priorité est systématiquement donnée au logiciel libre pour tout nouveau projet. C'est le cas du prélèvement à la source, dont la brique de collecte des revenus est intégralement libre. Cette stratégie a permis de réduire notre parc Oracle* » [(1)].

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 : « *Le ministère poursuit une politique du numérique cherchant à favoriser les solutions open source. Cette approche poursuit plusieurs objectifs de maîtrise technique, industrielle, des données et des coûts. Toutefois, des contraintes*

*(1) Audition de M. Tomasz Blanc, chef du service des systèmes d'information de la direction générale des finances publiques (DGFIP), le 7 mai 2026.*

*techniques et organisationnelles limitent certains déploiements. Cette démarche se retrouve ainsi dans le choix de la suite bureautique :*

« *– La suite bureautique libre Libre Office est privilégiée par rapport à la suite payante Microsoft Office. Ainsi, on recense pour l'administration centrale, (…) 3 578 licences pour 4 700 PC, pour l'administration territoriale (…), 4 793 licences sur 73 320 PC. Le maintien du recours à Microsoft Office s'explique par des contraintes pour des raisons de compatibilité avec des outils tiers, ou pour les échanges avec des entités partenaires. La gendarmerie nationale fait office de précurseur, avec une politique volontariste ayant permis de limiter l'usage de Microsoft Office à moins de 2 % du parc des postes de travail.*

« *– Les logiciels libres Firefox, Thunderbird, et VLC sont également déployés sur chaque poste de travail du ministère de l'Intérieur, en plus de la suite Libre Office* ».

Enfin, 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. « *S'agissant des solutions* open source*, la direction du numérique est depuis longtemps investie dans leur mise à disposition et leur usage, en complément ou à la place des logiciels bureautiques grand public. Ce choix tient à la culture ingénieur du pôle ministériel, mais aussi à la difficulté à suivre les augmentations tarifaires imposées par Microsoft au début des années 2000 sur un périmètre large, comprenant Exchange et le Pack Office. Le ministère a ainsi fait le choix de LibreOffice pour les éditeurs de documents, et a construit un service de messagerie Mélanie centralisé, sur serveurs nationaux, à partir de briques open source telles que Postfix, Cyrus, Thunderbird, Horde et OpenLDAP. Pour les partages de fichiers Windows, le choix s'est porté sur Samba pour les services territoriaux. Autour de 2010, la gestion des agendas a été ajoutée à Mélanie sans modifier substantiellement le paysage technique (…). Ce positionnement n'exclut pas des recours ciblés à des solutions propriétaires, lorsqu'ils sont justifiés par les usages.* ***Le choix est pragmatique : privilégier d'abord les solutions souveraines ou open source lorsqu'elles répondent au besoin, et recourir à des solutions non souveraines seulement lorsque l'écart fonctionnel le justifie clairement****.* »

### C. VULNÉRABILITÉ DES DONNÉES ET DÉPENDANCES AUX INFRASTRUCTURES DE STOCKAGE

Les informations collectées par la rapporteure sur les modalités d'hébergement des systèmes d'information de l'État font apparaître une moindre dépendance qu'en matière de logiciels. Les administrations stockaient historiquement leurs applications et leurs données en interne, en s'appuyant sur le parc de data centers de l'État, qui comptait 166 sites en 2012, réduit à 58 après des efforts de rationalisation. Le basculement vers le cloud a ensuite conduit l'État à formaliser une doctrine qui impose un hébergement sur des infrastructures souveraines pour les données les plus sensibles afin d'en conserver la maîtrise.

Plusieurs situations d'exposition de données sensibles à des fournisseurs américains ont cependant été identifiées.

### 1. Un impératif de protection des données sensibles formalisé par la doctrine Cloud au centre de l'État

Dans un contexte de prépondérance des *hyperscalers* sur le marché de l'informatique en nuage, la stratégie de l'État sur le cloud a dû pleinement intégrer les enjeux de souveraineté. La doctrine Cloud au centre, introduite par la circulaire du Premier ministre du 5 juillet 2021, s'est ainsi efforcée d'articuler l'objectif de généralisation du cloud avec de fortes garanties en matière de protection des données.

Tout en demandant aux administrations de recourir au cloud pour tout nouveau projet numérique, la circulaire leur impose de s'orienter vers l'un des clouds interministériels ou une offre commerciale disposant de la qualification SecNumCloud de l'Anssi dès lors que « *le système ou l'application informatique manipule des données d'une sensibilité particulière, qu'elles relèvent notamment des données personnelles des citoyens français, des données économiques relatives aux entreprises françaises, ou d'applications métiers relatives aux agents publics de l'État* » (1).

*(1) Circulaire du Premier ministre du 5 juillet 2021.*

**Le référentiel SecNumCloud**

La qualification SecNumCloud a été élaborée par l'Anssi pour reconnaître les offres d'informatique en nuage qui garantissent un niveau élevé de sécurité face aux menaces cybercriminelles et aux lois extraterritoriales.

Le référentiel comporte plus de1 200 exigences, à la fois techniques, organisationnelles et juridiques, dans quatorze domaines (les ressources humaines, la gestion du risque, le contrôle d'accès et la gestion des identités, la cryptologie, la sécurité physique et environnementale, la gestion des incidents, la continuité d'activité etc.).

Il comprend des exigences spécifiques pour prémunir contre les divulgations de données à des autorités étrangères en vertu de lois extraterritoriales : le siège social du prestataire doit être situé dans l'Union européenne ; aucune entité extra-européenne ne doit détenir seule plus de 24 % du capital, et plus de 39 % collectivement ; le prestataire doit être autonome dans l'exploitation de la solution et aucun sous-traitant extra-européen ne doit avoir la possibilité technique d'accéder aux données.

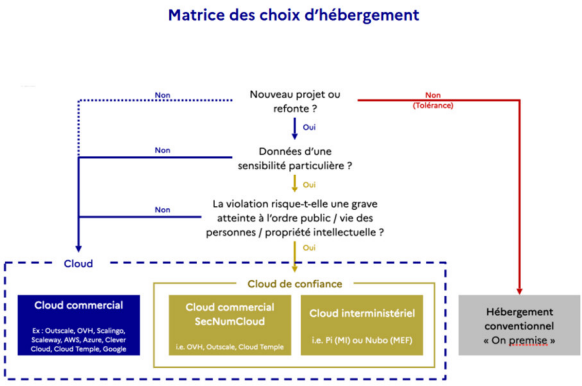
Ces critères n'ont pas pour effet d'exclure les offres de cloud qui reposeraient sur une technologie extra-européenne, à la condition que le prestataire européen soit en mesure de démontrer qu'il maîtrise l'exploitation de la solution et que le fournisseur de la technologie n'a pas accès aux données. L'offre « hybride » S3NS, fournie par Thalès en partenariat avec Google Cloud, a ainsi obtenu la qualification en décembre 2025.

La qualification n'est délivrée par l'Anssi qu'à l'issue d'un processus formalisé d'évaluation, comprenant un audit sur site, qui vise à vérifier que la solution candidate satisfait l'ensemble des critères. La qualification est accordée pour une durée maximale de trois ans, avec des contrôles annuels.

En juin 2026, 17 offres de service disposent de la qualification SecNumCloud, portées par 10 opérateurs (1).

Le champ d'application de cette obligation a été redéfini à l'occasion de l'actualisation de la doctrine Cloud au centre en 2023. La circulaire du 31 mai 2023 n'exige désormais que la solution d'hébergement soit qualifiée SecNumCloud que si deux conditions cumulatives sont remplies : d'une part, il s'agit de données, à caractère personnel ou non, d'une sensibilité particulière ; d'autre part, leur violation est susceptible d'engendrer une atteinte à l'ordre public, à la sécurité publique, à la santé et la vie des personnes ou à la protection de la propriété intellectuelle.

*(1) Anssi, catalogue des produits, services, profils de protection et sites certifiés, qualifiés, agréés, en juin 2026*




*Source : Dinum, Bilan de la doctrine Cloud au centre 2021-2024.*

Le Parlement a élevé cette exigence au niveau législatif par l'adoption de la loi visant à sécuriser et à réguler l'espace numérique du 21 mai 2024, dite loi Sren. Pour les données remplissant les deux conditions précitées, l'article 31 de la loi impose à l'administration de l'État, à ses opérateurs, et à certains groupements de veiller à ce que le service d'informatique en nuage garantisse « *la protection des données traitées ou stockées contre tout accès par des autorités publiques d'États tiers non autorisé par le droit de l'Union européenne ou d'un État membre* ». La définition des critères de sécurité à remplir, la liste des groupements d'intérêt public concernés, et les modalités de dérogation temporaire étaient renvoyées à un décret en Conseil d'État.

Alors que le décret était attendu dans un délai de six mois à compter de la promulgation de la loi, il n'a été publié que le 14 avril 2026. Il prévoit que les offres commerciales devront obtenir une qualification attestant leur conformité au référentiel de l'Anssi qui fixe le niveau d'exigence requis en matière de sécurité des systèmes d'information, de localisation de l'hébergement des données, ou la protection contre tout accès par des autorités publiques d'un État tiers. Les administrations ayant engagé un projet de migration vers le cloud avant la publication du décret pourront solliciter une dérogation auprès du ministre, pour une durée maximum de dix-huit mois si une offre acceptable est disponible en France, et d'un an renouvelable jusqu'à ce qu'une telle offre soit disponible.

### 2. Un hébergement en interne largement privilégié

**Malgré l'existence de la doctrine Cloud au centre, l'administration n'a pas été en mesure de fournir un recensement exhaustif des modalités d'hébergement des systèmes d'information de l'État**. En l'absence de mesure consolidée des dépenses liées aux data centers ministériels (achats de serveurs, capacité de stockage, consommation d'énergie) et des achats de services cloud, qui ne sont pas tous correctement identifiés dans l'application budgétaire et comptable de l'État – Chorus –, il n'est en effet pas possible de les mettre en regard et d'évaluer l'avancée de la migration vers le cloud. Il n'existe pas davantage de recensement

centralisé et systématique des données sensibles à l'échelle interministérielle, leur cartographie étant laissée à la responsabilité de chaque ministère.

Les données collectées par la rapporteure auprès des administrations sur la liste des contrats cloud, complétées par leurs réponses écrites, dégagent cependant un constat clair : **le stockage interne est largement privilégié, avec une ouverture variable aux offres commerciales selon les missions de chaque ministère et la nature des données qu'il est amené à traiter**. Ces résultats sont corroborés par la direction interministérielle du numérique (Dinum), qui indique que « *malgré une augmentation significative du recours au cloud (de l'ordre de 60 %), l'hébergement interne demeure encore largement prépondérant au sein de l'État, les montants concernés restant en valeur absolue modérés, de l'ordre de quelques dizaines de millions d'euros* » (1).

**MODALITÉS D'HÉBERGEMENT DES SYSTÈMES D'INFORMATION DES MINISTÈRES CONSULTÉS**

| Ministère | Recours aux clouds internes | Recours aux clouds commerciaux |
|---|---|---|
| **Affaires étrangères** | Cloud Pi pour France Visas<br>Réflexion pour recourir au cloud Pi pour la diffusion restreinte. | Oui – uniquement SecNumCloud |
| **Culture** | Cloud Nubo (Archives nationales) | Oui - uniquement non SecNumCloud |
| **Économie et finances** | Nubo (principal utilisateur) | Oui - à parts égales SecNumCloud et non SecNumCloud |
| **Intérieur** | Pi (principal utilisateur) | Oui - majoritairement SecNumCloud |
| **Justice** | Projet de migration vers le cloud Pi | Oui - uniquement SecNumCloud |
| **Travail, santé, solidarités et familles** | Non | Oui -majoritairement non SecNumCloud |
| **Agriculture** | Cloud interne Oshimae | Oui - uniquement SecNumCloud |
| **Éducation nationale et recherche** | Cloud interne Cloé | Oui - uniquement non SecNumCloud |
| **Transition écologique** | Cloud interne Eco | Oui – majoritairement SecNumCloud |

*Source : Réponses écrites des ministères.*

### *a. Une forte maîtrise de l'hébergement des systèmes d'information sur le périmètre régalien*

**Le ministère de l'intérieur et la DGFIP 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.

*(1) Réponse écrite de la Dinum au questionnaire de la rapporteure.*

**Le ministère de l'intérieur préconise un hébergement sur le cloud Pi ou sur ses data centers**, comme l'a explicité M. Mathieu Weill, directeur de la transformation numérique, devant la commission d'enquête : « *Nous avons d'ailleurs toujours privilégié la stratégie consistant à héberger nos propres systèmes, dans des centres de données maîtrisés par la puissance publique. Concernant les systèmes d'information les plus sensibles, nous ne pouvons en effet nous permettre la moindre dépendance, même intra-européenne ou nationale. Quand on fait la remontée des résultats des élections, par exemple, on n'a pas très envie qu'un acteur économique, quel qu'il soit, puisse interférer dans le processus, tout simplement pour des raisons de confiance dans la vie démocratique de notre pays. (…) La capacité à héberger nos systèmes dans nos infrastructures, comme le font nos collègues de la DGFIP, qui est le deuxième opérateur interministériel, garantit une forme de continuité, car personne ne peut agir sur ces systèmes ni les interrompre. Cela permet de maîtriser les enjeux d'accès par des tiers à ces infrastructures – et nous savons quel défi cela représente.* » (1) Compte tenu des capacités limitées du cloud Pi, le ministère recourt également aux offres commerciales satisfaisant aux exigences de sécurité de la qualification SecNumCloud, pour les données non sensibles.

L'Anfsi, qui assure la direction des systèmes d'information pour la police et la gendarmerie nationale, applique ce principe de façon encore plus stricte. Son directeur, le général Marc Boget, a ainsi affirmé conserver toutes les données sensibles dans les data centers souverains de Rosny-sous-Bois et de Nogent-sur-Marne, opérés par les équipes de l'Anfsi : « *Comme un trésor que l'on protège, nos données sensibles ne sortent jamais de nos centres car même un SecNumCloud ne peut offrir les garanties de sécurité que procure une exploitation directe par des gendarmes au sein de nos propres casernes* » (2).

Certaines données non sensibles, notamment celles qui ont vocation à être échangées avec les usagers ou des collaborateurs extérieurs aux institutions régaliennes, sont hébergées à l'extérieur par un prestataire français. Le général Marc Boget précise : « *Pour protéger mes données sensibles, j'ai instauré un barrage interdisant toute intrusion dans mon système interne depuis l'extérieur. Toutefois, ce dispositif devient inopérant lorsqu'il s'agit d'interagir avec les usagers, ces derniers n'ayant pas de droit d'accès. J'utilise donc un point applicatif externe, hébergé chez un prestataire rigoureusement sélectionné, où je viens recueillir les données pour les rapatrier. Ce processus repose sur une coupure protocolaire permanente, évitant ainsi tout lien direct avec mes systèmes internes*. »

**La DGFIP, garante du secret fiscal et du secret des affaires, héberge également l'essentiel de ses données dans ses propres infrastructures exploitées par ses agents, contrôleurs ou inspecteurs des finances publiques**, comme l'a expliqué M. Tomasz Blanc devant la commission d'enquête : « *En pratique, la*

*(1) Audition de M. Mathieu Weill, directeur de la transformation numérique du ministère de l'Intérieur, le 9 avril 2026.*

*(2) Audition du général Marc Boget, directeur de l'agence du numérique des forces de sécurité intérieure (Anfsi), le 7 mai 2026.*

*quasi-totalité de nos données, même non sensibles, est hébergée en interne dans nos propres centres de données. Le recours aux Gafam demeure tout à fait exceptionnel et ne concerne que les données publiques, comme c'est le cas pour l'exploitation de photos aériennes au sein de notre SI.* » Si 25 % du SI a migré sur le cloud Nubo, la DGFIP conserve toujours une part élevée *on premise* (sur site). Ce primat donné à l'hébergement interne, même quand la sensibilité des données ne le requiert pas, s'expliquerait par des besoins de standardisation des filières d'hébergement : « *Notre SI traitant très majoritairement des données sensibles, qu'elles soient fiscales ou personnelles, tant pour les particuliers que pour les professionnels, nous ne souhaitons pas développer de filière spécifique pour les rares applications qui n'en contiendraient pas. Nous privilégions une standardisation massive en maintenant ces applications sur les architectures et les filières utilisées pour le reste de nos activités. ».*

Cette vigilance semble s'imposer de façon transversale au sein des ministères économiques et financiers, la réponse écrite du secrétariat général faisant valoir que « *la sollicitation des clouds commerciaux pour l'hébergement des applications ministérielles est très rare et minoritaire et l'hébergement interne est privilégié (cloud DGFIP NUBO ou infrastructures virtualisées internes)* ». Certaines directions ministérielles se tournent cependant vers les offres commerciales, notamment l'Agence pour l'informatique financière de l'État (AIFE) qui n'utilise pas le cloud Nubo.

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**. S'agissant du MEAE, la gestion du SI est entièrement assurée en interne par des équipes dédiées, et l'utilisation du cloud, même interne à l'État, demeure très faible en raison des contraintes du contexte « diffusion restreinte » – un emploi du cloud Pi, qui inclut ce niveau d'exigence de sécurité, est en discussion. Le ministère de la justice héberge également la quasi-totalité de ses applications *on premise*, mais en délègue la gestion à des prestataires français dans le cadre d'infogérances. Déjà utilisateur du cloud Pi, il envisage d'y migrer une plus grande part du SI, en raison du haut niveau de sécurité fourni et de l'intérêt d'un hébergement partagé dans le cadre de la procédure pénale numérique.

### *b. Un hébergement majoritairement interne pour les ministères dotés d'infrastructures historiques*

L'hébergement interne est également très majoritaire parmi les grands ministères, qui disposent d'un parc historique de data centers et ont engagé le développement de leur propre cloud interne pour demeurer autonomes.

Le ministère de la transition écologique privilégie ainsi une stratégie d'hébergement interne selon une « *logique de souveraineté et de sécurité* » comme développé dans ses réponses écrites : « *Les serveurs hébergeant les systèmes*

*d'information et les données correspondant aux outils bureautiques et collaboratifs sont pour l'essentiel situés dans les salles serveurs du ministère, sur des machines " on prem " ou sur le cloud ministériel, avec un débord limité chez un hébergeur SecNumCloud ou chez IMT pour certaines briques. En utilisant ses propres serveurs pour l'essentiel des services et en imposant des niveaux élevés d'authentification, le ministère limite les surcoûts d'infrastructure et réduit sa dépendance à des infrastructures externes*. » Environ 70 % du parc applicatif ministériel est ainsi hébergé sur son cloud souverain Eco, basé sur des logiciels open source, en particulier la suite Openstack. Les applications les plus anciennes qui n'ont pas pu être migrées sur le cloud restent dépendantes de la solution de virtualisation VMWare et de technologies de stockage américaines, notamment NetApp.

Le ministère de l'éducation nationale a mis en place, en 2018, la plateforme Cloé, hébergée dans le centre informatique des douanes en région parisienne et maintenue par une équipe interne du ministère, avec l'objectif d'accueillir les 160 applications nationales du ministère. La direction du numérique pour l'éducation indique ainsi que le ministère « *héberge très essentiellement ses applications en interne (*on premise*) dans des data centers interministériels ou au sein d'hébergements dédiés privatifs. Par exception, lorsque les applications traitent des données dont la sensibilité l'autorise et que le cloud apporte des avantages singuliers, le ministère opère des hébergements dans le cloud commercial via le marché cloud cercle 3* ». L'hébergement des sites web institutionnels de l'administration centrale et des services déconcentrés, ainsi que celui des systèmes d'information du domaine jeunesse et sports – au total, 150 services numériques – sont cependant externalisés auprès d'un acteur français.

Le ministère de l'agriculture et de la souveraineté alimentaire dispose également de sa propre plateforme d'hébergement, reposant sur des infrastructures situées en Haute-Garonne.

#### *c. Un recours plus fréquent aux offres de cloud commercial parmi les ministères les plus faiblement dotés*

Les ministères dotés de moyens plus faibles ne sont pas en mesure d'assurer l'hébergement en interne de leurs systèmes d'information et sont donc plus enclins à se tourner vers les offres de cloud commercial.

Le service du numérique du ministère de la culture explique ainsi, dans ses réponses écrites, privilégier le mode « logiciel à la demande », avec un hébergement dans le cloud auprès d'offres commerciales. Lorsque des données sensibles doivent être manipulées, les applications sont hébergées soit sur les infrastructures du ministère, soit sur le cloud interministériel Nubo, comme c'est le cas pour les documents nativement numériques des Archives nationales.

Selon la même logique, les ministères sociaux ont basculé leurs systèmes d'information vers le cloud, en ayant systématiquement recours aux offres commerciales pour les nouveaux projets ou les refontes significatives. Ils continuent

d'héberger une partie de leur système d'information dans des centres techniques informatiques ministériels et en délèguent la gestion à des infogérances effectuées par la société Orange Business pour un coût d'environ 15 millions d'euros par an, tout en externalisant l'hébergement des données de santé au prestataire français Cegedim.

Il faut également relever les stratégies divergentes des caisses de sécurité sociale placées sous la tutelle du ministère. Alors que la Cnam assure l'hébergement et l'exploitation de ses applications cœur de métier et de ses téléservices en interne sur ses quatre data centers, dont deux certifiés « Hébergeur de données de santé » (HDS), **la Cnaf a externalisé l'exploitation de certains composants chez des opérateurs américains, notamment Oracle et Microsoft Azure, pour des montants très significatifs : 15 millions d'euros pour l'année 2025.**

#### *d. Une externalisation globalement limitée parmi les opérateurs de l'État et les services déconcentrés*

La Dinum relevait, dans son bilan de décembre 2025 de la doctrine Cloud au centre, que le déploiement du cloud demeurait faible parmi les opérateurs de l'État. Seuls 14 % d'entre eux ont effectué une commande sur le marché cloud de l'Ugap en 2024. Cette situation s'expliquerait notamment par des raisons comptables et budgétaires : la migration obligerait les opérateurs à convertir des dépenses d'investissements – les achats de serveurs –, en coûts d'abonnement à des services informatiques, qui s'assimilent à des dépenses de fonctionnement, alors que l'architecture budgétaire empêche toute fongibilité entre ces deux catégories de dépenses. Les opérateurs sont donc incités à conserver leurs propres data centers.

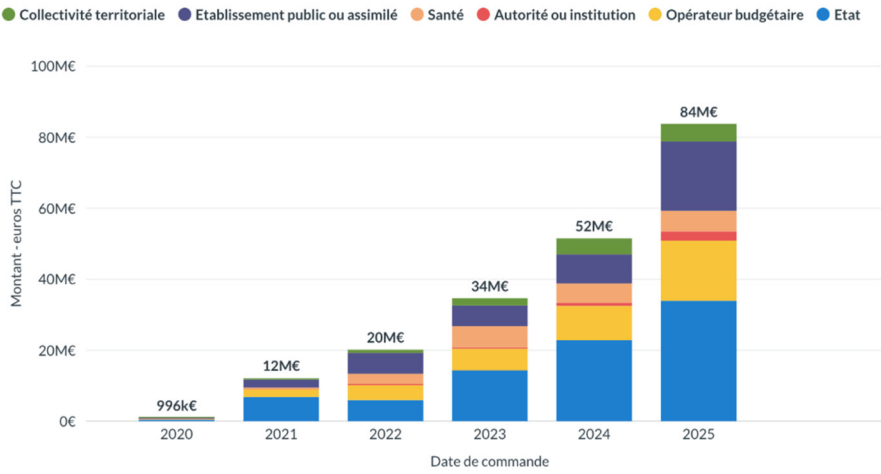
Dans le domaine de la recherche, les opérateurs sont très vigilants sur la protection de leurs données, comme l'a montré l'audition des directeurs des systèmes d'information des instituts de recherche par la commission d'enquête. L'Institut national de la santé et de la recherche médicale (Inserm) et l'Institut national de recherche pour l'agriculture, l'alimentation et l'environnement (Inrae) s'appuient sur des centres de données régionaux labellisés par le ministère de l'enseignement supérieur et de la recherche, et généralement opérés par des universités, au sein desquels ils ont installé leurs propres capacités de stockage et de calcul. Concernant le CEA, M. Baptiste Grigy a déclaré : « *le CEA a un système d'information qui est à 99 % sur site* (on premise*). Notre informatique est localisée dans nos propres centres de données, répartis et redondés sur différents sites, et il existe une culture très forte de l'usage d'outils et de services locaux* ».

### 3. 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, comme le montrent les chiffres des achats de services d'hébergement externes. 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 à 84 millions d'euros.

**CONSOMMATION DE CLOUD COMMERCIAL**
**PAR AN ET PAR TYPE D'ADMINISTRATION PUBLIQUE**




*Source : Dinum, février 2026.*

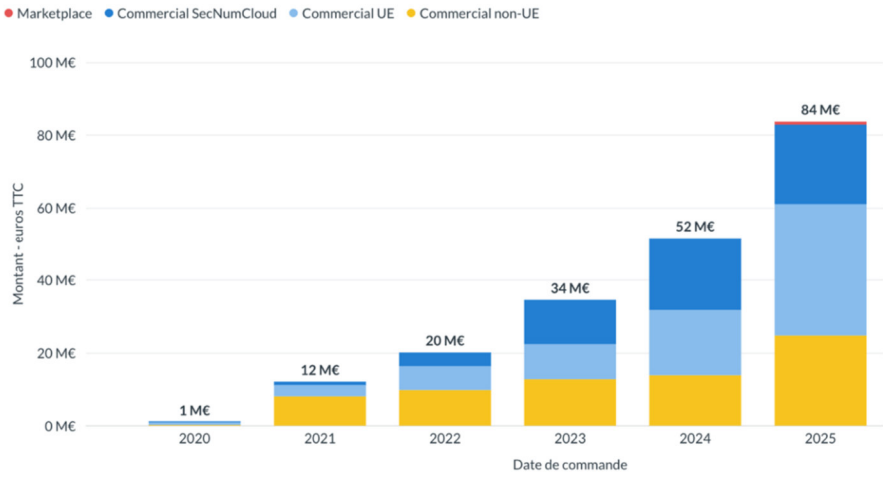
**La mise en œuvre de la doctrine a produit de réels effets sur la nationalité des fournisseurs sélectionnés ainsi que sur le recours à des offres labellisées SecNumCloud.**

### *a. Un hébergement des données majoritairement assuré par des prestataires européens*

Lors de son audition par la commission d'enquête, la directrice interministérielle du numérique a fait valoir qu'en 2025, **sur le périmètre strict des administrations centrales, « *99 % de la commande publique de l'État est orientée vers des acteurs européens, essentiellement français* »**.

**La part de fournisseurs européens descend à 89 % lorsqu'on étend le champ aux opérateurs de l'État, et elle n'est plus que de 70 % sur l'ensemble du marché de l'Ugap.** Le niveau de dépendance à des prestataires étrangers reste cependant bien plus maîtrisé que celui constaté sur le marché multi-éditeurs de l'Ugap.

**RÉPARTITION PAR AN DE LA COMMANDE DE SERVICES CLOUD SUR LE MARCHÉ DE L'UGAP EN FONCTION DE LA CATÉGORIE DE FOURNISSEUR (TOUTES ADMINISTRATIONS CONFONDUES)**




*Source : Dinum, février 2026.*

En parallèle, les *hyperscalers* perdent des parts de marché de l'Ugap : alors qu'ils captaient 45 % de la commande en 2022, ils n'en reçoivent plus que 25 % en 2025. La Dinum relevait dans son bilan de décembre 2025 que « *les acteurs extra-européens investissent d'ailleurs peu dans le marché Ugap (baisse des remises octroyées, priorité mise sur les collectivités ou les établissements publics qui n'ont pas l'obligation de recourir au marché Ugap)* ». Les dépenses adressées aux *hyperscalers* continuent cependant de croître en valeur pour atteindre 21,7 millions d'euros en 2025, contre 12,9 millions en 2024. Elles sont tirées vers le haut par une unique commande pluriannuelle de 7 millions passée auprès d'AWS par un groupement d'intérêt économique.

**RÉPARTITION DE LA COMMANDE DE SERVICES CLOUD SUR LE MARCHÉ DE L'UGAP EN FONCTION DES FOURNISSEURS**

| Fournisseurs | Montant 2025 (€ TTC) | Montant 2024 (€ TTC) | Montant 2023 (€ TTC) | Croissance montant 2025 | Croissance montant 2024 | Entités clientes 2025 | Entités clientes 2024 | Entités clientes 2023 | Croissance clients 2025 | Croissance clients 2024 |
|---|---|---|---|---|---|---|---|---|---|---|
| OVH | 30 188 241 | 23 398 682 | 11 930 055 | 29% | 96% | 173 | 125 | 88 | 38% | 42% |
| AWS | 11 063 684 | 2 521 894 | 2 879 082 | 339% | -12% | 27 | 23 | 21 | 17% | 10% |
| Outscale | 9 842 714 | 4 456 937 | 4 311 474 | 121% | 3% | 46 | 39 | 28 | 18% | 39% |
| Microsoft | 8 647 561 | 9 275 789 | 7 644 970 | -7% | 21% | 106 | 84 | 59 | 26% | 42% |
| Scaleway | 6 673 104 | 4 303 666 | 2 459 123 | 55% | 75% | 59 | 41 | 30 | 44% | 37% |
| Cegedim | 4 137 525 | 260 823 | 14 409 | 1486% | 1710% | 9 | 5 | 1 | 80% | 400% |
| Cloud Temple | 3 229 099 | 2 848 330 | 1 960 160 | 13% | 45% | 12 | 10 | 10 | 20% | 0% |
| Oracle | 2 158 683 | 982 534 | 1 353 795 | 120% | -27% | 17 | 14 | 16 | 21% | -13% |
| Scalingo | 2 051 331 | 1 756 692 | 797 878 | 17% | 120% | 21 | 14 | 7 | 50% | 100% |
| GCP | 1 979 484 | 1 035 772 | 860 991 | 91% | 20% | 24 | 14 | 15 | 71% | -7% |
| Kyndryl | 1 649 021 | | | | | 1 | - | - | | |
| Numspot | 688 668 | | | | | 3 | - | - | | |
| Upsun | 492 705 | 435 061 | 208 611 | 13% | 109% | 9 | 7 | 3 | 29% | 133% |
| Ecritel | 475 323 | | | | | 5 | - | - | | |
| Clever Cloud | 336 538 | 168 529 | 13 956 | 100% | 1108% | 13 | 5 | 3 | 160% | 67% |
| S3NS | 72 751 | | | | | 5 | - | - | | |
| Orange | 8 822 | 127 852 | 60 446 | -93% | 112% | 1 | 3 | 2 | -67% | 50% |

*Source : Dinum, février 2026.*

**Ces chiffres n'offrent cependant qu'une vision partielle des données publiques hébergées sur des offres commerciales**. Ils ne permettent pas d'appréhender les commandes qui ne reposent pas sur le marché interministériel de l'Ugap mais sur d'autres centrales d'achat – Resah, Canut ou Sipperec – ou qui sont passées directement par l'administration auprès d'un prestataire de services. De même, **les achats de logiciels en mode SaaS, qui incluent un hébergement en nuage, ne sont pas retracés**.

**Le périmètre des SI de l'État à surveiller comporte également des angles morts, dans la mesure où les choix en matière de numérique des établissements de santé et des universités ne sont pas centralisés**. La Dinum relève ainsi que les établissements publics de santé ou ceux relevant de l'enseignement supérieur et de la recherche (ESR) échappent aux efforts de mutualisation : « *les premiers n'étaient pas dans le champ d'application de la circulaire dans l'esprit de ses rédacteurs, qui n'ont pas prévu de cible d'hébergement adaptée à leurs contraintes* » tandis que « *les établissements de la sphère ESR estiment que les choix d'infrastructure leur appartiennent du fait de leur indépendance statutaire* ».

**Certains opérateurs continuent cependant de dépendre très largement de solutions extra-européennes.** C'est notamment le cas de **France Travail, dont 83 % des dépenses de services cloud de l'année 2025 étaient concentrées sur trois fournisseurs américains : essentiellement ServiceNow, mais également AWS et Microsoft Azure**. Une partie des données concernées sont à caractère personnel, mais France Travail estime qu'elles n'entrent pas dans le champ d'application de l'article 31 de la loi Sren. Les hébergeurs américains représentent également près de 98 % des dépenses de cloud de la Cnaf.

***b. Un recours croissant aux offres certifiées SecNumCloud***

**En 2025, les offreurs qualifiés SecNumCloud ont représenté 49,7 % des commandes passées par les administrations centrales sur le marché Nuage public**. Si la plupart des ministères ne recourent aux offres commerciales que pour héberger leurs données non sensibles, les auditions et les questionnaires écrits ont mis en lumière des stratégies différentes en matière de sélection du fournisseur.

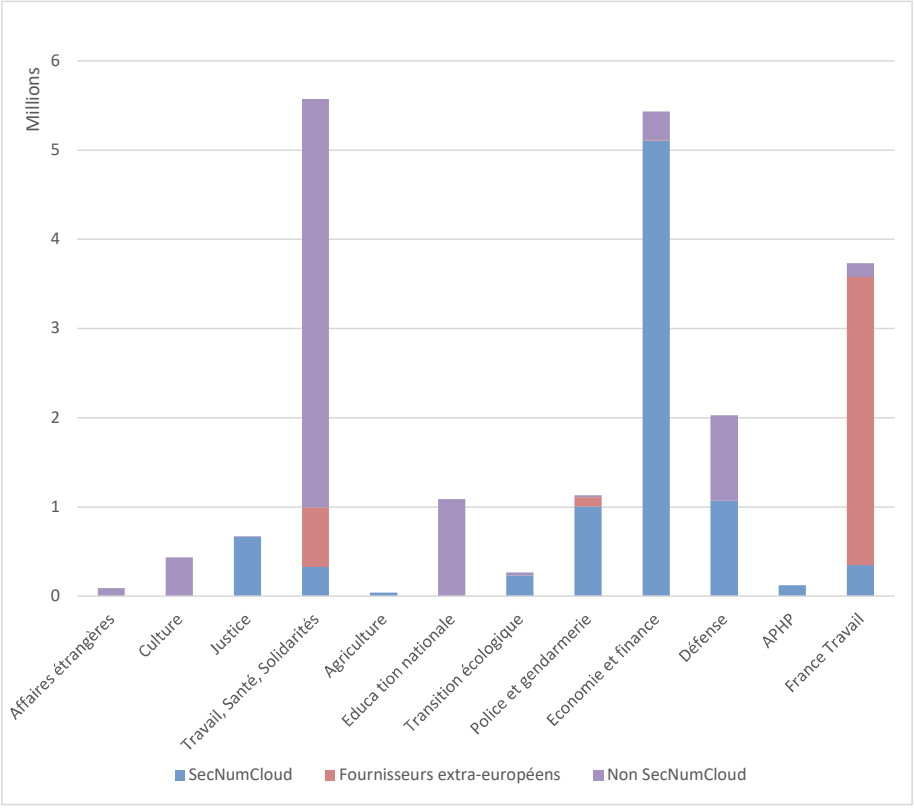
**Certaines administrations se tournent exclusivement vers des solutions SecNumCloud, même lorsqu'elles n'en ont pas l'obligation juridique** car les données ne sont pas d'une sensibilité particulière au sens de la loi Sren. C'est notamment le cas du ministère de la justice, du ministère de l'agriculture ou de la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF), qui ne retiennent que des prestataires SecNumCloud pour héberger des données parfois personnelles mais non sensibles.

**D'autres ministères, au contraire, tirent parti de la non sensibilité des données pour recourir à des offres moins sécurisées et donc moins onéreuses**. Le ministère de l'éducation nationale n'utilise ainsi que des solutions non-

SecNumCloud, quoique françaises, pour héberger entre autres le produit Webinaire ou la plateforme Moodle. La direction du numérique des ministères sociaux indique exiger une qualification HDS pour héberger des données de santé, et une qualification SecNumCloud pour les données d'une sensibilité particulière, mais recourir « *dans tous les autres cas, pour des raisons d'optimisation des coûts, à des offres dites de* Public Cloud *ou de* Private cloud ». De fait, les commandes SecNumCloud représentent moins de 20 % des 6 millions d'euros de dépenses cloud renseignées par les ministères sociaux pour l'année 2024.

L'obligation de recourir à un prestataire SecNumCloud a constitué un levier de réorientation de la commande publique vers des fournisseurs français, comme l'ont salué les acteurs industriels auditionnés par la commission d'enquête. M. Philippe Miltin, directeur général d'Outscale Dassault Systèmes, a déclaré « *qu'elle a joué un rôle important dans l'orientation de l'achat public vers des offres de marché souveraines* ». M. Octave Klaba, président-directeur général d'OVHcloud considère également que « *la commande publique a évolué positivement, surtout ces trois dernières années, grâce notamment à SecNumCloud* ».

**DÉPENSES ANNUELLES MOYENNES DE CLOUD COMMERCIAL ENTRE 2023 ET 2025 PAR CATÉGORIE DE FOURNISSEUR**




*Source : Assemblée nationale à partir des réponses transmises par les ministères et les organismes publics.*

### 4. Plusieurs situations de vulnérabilité identifiées

Les réponses aux questionnaires font cependant apparaître **plusieurs cas d'hébergement de données personnelles ou sensibles sur des solutions extra-européennes, pour certains en contradiction avec l'article 31 de la loi Sren**. Les cas emblématiques en sont la Plateforme des données de santé, qui a fait le choix d'un hébergement sur Microsoft Azure – le sujet sera traité au chapitre 8 – et certaines suites collaboratives telles qu'Office 365 de Microsoft.

**SITUATION D'HÉBERGEMENT DE DONNÉES AUPRÈS DE FOURNISSEURS EXTRA-EUROPÉENS IDENTIFIÉES PAR LA COMMISSION D'ENQUÊTE**

| Administration | Fournisseur (pays d'origine) | Données à caractère personnel | Données d'une sensibilité particulière | Données dont la violation est susceptible d'engendrer une atteinte à l'ordre publique, à la sécurité publique, à la vie des personnes ou à la protection de la propriété intellectuelle |
|---|---|---|---|---|
| **Ministères sociaux** | Microsoft (US) | x | x | |
| | Microsoft (US) | x | | |
| | Google (US) | x | | |
| | Microsoft (US) pour hébergement SaaS d'Office 365 | x | x | x |
| **DGPN et DGGN** | Google (US) | | | |
| | Salesforce (US) pour hébergement SaaS du téléservice relation usager | x | | |
| **Justice** | Microsoft (US) pour hébergement SaaS d'Office 365 | x | x | x |
| **Culture** | Microsoft (US) pour hébergement SaaS d'Office 365 | x | x | x |
| **Éducation nationale** | Salesforces (US) pour l'hébergement de Virtuo | | | |
| **Insee** | AWS (US) | | | |
| | Google (US) | | | |
| **DGFIP** | Google (US) | x | | |
| **Cnaf** | Oracle (US) | x | x | x |
| | Microsoft (US) | x | x | |
| | Microsoft (US) pour hébergemennt SaaS d'Office 365 | x | x | x |
| **France Travail** | ServiceNow (US) | x | x | |
| | AWS (US) | | | |
| | Microsoft (US) | | | |
| | Kyndril (US) | | | |
| | Microsoft (US) pour hébergement SaaS d'Office 365 | x | x | x |

*Source : Réponses écrites.*

La diffusion des **logiciels en mode SaaS (*Software as a service)*,** hébergés sur le cloud et fournis à la demande, a de fait complexifié la préservation de la maîtrise des systèmes d'information. Pour les administrations qui privilégiaient l'hébergement *on premise* de leurs applications, comme en attestent les ministères économiques et financiers, « *l'émergence d'une offre logicielle en mode SaaS a obligé à ajuster la stratégie (...), l'hébergement internalisé d'une offre logicielle n'étant pas systématiquement proposé par l'éditeur* ». M. Audran Le Baron, directeur du numérique pour l'éducation, a confirmé cette bascule tout en regrettant l'absence de solutions apportant les garanties de sécurité nécessaires : « *La transition vers les redevances annuelles s'explique aussi par la difficulté croissante que nous éprouvons à héberger les éditeurs en interne,* on premise*. Aller vers le SaaS (*software as a service*) est une facilité collective, ce qui nous amène à la réflexion sur le SecNumCloud : l'éditeur est-il prêt à nous soumettre une offre suffisamment souveraine et sécurisée, eu égard aux enjeux auxquels nous faisons face ?* » (1)

De fait, en février 2026, seuls trois fournisseurs d'offres de type SaaS avaient été qualifiés SecNumCloud : Oodrive, Whaller et Index Education. Les sociétés américaines sont encore très dominantes sur ce segment.

### *a. Office 365*

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**, justifiée par l'absence d'une alternative souveraine opérationnelle.

Les autres administrations utilisatrices de Microsoft ont pourtant toutes privilégié une installation en local. Le directeur du numérique pour l'éducation a ainsi précisé lors de son audition que le ministère de l'éducation nationale, bien qu'ayant doté les agents administratifs de la suite Office, n'utilisait pas les services cloud de Microsoft, mais uniquement la suite bureautique installée sur les postes : « *Toute la collaboration a lieu sur les outils que j'ai cités précédemment, des outils libres et hébergés soit dans nos data centers interministériels, soit dans des clouds souverains* ». Le basculement obligatoire vers le cloud, imposé par certains *hyperscalers,* a même pu constituer un accélérateur de projets de migration vers des solutions libres, comme pour le CNRS avec Sharepoint : « *Microsoft nous pousse vers le cloud à partir de 2029, ce qui est orthogonal avec les injonctions de souveraineté* », a expliqué Mme Marie-Pierre Fontanel, directrice des systèmes d'information. « *Nous avons donc décidé de sortir à terme de cette dépendance en utilisant soit des outils que nous proposons en interne, soit ceux de la Dinum* ». (2)

---

*(1) Audition de M. Audran Le Baron, directeur du numérique pour l'éducation au ministère de l'éducation nationale, le 9 avril 2026.*

*(2) Audition de Mme Marie-Pierre Fontanel, directrice des systèmes d'information du CNRS, le 1er avril 2026.*

Le maintien d'un hébergement sur site suppose d'être en mesure d'assumer la charge de développement et le coût supplémentaire qu'il peut induire. M. Damien Rousset, directeur général délégué à l'administration de l'Inserm, en a témoigné devant la commission d'enquête : « *Pour la gestion de nos courriels, nous nous appuyons sur l'application Microsoft Exchange. Alors que cette solution s'accompagne d'une offre d'hébergement sur le cloud Azure, nous avons choisi de faire héberger ces données en France. Ce choix a un coût supplémentaire, qui double presque la facture, mais nous l'avons assumé.* » (1) M. Yves Billon, chef du service du numérique des ministères économiques et financiers, attestait pour sa part des difficultés à se passer des services du cloud de Microsoft en termes de performance et d'expérience utilisateur : « *On peut faire de la bureautique avec LibreOffice, mais on ne bénéficie pas de l'expérience utilisateur d'Office 365, de l'expérience cloud – il a fallu reconstruire beaucoup de choses derrière. On y a beaucoup perdu sur le plan fonctionnel ; les utilisateurs l'ont ressenti* ». (2)

Les ministères concernés travaillent à un plan de sortie d'Office 365. La direction du numérique des ministères sociaux a conduit une étude, à l'été 2025, explorant deux alternatives : la solution Bleu, opérée par Capgemini et Orange sur la base de technologies Microsoft, qui vise une certification SecNumCloud en 2026, permettrait une forte continuité des usages tout en maintenant la dépendance technologique à Microsoft ; ou La Suite, portée par la Dinum.

#### *b. Des applications métiers critiques hébergées par des prestataires américains*

Les administrations sont également dépendantes de solutions SaaS extra-européennes pour certaines de leurs applications métiers qui n'auraient pas d'équivalent au niveau européen.

**Au ministère de l'éducation nationale, le projet Virtuo de gestion RH qualitative couvrant le recrutement, la formation, l'évaluation des agents et la gestion des compétences, repose sur la solution SaaS de l'éditeur américain Salesforce**, qui a été sélectionné pour ses « *qualités fonctionnelles exclusives sur le marché »* selon la direction du numérique pour l'éducation.

Le premier appel d'offres, lancé au début de l'année 2021, avait été déclaré sans suite pour motif d'intérêt général après la parution de la circulaire du Premier ministre du 5 juillet 2021 établissant la doctrine Cloud au centre. Le projet Virtuo ayant vocation à traiter les données personnelles des agents du ministère de l'éducation nationale, il devait se conformer à l'obligation d'un hébergement sur un cloud de confiance, qui dispose de la certification SecNumCloud ou d'une qualification européenne de niveau équivalent. Parmi les deux offres reçues, la seule qui disposait de la qualification SecNumCloud a été rejetée sans être analysée, au motif qu'elle dépassait le montant du marché.

---

*(1) Audition de M. Damien Rousset, directeur général délégué à l'administration de l'Inserm, le 1er avril 2026.*

*(2) Audition de M. Yves Billon, chef du service du numérique au secrétariat général des ministères économiques et financiers, le 9 avril 2026.*

La Cour des comptes relevait ainsi que « *le ministère a choisi de privilégier l'amélioration de la performance de sa gestion des ressources humaines au respect des règles de souveraineté, dont le risque pouvait paraître moins tangible* » (1). **Salesforce** a notamment reconnu, dans une réponse à une demande de précision du ministère, qu'il pouvait faire l'objet de demandes d'accès aux données des clients de la part d'autorités étrangères. La Cnil et l'Anssi ont rendu un avis négatif, considérant que la protection à l'égard des lois extraterritoriales était insuffisante. M. Audran Le Baron observait cependant, lors de son audition, que des mesures de sécurité avaient été mises en place : « *afin de minimiser le nombre de données personnelles traitées par l'éditeur, un important travail de filtrage et de cisèlement a été mené pour déterminer qu'elles pouvaient ou non être stockées sur le cloud de l'éditeur, ou y transiter de manière transitoire avant d'être effacées une fois traitées* ». Ce choix a cependant dû être régularisé *a posteriori* par l'actualisation de la doctrine Cloud au centre de 2023. Le ministère a alors 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, et qu'elles n'ont donc pas à être hébergées chez un prestataire SecNumCloud.

**La police nationale et la gendarmerie nationale hébergent leurs plateformes d'aide aux victimes sur les plateformes non SecNumCloud, portées respectivement par Easiware et l'éditeur américain Salesforce,** en l'absence d'offres équivalentes identifiées. L'Anfsi a fait part à la rapporteure de l'objectif d'évoluer vers une plateforme commune hébergeable en SecNumCloud.

**La rapporteure a pris connaissance d'autres cas de non-conformité à l'article 31 de la loi Sren, mais sans risque de soumission à des lois extraterritoriales dans la mesure où l'hébergeur est français**. L'AIFE héberge la plateforme pour les achats de l'État, Place, chez un hébergeur français mais non qualifié SecNumCloud, alors que les données traitées entrent dans le champ de l'obligation. Les ministères économiques et financiers ont justifié ce choix dans leur réponse écrite à la rapporteure, tout en annonçant un plan de sortie à court terme : « *L'application est relativement ancienne (2012) et lorsque l'AIFE l'a basculée dans le Cloud en 2019, les solutions SecNumCloud de l'époque auraient nécessité une refonte conséquente de l'application, c'est pourquoi l'AIFE a choisi le Private Cloud d'OVH. Les solutions SecNumCloud s'étant enrichies depuis, l'AIFE va lancer une étude pour migrer Place sur une architecture SNC, avec un objectif de bascule à mi-2027*. »

Le ministère de la transition écologique recourt également à un cloud commercial privé qui ne bénéficie pas de la qualification SecNumCloud pour héberger l'application SIAO qui traite des demandes d'hébergement d'urgence.

---

*(1) Cour des comptes, « Les enjeux de souveraineté des systèmes d'information civils de l'État », septembre 2025.*

**Non soumise à la loi Sren, la Cnaf héberge quelques composants de ses applications métiers chez Oracle et Microsoft Azure, bien qu'elles traitent de données d'une sensibilité particulière**. La Cnaf a expliqué, dans ses réponses écrites, avoir fait « *le choix de la solution Oracle en 2016 pour moderniser son dispositif informatique de représentation des règles de calcul des droits allocataires dans le cadre de la réforme réglementaire PPA/RSA et pour l'allocation logement. Ce faisant, le choix a également été fait de déporter l'hébergement associé sur le cloud Oracle. À cette date, la qualification SecNumCloud venait d'être créée et il n'existait pas d'offre commerciale qualifiée.* » Elle dit également avoir retenu, en 2021, le cloud Azure « *afin de moderniser son SI décisionnel et se désengager de la solution SAS* ». La Cnaf s'est cependant fixé l'objectif d'une « *réduction drastique de [ses] dépendance vis-à-vis des fournisseurs non européens* » et travaille à court terme sur la réversibilité des services consommés dans le cloud Oracle. Elle a ainsi retenu le langage Catala de l'Institut national de recherche en sciences et technologies du numérique (Inria) pour permettre une migration OIA d'Oracle vers Catala, et envisage des hébergements chez OVH.

### D. INTELLIGENCE ARTIFICIELLE : LE DÉBUT DE NOUVELLES DÉPENDANCES

Avec le déploiement naissant des outils d'intelligence artificielle pour les agents publics, le risque de développer de nouvelles dépendances est important.

L'une des explications à ce phénomène est la mise à disposition de solutions en mode SaaS, en raison du besoin de disposer d'un outil offrant à la fois les modèles et des capacités de calcul. Les ministères régaliens semblent privilégier des solutions à façon, développées à partir de modèles d'IA open source ou propriétaires, notamment celles du français Mistral AI, et hébergées par des acteurs français. Cependant, les travaux de la commission d'enquête ont mis en évidence des cas d'usage **du modèle Claude d'Anthropic, de Copilot de Microsoft, de Gemini de Google ou de GPT d'OpenAI** au sein de plusieurs ministères, des caisses de sécurité sociale, de l'AP-HP et de France Travail. Ces différents modèles sont, pour beaucoup, portés par les *hyperscalers* Microsoft, AWS ou Google. Le ministère de la transition écologique, qui a construit un portail permettant d'accéder à différents modèles d'IA génératives (PIAG), recommande néanmoins aux agents de privilégier Mistral, opéré en SecNumCloud, lorsqu'ils ont à traiter de données sensibles.

**DÉPLOIEMENT DE L'IA GÉNÉRATIVE DANS LES ADMINISTRATIONS CONSULTÉES**

| | |
|---|---|
| **Affaires sociales** | Les ministères disposent du système d'IA Copilot dans le cadre de leur contrat avec Microsoft et détiennent quelques licences pour le modèle Claude d'Anthropic, quoique dans une bien plus faible mesure. Ils ont également recours à la plateforme Albert API de la Dinum. |
| **Transition écologique** | Le ministère a construit, pour près d'un million d'euros, le portail des IA génératives (PIAG) qui donne accès à plusieurs modèles d'IA génératives adaptés à différentes tâches et plusieurs niveaux de sensibilité des données : le modèle Mistral, hébergé sur l'offre SecNumCloud d'Outscale ; GPT sur Microsoft Azure ; Claude sur AWS ; et Perplexity. L'utilisation de Mistral représente plus de 90 % des dépenses totales de licences. |
| **Agriculture** | Le ministère a accès au portail des IA génératives (PIAG) du ministère de la transition écologique. |
| **Ministères économiques et financiers (MEF)** | Les ministères économiques et financiers ont déployé les modèles LLM de Mistral, mais indiquent également disposer de quelques licences pour Claude. Le principal contrat de l'AIFE porte sur la solution SSAI, qui repose sur le modèle Watson et les services de cloud d'IBM, en partenariat avec SopraSteria. |
| **Intérieur** | Le ministère a développé une plateforme d'IA générative souveraine, MIRAI, qui est hébergée en France et a vocation à migrer vers le cloud Pi ou une offre SecNumCloud pour les usages métiers sensibles. Il dénombre 120 initiatives en matière d'IA, regroupant des usages très divers, dont 18 % s'appuient sur des solutions développées par des tiers, dont très majoritairement des entreprises françaises. |
| **DGFIP** | La DGFIP a déployé des modèles de langages libres dans ses data centers, reposant sur ses propres GPU, afin d'assurer la sécurité des données et des traitements. |
| **Culture** | Après l'expérimentation de différents outils d'IA en 2025, le ministère a choisi de n'utiliser que l'assistant IA de la Dinum en 2026 (500 accès). |
| **Éducation nationale** | Le ministère vise l'ouverture de 100 000 accès à l'assistant IA de la Dinum et à la plateforme Albert API en juin 2026.<br>Sur le volet pédagogique, le ministère a déployé avec le fournisseur Docaposte l'outil M.I.A Seconde de remédiation en français et mathématique qui doit bénéficier à 800 000 élèves. Il a également conclu un partenariat d'innovation intelligence artificielle (P2IA) avec l'entreprise Lalilo pour développer des algorithmes d'apprentissage de la lecture, destiné à 40 000 enseignants et 400 000 élèves.<br>Certaines régions académiques ont mis en place des systèmes d'IA générative développés en interne ou souscrits auprès de fournisseurs français, pour des coûts qui demeurent modestes. |
| **Gendarmerie nationale et police nationale** | L'Anfsi a développé en interne un modèle de langage appelé l'Agent à partir de la solution propriétaire Yolo v7, hébergé dans les data centers de la gendarmerie nationale pour garantir la confidentialité des données. Ce projet, qui a débuté en 2019, a représenté 4 millions d'euros de dépenses de développement et d'intégration, et 700 000 euros de dépenses de licences et de MCO en 2025. L'Anfsi prépare une migration vers la plateforme d'IA GéniAI du ministère des armées qui repose sur des modèles open source. |
| **Justice** | Le ministère a déployé son outil interne d'IA générative, baptisé « Mon assistant Justice », dérivé de l'assistant IA de la Dinum. Il compte 90 000 utilisateurs. En parallèle, l'incubateur de la justice construit « Mon assistant pénal » et « Mon assistant civil », avec l'appui de la Dinum, pour faciliter et accélérer le traitement des procédures. Il est prévu de recourir à un hébergement souverain. |
| **MEAE** | Le ministère a développé son outil d'IA générative interne, DiploIA, pour des fonctions de transcription audio et vidéo, de traduction et de synthèse, avec un hébergement souverain. Le projet a été réalisé en interne, avec l'appui de prestataires, pour un coût de développement et d'intégration de 839 000 euros. |
| **France Travail** | L'opérateur a conclu un contrat avec Mistral AI pour l'utilisation de ses modèles propriétaires. Il recourt également à des outils reposant sur des modèles américains (GPT, Claude, Gemini) et hébergés par des *hyperscalers* (Google, Microsoft Azure). Google est notamment impliqué dans l'outil de recrutement Aglae, fourni par GoJob, qui représentera des dépenses significatives en 2026. |
| **Cnav** | La Cnav a développé un assistant IA interne et un outil de transcription en faisant appel à des fournisseurs français. Elle expérimente également l'outil d'IA Copilot M365 de Microsoft. |
| **Cnam** | La Cnam développe sa plateforme d'IA générative Camelia à partir des modèles LLM de Mistral. |
| **Cnaf** | La Cnaf expérimente Copilot de Microsoft depuis 2025, et la solution de Mistral depuis 2026. |
| **AP-HP** | En dehors de quelques cas d'usage du modèle Claude Code d'Anthropic et Anysphere de Cursor Teams, l'AP-HP utilise un chatbot fondé sur des modèles open source et hébergé par OVHCloud. Ils disposent également de systèmes d'IA spécialisés sur des fonctions d'aide au diagnostic, fournis par des entreprises finlandaise et américaine. |

*Source : Réponses écrites.*

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.** C'est pour cette raison que l'Inserm a décidé de développer des outils LLM (*Large Language Model*) sur son infrastructure cloud interne, comme l'a expliqué M. Damien Rousset, directeur général délégué à l'administration : « *Nous ne souhaitions pas que nos chercheurs utilisent les services disponibles sur internet, car nous savons que les données qu'ils y soumettent nourrissent le modèle et peuvent devenir accessibles à d'autres.* » (1)

Dans la même logique, la DGFIP a fait le choix de modèles LLM en open source hébergés en interne, comme l'a expliqué le chef du service des systèmes d'information Tomasz Blanc : « *L'enjeu majeur, lors de chaque révolution technologique, est d'éviter de créer de nouvelles dépendances. L'intelligence artificielle en est l'exemple type : si l'apparition de ChatGPT a suscité un fort engouement, il faut garder le recul nécessaire pour comprendre que, sous l'angle de la souveraineté, le recours à un tel outil est exclu.*

« *À la DGFIP, nous appliquons à l'IA le modèle de maîtrise interne que j'ai exposé. Nous nous appuyons sur nos propres data scientists et ingénieurs pour exploiter des modèles de langage libres sur nos propres puces GPU, hébergées dans nos centres de données. Cette infrastructure garantit que les données ne sortent jamais de nos murs et offre la flexibilité nécessaire pour changer de modèle aisément. Cette plateforme centralisée alimente déjà plusieurs cas d'usage, dont le plus visible est le nouveau moteur de recherche du site impots.gouv.fr, qui utilise l'IA pour améliorer la pertinence des résultats.*

« *Je ne m'interdis pas, à l'avenir, d'intégrer des modèles de langage propriétaires tels que Mistral, à la condition impérative qu'ils soient suffisamment standardisés pour s'insérer dans notre architecture. Cela nous permettrait de bénéficier d'éventuels gains de performance tout en conservant la faculté de basculer à nouveau vers des modèles libres si la politique commerciale de l'éditeur ou les risques pour notre souveraineté l'exigeaient. Enfin, nous allons également étudier de près le modèle Génial du ministère des armées afin de déterminer s'il peut nous aider à accélérer nos propres travaux.* » (2)

La directrice interministérielle du numérique Stéphanie Schaer confirme qu'« *une capacité de calcul qui préserve la sécurité des données est essentielle pour le déploiement de l'IA au sein de l'État* ». **Pour prévenir les risques de déploiements non maîtrisés, la Dinum s'est ainsi attachée à identifier des solutions répondant aux besoins de la sphère publique**, en portant une attention particulière aux conditions d'hébergement : « *Dans le tableau répertoriant l'ensemble de ces solutions d'IA (…), une colonne précise si la solution est hébergeable en SecNumCloud. À l'époque où nous avons lancé l'appel, il y a un an, c'était le cas de très peu de solutions. Nous avions souhaité montrer la diversité des logiciels français qui existaient, stimulés*

*(1) Audition de M. Damien Rousset, directeur général délégué à l'administration de l'Inserm, le 1er avril 2026.*

*(2) Audition de M. Tomasz Blanc, chef du service des systèmes d'information de la DGFIP, le 7 mai 2026.*

*par la French Tech, mais aussi donner de la visibilité à la capacité d'hébergement en SecNum, qui est quelque chose de très important.* » (1)

Ce travail a permis la **construction d'un socle interministériel de l'IA générative, reposant sur des infrastructures de confiance et des modèles d'IA open source et français**. Ce socle s'articule en trois grandes couches :

– l'API Albert, une plateforme interministérielle qui permet aux administrations d'accéder à de nombreux modèles de langage, pour plus d'une centaine de cas d'usages, hébergés sur une infrastructure SecNumCloud ou sur le cloud interministériel Nubo ;

– la plateforme de données, qui permet d'agréger et de structurer des données, principalement issues de sources publiques, afin de les rendre exploitables pour l'entraînement de systèmes d'intelligence artificielle ;

– l'assistant IA, un outil généraliste à destination des agents, construit sur les modèles Mistral AI en environnement SecNumCloud, qui doit être déployé auprès de 10 000 agents publics en juin 2026.

L'enjeu qui se dresse devant les administrations est celui de déployer une infrastructure sécurisée et performante dans un temps suffisamment rapide. Tant que les fonctionnalités des outils souverains développés par l'État seront perçues comme en-deçà de celles des modèles fournis gratuitement par les acteurs américains, perdurera un **risque important de *shadow IA*, c'est-à-dire d'utilisation d'outils d'IA extérieurs dans le cadre professionnel**. L'enquête réalisée par le ministère de l'action et des comptes publics entre janvier et avril 2026 auprès de 1 867 agents montre que 89 % des personnes interrogées utilisent déjà l'IA dans leur travail. Si 85 % disent recourir aux outils fournis par leur employeur, **55 % reconnaissent également utiliser des agents conversationnels de manière informelle**. Il existe dès lors un risque de divulgation de données sensibles de façon non maîtrisée.

Le ministre de l'action et des comptes publics, M. David Amiel, a appelé à engager une « *course de vitesse* » avec les acteurs extra-européens pour ne pas constituer « *un nouveau front de dépendance* » : « *Dans ce domaine, nous devons raisonner en semaines, voire en jours car, en ce moment même, des usages clandestins se généralisent dans les administrations, certains agents utilisant des outils grand public, accessibles gratuitement ou presque, pour la simple raison qu'ils sont efficaces. Si nous ne proposons pas nous-mêmes des alternatives souveraines de qualité, nous perdrons la bataille avant même de l'avoir commencée.* » (2)

Le développement de l'IA doit s'accompagner d'une réflexion indispensable sur ses usages pertinents et d'une alerte sur les biais et les limites de ses modèles.

---

*(1) Audition de Mme Stéphanie Schaer, directrice interministérielle du numérique, le 14 avril 2026.*

*(2) Audition commune de M. David Amiel, ministre de l'action et des comptes publics, et de Mme Anne Le Hénanff, ministre déléguée auprès du ministre de l'économie, des finances et de la souveraineté industrielle, énergétique et numérique, chargée de l'intelligence artificielle et du numérique.*

## CHAPITRE 2 – LE RISQUE NUMÉRIQUE : ÉLARGISSEMENT DE L'ANALYSE AUX ENTREPRISES PUBLIQUES ET PRIVÉES

« *Les commandes publiques en matière de produits et de services numériques représentent ainsi quelque 4,3 milliards d'euros. C'est à peu près dix fois moins que les dépenses des grands groupes français – lesquelles approchent 47 milliards d'euros dans les entreprises du CAC40* » (1). Les administrations sont au cœur des services publics essentiels, mais ne constituent qu'une infime partie de la vie économique et sociale de notre pays. Après avoir étudié en détail les dépendances techniques des systèmes d'information de l'État, la commission d'enquête a souhaité élargir son analyse en procédant par cercles concentriques. Il s'agissait ainsi de comprendre les éventuels risques systémiques provenant des entreprises publiques, puis de l'ensemble du tissu économique français.

### A. LES ENTREPRISES PUBLIQUES : DES SYSTÈMES D'INFORMATION INDUSTRIELS SÉCURISÉS, L'UTILISATION CROISSANTE DU CLOUD PUBLIC

La commission d'enquête a souhaité élargir le périmètre de ses analyses aux entreprises publiques chargées de l'exploitation de services publics essentiels. Les analyses ci-après s'appuient sur les réponses aux questionnaires envoyés aux entreprises listées en annexe, couvrant des secteurs différents.

Les questionnaires portaient sur le parc applicatif des systèmes d'information des sociétés interrogées, dans une approche similaire à celle suivie pour les administrations d'État, avec une attention supplémentaire portée aux systèmes d'information industriels, du fait de la nature même de l'activité.

#### 1. Dispositifs d'évaluation des dépendances numériques et stratégies de réduction des vulnérabilités

De par leur culture et les dispositions applicables aux opérateurs d'importance vitale (OIV), les entreprises consultées mettent en œuvre des processus qui évaluent leurs fonctions critiques, identifient les risques structurels qui les menacent et élaborent des plans de continuité d'activité/plans de reprise d'activité (PCA/PRA). Le sujet de la cybersécurité a d'ores et déjà pleinement été intégré à ces analyses. Les réponses aux questionnaires font apparaître la prise en compte récente du risque numérique dans sa nouvelle dimension géopolitique ou lié à la vulnérabilité à des fournisseurs extra-européens.

Comme l'indique Aéroports de Paris (ADP) : « *nous avons élaboré une cartographie de nos dépendances. Elle repose actuellement sur un indicateur spécifique à ADP : l'ISVL, pour indice de sensibilité au* vendor lock-in*, et un nouvel indicateur standardisé appelé IRN (indice de résilience numérique), plus largement reconnu. Les processus clefs sont documentés, des plans de continuité de l'activité*

*(1) Audition commune de M. David Amiel et de Mme Anne Le Hénanff, le 20 mai 2026.*

*sont en place. Par exemple, en cas de destruction du SI, ils prévoient une capacité à opérer l'aéroport sans l'IT, à capacité réduite* ». S'agissant d'EDF, les processus clés et les services numériques associés ont déjà fait l'objet d'un recensement depuis de nombreuses années à EDF, et il existe un plan de continuité d'activité / plan de reprise d'activité, testé chaque année, destiné à pouvoir reconstruire les applications essentielles en cas de sinistre. En complément, le contexte géopolitique a amené l'entreprise à *« engager plus récemment des actions en vue de maîtriser trois risques spécifiques liés aux dépendances dans le domaine du numérique :*

« *– risque d'espionnage des données : une entité non autorisée par EDF accède à nos données en vertu d'une loi extraterritoriale de type Cloud Act ;*

« *– risque de chantage commercial : un fournisseur de service ou infrastructure numérique en situation de quasi-monopole à EDF augmente brusquement et drastiquement ses tarifs.*

« *– risque de chantage diplomatique : un gouvernement étranger impose à ses entreprises de cesser la fourniture de services à EDF ».*

Une feuille de route a été établie pour lutter contre les risques croissants de dépendance numérique. Elle s'articule autour de plusieurs axes : la diversification des fournisseurs, le renforcement du recours à l'open source ou la mise en place de standards d'architecture favorisant la réversibilité et la portabilité. EDF a ainsi créé un indice de portabilité multi cloud visant à mesurer la capacité d'une application à migrer facilement d'un cloud à un autre. EDF est également très actif au sein de l'écosystème numérique français et européen pour favoriser les initiatives qui permettent de réduire les dépendances vis-à-vis de technologies et d'infrastructures digitales développées ou opérées par des acteurs extra-européens, telles que le projet d'espace de données pour le nucléaire « Data4Nuclear-X ».

Pour Natran, opérateur du réseau de transport de gaz naturel, « *la stratégie mise en œuvre repose en premier lieu sur une identification systématique, au sein de la cartographie du SI, des dépendances existantes ou à venir susceptibles de générer un impact immédiat sur l'activité, en particulier les dépendances critiques de type " kill switch " (interruption de service délibérée, par exemple sur certains services externalisés comme la messagerie ou des briques d'infrastructure opérées par des tiers). Pour ces dépendances, deux approches sont privilégiées : la recherche d'alternatives, notamment européennes et échappant aux contraintes d'extraterritorialité, ou leur cloisonnement et leur déploiement en environnement maîtrisé (on-premise), afin de limiter les risques d'indisponibilité brutale* ».

Le groupe RATP a lancé une cartographie de ses dépendances à l'aide de l'indice de résilience numérique (IRN), qui intègre la dépendance financière, la cybersécurité, le risque d'indisponibilité des systèmes et de confidentialité des données. « *Méthodologiquement, l'analyse a pour objectif de confronter plusieurs critères qui mesurent factuellement l'indépendance du système d'information de*

*l'organisation, à trois différentes échelles (nationale, européenne, extra-européenne). Il s'agit de :*

« *– la part des dépenses et achats de logiciels, licences, maintenance, et matériels alloués à des fournisseurs nationaux, européens ou extra-européens ;*

« *– la géolocalisation nationale, européenne et extra-européenne du stockage des données ;*

« *– le degré d'" openness ", c'est-à-dire l'appui des systèmes numériques critiques sur des technologies ouvertes (open source, open data, standards ouverts…) ;*

« *– la diversification des fournisseurs du portefeuille SI ainsi que la capacité à migrer entre fournisseurs* ».

### 2. Des systèmes d'information industriels généralement fournis par des sociétés européennes et opérés sur des infrastructures dédiées

Une attention particulière a été portée aux dispositifs de conduite des outils industriels – Scada (système de contrôle et d'acquisition de données) au regard de leur criticité, tant dans le choix des outils que dans leur hébergement sur des infrastructures sécurisées, généralement des data centers propriété des opérateurs.

S'agissant d'EDF, « *les systèmes Scada relèvent du périmètre des systèmes industriels critiques. Ils sont sélectionnés sur des critères de sûreté, robustesse et pérennité. La continuité d'exploitation repose sur des architectures redondées, le cloisonnement des réseaux et des dispositifs adaptés de maintien en condition opérationnelle.*

« *Nous utilisons de très nombreux Scada dépendant des différentes business units et des différents outils de production (…). Ces dispositifs s'inscrivent dans une approche globale de défense en profondeur. Les architectures mises en œuvre intègrent des principes de cloisonnement strict et de maîtrise des flux entre systèmes, en cohérence avec les exigences applicables aux systèmes industriels critiques.*

« *Dans le domaine du nucléaire, la planification de la maintenance est réalisée via l'application GPS qui est basée [sur un progiciel d'une société française]. Le paramétrage, le développement et la maintenance de l'application sont réalisés par des sociétés externes, sous le contrôle et le pilotage de quatre acteurs internes* ».

Pour le pilotage du réseau électrique, Enedis a fait le choix d'un Scada développé par ses propres équipes : « *L'application repose sur des OS open-source (RedHat) et le système de virtualisation est en cours de migration vers Openstask ou Kubernetes. Un secteur géographique régional dispose d'un SCADA du marché, fourni par une société allemande et est amené à migrer à moyen terme vers la solution développée par Enedis* ».

Concernant Natran, le Scada actuellement déployé repose majoritairement sur une solution commerciale industrielle d'origine nord-américaine, historiquement choisie au regard de sa richesse fonctionnelle, de sa capacité de configuration fine aux besoins spécifiques de l'activité et de son coût d'acquisition initial compétitif. Ce système est exploité dans un environnement découplé des services externes, avec des mécanismes de cloisonnement strict qui permettent de limiter les risques d'indisponibilité liés à une défaillance fournisseur ou à une dépendance externe. Toutefois, ce système est désormais couplé aux infrastructures industrielles et aux équipements de terrain, ce qui rend son remplacement particulièrement complexe et structurant. Compte tenu de la dépendance structurelle à l'éditeur et du coût total de possession en intégrant les frais de maintien en condition opérationnelle, l'entreprise n'exclut pas, à un horizon de cinq à dix ans, d'étudier des scénarios de transformation ou de redéveloppement partiel ou complet de cette solution afin de renforcer sa maîtrise stratégique.

Concernant la RATP, les Scada s'appuient sur des solutions européennes, dont certaines françaises. En phase d'exploitation et de maintenance, l'entreprise est indépendante des fournisseurs puisqu'elle dispose des compétences en interne pour assurer la maintenance courante de premier niveau des équipements et systèmes de ses outils. Elle dispose en outre de contrats de maintien en conditions opérationnelles pour la maintenance courante de niveau supérieur (de type expertise) et les infrastructures sont *on premise* et isolées de l'extérieur.

Enfin, s'agissant de 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. La résilience s'appuie sur la redondance des environnements et des procédures de repli sur les versions précédentes en cas d'incident. Les outils de supervision industrielle et de contrôle-commande reposent sur des fournisseurs majoritairement européens. Les systèmes fonctionnent sur un réseau fermé dédié (Infranet) sans connexion internet, ce qui réduit structurellement le risque de désactivation à distance. Les plans de continuité incluent des procédures de repli manuel et la diversification des fournisseurs permet d'absorber la défaillance d'un titulaire sans rupture de service. À noter, SNCF Réseau a engagé l'acquisition des droits de propriété intellectuelle du logiciel Mistral, historiquement opéré par Atos, avec un objectif de maîtrise opérationnelle complète d'ici 2027.

### 3. Systèmes d'information tertiaires : les mêmes dépendances que dans l'administration

S'agissant du SI tertiaire, les mêmes dépendances sont relevées que dans les administrations d'État. La suite Microsoft Office 365 est déployée très largement chez l'ensemble des opérateurs, sans perspective concrète de basculement vers des solutions open source. Une migration ne pourrait être envisagée que dans le cadre d'un processus long de plusieurs années.

EDF a restreint le déploiement de solutions alternatives à la gestion des échanges les plus sensibles : « *pour nos données les plus sensibles (classification interne C3), nous utilisons des solutions françaises indépendantes pour les échanges et la collaboration (…). Pour nos données de faible confidentialité, nous utilisons les services bureautiques et de collaboration Microsoft (MS 365). Nous sommes en train d'expérimenter des solutions alternatives européennes.* »

Pour Enedis, « *Les échanges collaboratifs s'appuient massivement sur les solutions de l'éditeur Microsoft (Office 365)* ».

Les constats sur le déploiement de la solution Microsoft sont les mêmes pour les autres opérateurs interrogés.

Les dépendances aux logiciels VMWare et Oracle, pour lesquels le choix est sans impact pour les utilisateurs finaux, font en revanche l'objet de travaux concrets de transition vers des solutions open source comparables. Par exemple, chez Enedis, l'utilisation de la solution VMWare a été « *fortement diminuée à la suite du déploiement de l'Open Source Openstack sur une partie du parc (40 % à date). Nous avons l'objectif à l'horizon 2030 de sortir totalement de VMware »,* de même que celle d'Oracle *« à la suite du déploiement de l'Open Source Postgre sur la majorité de parc (plus de 67 % à date). Nous avons également l'objectif de sortir de la solution à l'horizon 2030* ».

ADP étudie également le remplacement de VMWare par OpenStack, une alternative open source, avec comme déclencheur la très forte augmentation de tarif subie après le rachat de VMWare par Broadcom.

### 4. L'utilisation préoccupante et systématique de clouds extra-européens

Les informations recueillies auprès des organismes sollicités font apparaître une utilisation systématique des *hyperscalers* pour une partie des applications, comme le montre le tableau ci-dessous.

**OPÉRATEURS DE CLOUD DES SIX ENTREPRISES PUBLIQUES INTERROGÉES**

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

*Source : Réponses écrites*

Les architectures mises en œuvre sont hybrides. Les opérateurs indiquent privilégier le *on premise* pour les informations sensibles ou non confidentielles. Ainsi que l'indique EDF, « *les données de nos applicatifs sont situées soit dans nos propres data centers, soit dans le cloud. Nous sommes propriétaires et exploitants de deux data centers en France (…). En ce qui concerne le cloud, nous nous*

*appuyons sur plusieurs contrats. Pour le cloud public, un contrat signé avec [un intermédiaire] nous donne accès au cloud de Amazon Web Services (AWS), un contrat avec Google Cloud Platform (GCP), ainsi qu'un contrat plus modeste avec Azure (Microsoft) destiné à des usages particuliers liés à la mise en œuvre des technologies Microsoft. L'utilisation des clouds publics est strictement encadrée et réservée aux données non confidentielles* ».

Chez SNCF Réseau, « *le niveau de criticité de chaque application détermine son mode d'hébergement : les applications critiques sont hébergées sur des serveurs appartenant à SNCF Réseau en France, organisés en 3 niveaux de sécurité croissants. Les applications non-critiques peuvent être hébergées en cloud public. Deux hyperscalers américains sont actuellement utilisés sur le périmètre non-critique : Microsoft Azure et Amazon Web Services* ».

Dans le cas de Natran, « *les capacités de calcul de l'entreprise reposent sur une architecture hybride, répartie entre des infrastructures en data center (DC) maîtrisées et des environnements cloud. Le recours au cloud concerne principalement des services fournis par Amazon Web Services (hébergement européen), et de manière plus marginale par Microsoft Azure (hébergement européen). Les contrats associés à ces services sont fondés sur les offres standard proposées par ces fournisseurs, avec une capacité de négociation essentiellement limitée aux aspects financiers (volumétrie, engagements de consommation, conditions tarifaires)* ».

La sélection d'offres de cloud public mais répondant à des critères stricts de sécurité commence à devenir une option possible. Elle n'est toutefois pas déployée de façon systématique et n'implique pas nécessairement la qualification SecNumCloud. Ainsi, EDF a signé deux contrats, avec S3NS et Bleu, en 2025, pour des solutions qui sont en cours de qualification SecNumCloud 3.2.

SNCF Réseau a introduit un nouvel accord-cadre contenant un lot pour le cloud souverain certifié SecNumCloud, permettant à partir de 2026 de migrer progressivement les applications sensibles vers des offres protégées contre les injonctions extra-européennes de type « Cloud Act ».

Enedis explique également que « *[ses] infrastructures sont hébergées dans des zones sécurisées (…) que cela soit sur le* on premise *(en data center) ou sur le cloud AWS (landing zone)* » sans que les mesures de protection prises pour l'utilisation des données stockées sur les infrastructures AWS ne soient réellement explicitées.

Enfin, le recours au cloud public provient de l'utilisation de solutions en mode SaaS. Enedis indique ainsi héberger la totalité des services de Microsoft Office 365 sur le cloud (y compris messagerie et gestion documentaire), ce qui met en doute la préservation de la confidentialité des données sensibles de l'entreprise.

Ainsi que l'indique ADP, « *les outils de planification de la maintenance reposent sur le logiciel Maximo d'IBM, qui est exploité* on premise*. Les données*

*relatives aux actifs ne sont pas stockées dans le cloud. Néanmoins, la société Autodesk nous pose une difficulté : son outil Autocad est connu de nos ingénieurs et architectes, et largement utilisé par les bureaux d'étude. Il est la référence du marché. Sa version collaborative, qui permet l'édition collaborative de plan, tourne sur un cloud AWS, et* ***Autodesk a refusé de s'engager à ce que les plans que nous déposons ne soient utilisés pour entraîner les modèles d'IA d'Amazon ou d'un de leurs partenaires*** ».

L'ensemble de ces éléments font apparaître l'absence de cadre commun applicable à ces entreprises pourtant responsables de l'exploitation de services d'importance similaire. La criticité des données et des applications est laissée à la seule appréciation des entreprises concernées. Les mesures techniques de protection ne sont pas harmonisées et des questions peuvent se poser quant à l'effectivité des mesures prises.

Ainsi, une partie des données des actifs de Natran, considérées comme « sensibles », sont hébergées sur un cloud public opéré par AWS « *dans des environnements maîtrisés, privilégiant des infrastructures internes ou des architectures cloisonnées, afin de garantir la maîtrise de leur localisation et de limiter les risques liés à l'extraterritorialité ».* Mais l'opérateur du réseau de transport de gaz explique dans le même temps que ***« les clauses techniques et opérationnelles restent largement imposées par les fournisseurs et peu modifiables****, notamment celles relatives aux architectures de référence (telles que les " Minimum Architecture Rules "), aux modèles de responsabilité partagée et aux conditions d'exploitation* ».

Chez Enedis, « *la gestion de la relation client, l'analyse de donnée, ainsi que le dépannage et le raccordement qui s'appuient sur la cartographie des réseaux de l'entreprise [s'appuient sur des fournisseurs extra-européens] (…). L'analyse des données, notamment le service de traitement des mesures électriques s'appuie massivement sur les solutions fournies par Teradata et par Microsoft. Les processus de dépannage et de raccordement s'appuient sur des outils cartographiques fournis par les éditeurs ESRI et General Electric Vernova* ».

Pour la gestion de la billettique de la RATP, les systèmes sont hébergés *on premise,* à l'exception des équipements en mobilité, hébergés par un *hyperscaler*. « *Les composants en cloud des systèmes billettiques et monétiques [ont été choisis] dans une logique de " simplification des architectures ", tels que le support des outils " en mobilité et connectés en 5G ". Pour ces projets, la dimension cyber a été un axe de travail important tandis que la souveraineté extra-européenne l'a été mais dans une moindre mesure. Les composants extra-européens, le cas échéant, découlent du choix de leurs sous-traitants par les fournisseurs sélectionnés* ».

Se retrouve ici la question de l'appréciation de la criticité des données, déjà perçue dans l'application de la doctrine Cloud au centre. Ainsi que l'indiquait Vincent Strubel, directeur général de l'Anssi devant la commission d'enquête : « *Pour les OIV, l'exigence est claire : tout système d'information critique hébergé*

*dans le cloud doit relever de SecNumCloud. Pour les autres systèmes, il convient d'identifier les données sensibles, d'éviter leur concentration et de ne pas les placer dans des environnements soumis à des droits extraterritoriaux* ». [(1)]

Au regard de ces éléments, les systèmes d'information des entreprises publiques doivent être soumis aux mêmes principes que ceux des administrations. Le contrôle réalisé par l'Anssi, destiné à examiner la robustesse des systèmes d'information d'importance vitale, doit être complété par un examen par l'État des risques en matière de protection des données sensibles.

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

Les constats des dépendances et vulnérabilités des opérateurs de services publics rejoignent ceux dressés pour les administrations. Les systèmes d'information industriels, constituant le cœur des applications critiques, ont fait l'objet d'une très forte attention : les fournisseurs sont en majorité européens, des solutions de repli existent, les équipes internes maîtrisent les produits, et l'hébergement des infrastructures repose sur des serveurs dédiés propriété des opérateurs. En revanche, concernant le SI tertiaire, les mêmes dépendances à Microsoft, Oracle et VMware sont relevées, avec peu de perspectives de transition à moyen terme.

Enfin, pour certaines applications métiers essentielles, dans la gestion des utilisateurs ou des clients par exemple, on peut constater une tendance à minimiser la sensibilité des données afin d'échapper aux règles de sécurité nécessaires à leur protection.

### B. LES ENTREPRISES PRIVÉES : UNE PRISE EN COMPTE BALBUTIANTE, PAS D'ACTIONS CONCRÈTES

Le secteur privé représente un poids majoritaire dans l'économie française. Les sociétés non financières comptaient ainsi pour 57 % de la valeur ajoutée brute nationale en 2020, contre 19 % pour les administrations et 12 % pour les ménages [(2)]. Ainsi que l'indique Mme Catherine Mayenobe, directrice générale déléguée de la Caisse des dépôts [(3)] : « *La commande publique est un levier, mais ce n'est pas le seul. On estime qu'elle représente environ 20 % du marché. Un de nos messages forts est qu'il faut s'adresser aux 80 % restants, c'est-à-dire les entreprises* ».

---

*(1) Audition de M. Vincent Strubel, directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi), 30 avril 2026.*

*(2) Insee, les comptes de la Nation en 2020, juillet 2021 https://www.insee.fr/fr/statistiques/5412399?sommaire=5354786*

*(3) Audition, ouverte à la presse, de Mme Catherine Mayenobe, directrice générale déléguée de la Caisse des dépôts, directrice des opérations et du pilotage de la transformation opérationnelle, le 18 mars 2026.*

Aujourd'hui, les vulnérabilités liées au numérique commencent à devenir un sujet de préoccupation des grandes entreprises, sans que cela ne soit un vecteur suffisant de changement. Pour celles qui s'emparent du sujet, le premier objectif est de mesurer l'ampleur de leurs dépendances et vulnérabilités.

La création de l'**indice de résilience numérique (IRN),** en janvier 2026, vise à fournir un outil de mesure du degré de dépendance pour les organisations partenaires : RTE, Docaposte, Caisse des dépôts, CMA-CGM, MAIF, SNCF Aéroports de Paris, Orange et Ouest-France. Les grandes entreprises mettaient déjà systématiquement en œuvre des analyses de risque et des plans de résilience face aux principaux risques identifiés. Phénomène nouveau, la dépendance à des outils propriétaires clés est désormais identifiée comme un risque majeur compte tenu du contexte géopolitique, ainsi que l'indique M. Arnaud Martin, directeur des risques opérationnels de la Caisse des dépôts :

« *Sur l'IRN, certains de ses huit axes de restitution sont nouveaux, d'autres préexistaient. L'axe stratégique et géopolitique, qui inclut le risque de kill switch, est plutôt nouveau et a émergé de manière concomitante avec les récentes échéances électorales américaines. La notion de dépendance économique et juridique, bien que latente, est devenue plus exacerbée avec l'essor de certaines solutions, comme dans la virtualisation récemment.*

« *En revanche, les axes de dépendance opérationnelle et de continuité d'activité existent depuis longtemps ; toutes les banques sont assujetties à des plans de poursuite d'activité. De même, la sécurité et la continuité, c'est-à-dire le volet cyber, sont des sujets qui montent en puissance mais qui existent depuis des décennies. L'axe environnemental est également émergent. Les axes technologiques, données, IA et chaîne d'approvisionnement (supply chain) existaient, mais prennent une importance croissante. Je pense notamment à la supply chain, sur laquelle Dora et Nis 2 mettent un accent particulier, car les dépendances et les attaques passent de plus en plus par ce biais.*

« *La force de l'IRN réside dans cette conjonction d'axes nouveaux et anciens. Auparavant, les informations sur ces risques parvenaient souvent au niveau du DSI ou du directeur des risques, mais rarement jusqu'au comité exécutif. L'IRN permet de consolider cette information et de donner une vision à 360 degrés, dépassant les seuls sujets de cybersécurité ou de continuité d'activité* ».

Le constat dressé par M. Henri d'Agrain, délégué général du Club informatique des grandes entreprises françaises (Cigref), est le même. La prise de conscience des risques potentiels entraîne dans un premier temps la mise en place d'outils de mesure du risque :

*« Depuis des décennies, les conséquences systémiques des dépendances numériques des entreprises, des administrations publiques et, plus largement, de notre économie ont été largement sous-estimées. Elles ont été insuffisamment analysées et souvent minimisées par de nombreux décideurs, qu'ils soient*

*économiques ou politiques. Dans un contexte de conflictualité croissante, la résilience numérique est ainsi devenue une préoccupation de tout premier plan pour l'ensemble des membres du Cigref (…).*

« *Enfin, nous ne recommandons pas d'étendre mécaniquement l'application de Dora à toutes les entreprises, ce qui serait irréaliste et difficilement applicable. En revanche, promouvoir* ***une définition commune de la résilience numérique, partagée par le secteur public comme par le secteur privé, nous paraît constituer une démarche pertinente*** *».* (1)

Toutefois, le décalage entre la prise de conscience et la mise en place d'actions concrètes est clairement souligné :

« *La conscience est désormais largement partagée : il est impératif de renforcer la résilience de l'économie européenne. Cette prise de conscience se traduit par des réflexions engagées au sein de nombreux acteurs.*

« *(…) La réalité est aujourd'hui la suivante : pour opérer efficacement à l'échelle mondiale – et, a minima, à l'échelle européenne –, peu d'acteurs sont en mesure d'offrir les performances, l'étendue fonctionnelle et la maturité technologique des hyperscalers américains. Nous pouvons toutefois espérer une réduction progressive de cet écart. Des acteurs européens comme OVHcloud, Scaleway ou encore Stackit au sein du groupe Schwarz, commencent à proposer des services à l'échelle (…)*

« *Pour les grandes entreprises, celles que je connais et que je représente, il est indispensable d'aboutir enfin à ce marché numérique unique, ce " digital single market " dont nous parlons depuis quinze ou vingt ans, sans jamais réellement le concrétiser. Il ne s'agit plus de raisonner en termes d'acteurs nationaux, mais d'identifier les grands opérateurs européens de cloud sur lesquels il conviendrait de concentrer des investissements massifs.*

« *Si une telle dynamique voyait le jour, appuyée par des instruments comme un schéma européen de certification type EUCS garantissant une protection juridique effective des données, un consensus émergerait rapidement parmi les grandes entreprises. En revanche, désoptimiser l'organisation européenne pour multiplier des solutions fragmentées selon les pays n'est ni viable ni soutenable. »* (2)

Ainsi, les grandes entreprises, qui ne représentent elles-mêmes que 35 % de la valeur ajoutée (3), commencent seulement à identifier le risque engendré par l'utilisation de produits propriétaires extra-européens, sans pour autant mettre en œuvre des plans de transition. On peut supposer que la prise en compte du risque

---

*(1) Audition de M. Henri d'Agrain, le 30 avril 2026.*

*(2) Audition Henri d'Agrain, délégué général du Club informatique des grandes entreprises françaises (Cigref), le jeudi 30 avril 2026.*

*(3) Insee, Les entreprises en France édition 2023, décembre 2023 https://www.insee.fr/fr/statistiques/7678542?sommaire=7681078*

numérique au sein des organisations de plus petite taille, est encore moins avancée. Le poids économique de la commande privée, bien supérieur à celui de la commande publique, pourrait lui conférer un rôle important dans la réduction des dépendances systématiques 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.

Henri d'Agrain, lors de son audition, reconnaissait d'ailleurs qu'à ce stade, les enjeux de protection des données ou de souveraineté des solutions utilisées ne sont pas dans les critères prioritaires en termes de choix d'outils numériques : « *Une entreprise ne décidera jamais de quitter une solution existante et d'engager des efforts significatifs si cette démarche n'apporte aucun bénéfice tangible. Elle ne le fait que si cela répond à un besoin directement lié à son activité, à sa productivité, à sa compétitivité. En l'absence d'enjeu avéré, notamment en matière de sécurité, les entreprises n'ont aucun rationnel économique pour changer* ».

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.

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

## C. LE CAS PARTICULIER DU SECTEUR BANCAIRE ET DES OUTILS DE PAIEMENT

### 1. La détection de la dépendance à des fournisseurs critiques de technologies numériques imposée par le règlement Dora

Dans un contexte d'utilisation de plus en plus massive des outils numériques par les entités du secteur financier, le règlement 2022/2554 du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier, plus communément appelé règlement Dora (Digital Operational Resilience Act) est entré en application le 17 janvier 2025.

Dora a vocation à couvrir l'ensemble des risques opérationnels liés à l'utilisation des technologies numériques, et s'est donc structuré autour de quatre piliers : un cadre de gestion du risque renforcé, une nouvelle procédure de gestion et de notification des incidents majeurs, l'introduction d'exigences en matière de tests de résilience et, enfin, la gestion du risque de tiers. C'est ce dernier pilier qui traite directement de la dépendance à des fournisseurs extra-européens.

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, dix ont leur siège aux États-Unis, et seulement cinq dans l'Union européenne.

**LISTE DES ENTITÉS DÉSIGNÉES FOURNISSEURS DE SERVICES TIERS ESSENTIELS EN APPLICATION DU RÈGLEMENT DORA**

| Entité | Secteur d'activité | Siège social maison-mère |
|---|---|---|
| Accenture plc | Services numériques | Irlande |
| Amazon web Services EMEA Sarl | Cloud et logiciels | États-Unis |
| Bloomberg L.P. | Services financiers | États-Unis |
| Capgemini SE | Services numériques | France |
| Colt Technology Services | Télécommunications | Royaume-Uni |
| Deutsche Telekom AG | Télécommunications | Allemagne |
| Equinix (EMEA) B.V. | Data centers | États-Unis |
| Fidelity National Information Services, Inc. | Services financiers | États-Unis |
| Google Cloud EMEA Limited | Cloud et logiciels | États-Unis |
| International Business Machine Corporation | Cloud et logiciels | États-Unis |
| InterXion HeadQuarters B.V. | Data centers | États-Unis |
| Kyndryl Inc. | Services numériques | États-Unis |
| LSEG Data and Risk Limited | Services financiers | Royaume-Uni |
| Microsoft Ireland Operations Limited | Cloud et logiciels | États-Unis |
| NTT DATA Inc. | Services numériques | Japon |
| Oracle Nederland B.V. | Cloud et logiciels | États-Unis |
| Orange SA | Télécommunications | France |
| SAP SE | Cloud et logiciels | Allemagne |
| Tata Consultancy Services Limited | Services numériques | Inde |

*Source : European securities and markets authority, (1).*

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. S'y ajoutent des entreprises de services numériques et financiers de taille internationale ainsi que des opérateurs de data centers.

Les règles s'imposent à la fois aux fournisseurs désignés comme CTTP et aux établissements financiers qui sont leurs clients. Les premiers font l'objet d'une surveillance réalisée par des équipes conjointes d'examen (*Joint Examination Team*) auxquelles des agents de l'Autorité de contrôle prudentiel et de résolution (ACPR) française et de la Banque de France participent depuis le 1er janvier 2026. Ils sont soumis, en théorie, à des audits et inspections, à des tests de résilience et à des recommandations correctrices pouvant aller jusqu'à des injonctions contraignantes. Quant aux seconds, ils ont l'obligation d'identifier et de cartographier l'ensemble de leurs sous-traitants dans ce domaine et d'analyser les risques liés à la localisation géographique des sous-traitants. Cette analyse de risques, qui doit être documentée, porte sur les risques de verrouillage technologique (*vendor lock-in*), la substituabilité réelle des prestataires, la capacité

*(1) European securities and markets authority, novembre 2025, List of designated CTPPs*

à maintenir les fonctions critiques en cas de défaillance d'un sous-traitant ou encore la concentration des services sur un nombre limité d'acteurs. Ils doivent définir des plans de sortie réalistes (aussi bien aux plans financier, juridique et technique) avec une réversibilité des données (migration, portabilité, interopérabilité).

Ainsi que l'indique la Banque de France dans les réponses écrites à la rapporteure : pour la majeure partie des deux cents entités du secteur ayant été interrogées, à l'été 2025, par le biais d'un questionnaire sur l'application du règlement Dora, la gestion du risque de tiers est « *le pilier de Dora qui est le plus difficile à mettre en œuvre, la (re)négociation des contrats avec les prestataires informatiques constituait un véritable défi pour les entités. Il constitue cependant un levier essentiel afin de rééquilibrer le rapport de force entre les plus gros prestataires et les entités financières* ».

Ces éléments sont-ils de nature à entamer une véritable transition vers des acteurs européens ? La réglementation n'impose techniquement aucune obligation en ce sens, mais les critères à respecter poussent ainsi le secteur bancaire à prendre en compte de façon structurelle les risques liés à la mono-dépendance à un fournisseur et à l'extra-territorialité du droit. Selon M. Olivier Fliche, directeur du pôle Fintech – Innovation de l'Autorité de contrôle prudentiel et de résolution (ACPR), « *Quant à la question de la dépendance de certains grands prestataires cloud, le règlement Dora la prend partiellement en charge. Il n'impose pas le recours à des solutions souveraines, mais il essaie de rééquilibrer la relation entre le prestataire cloud et l'établissement financier, en proposant notamment des clauses contractuelles, des programmes de sortie et des plans de continuité d'activité* » [(1)]. À la question de la rapporteure, M. Fliche répondait ainsi que l'application de Dora était encore trop précoce pour en estimer les effets : « *Je ne dispose pas d'éléments suffisants pour répondre à votre question, mais les reportings prévus par le règlement Dora permettront de les compléter et d'estimer le niveau de dépendance.*

« *Un premier exercice a eu lieu en 2025, mais les données restent indicatives et ne concernent pas l'ensemble du périmètre, toutes les entités n'ayant pas répondu. Une petite moitié des répondants avait au moins un contrat Microsoft en lien avec une fonction critique ou importante, un quart avec Amazon et un sixième avec Google, sachant qu'il est probable que ces données s'additionnent, les groupes pouvant détenir plusieurs contrats avec plusieurs prestataires* ».

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.

---

*(1) Table ronde sur les services de paiement, le mercredi 8 avril 2026.*

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

Ainsi que l'indique la Banque de France dans les réponses adressées à la rapporteure, on observe une numérisation croissante des usages des Français dans les paiements de détail. Même s'ils restent très attachés aux espèces, la carte bancaire est devenue en 2024 le premier moyen de paiement en magasin (48 % des achats en 2024 contre 43 % réglés en espèces), notamment en raison du paiement sans contact et du paiement mobile. Le recours croissant au commerce en ligne (25 % des transactions en France en 2024) contribue également à cette numérisation des paiements. La rapporteure a souhaité comprendre dans quelle mesure ces évolutions ont des répercussions sur le niveau de dépendance de notre économie à des solutions extra-européennes.

#### *a. Paiements par carte bancaire : une dépendance réduite mais qui demeure toutefois menacée*

La numérisation du paiement soulève des enjeux forts, et il est intéressant de constater que, de ce point de vue, la France est bien mieux positionnée que la plupart de ses homologues européens grâce à la constitution historique du groupement d'intérêt économique (GIE) des cartes bancaires (CB). Au moment de la création du GIE CB, l'action du ministre de l'économie Pierre Bérégovoy a permis de donner l'impulsion politique nécessaire pour surmonter la fragmentation entre les deux réseaux concurrents Carte Bleue et Carte Verte.

Comme l'explique M. Philippe Laulanie, directeur général du groupement des Cartes bancaires : « *C'est un modèle coopératif et non mercantile, créé en 1984 sous l'impulsion de Pierre Bérégovoy, afin de soutenir l'invention industrielle de la carte à puce, dans le cadre des plans de l'aménagement des territoires et des télécoms. C'est donc une filière française soutenue par l'État et déployée par les banques au service de nos citoyens, sous la surveillance de la Banque de France pour les aspects sécuritaires et inclusifs. Cette filière est encore aujourd'hui française de bout en bout : de la puce, que nous pouvons fabriquer en indépendance et libre de droits grâce à notre histoire industrielle, au terminal d'acceptation chez les commerçants, et jusqu'aux rails et usines de traitement des transactions, qu'elles soient dans les banques ou mutualisées au sein de la société STET (…).*

« *95 % des paiements de détail français – carte, cash, mobile – sont domestiques et gérés par CB. Ce n'est pas nécessairement le cas dans d'autres pays. En Allemagne, par exemple, l'e-commerce est dominé par PayPal. Sur les 5 % restants, 3 % sont des paiements intra-européens et 2 % des paiements extra-européens. Le paiement est donc avant tout un enjeu domestique.*

« *En matière de sécurité, nous enregistrons deux fois moins de fraudes que les réseaux de cartes internationaux grâce à des traitements assurés par une intelligence artificielle entraînée exclusivement sur des données françaises qui ne sont ni revendues ni adressées à l'étranger, et à des systèmes totalement souverains.*

*La fraude sur la vente à distance, qui était un problème majeur, a baissé de 45 % grâce à la mise en œuvre du règlement DSP2 RTS avec les commerçants, les industriels, les banques et les régulateurs (…).*

« *CB protège chaque année plusieurs milliards d'euros de valeur nationale, et ce depuis quarante ans. Le coût d'une transaction CB est en moyenne dix fois moins important pour un commerçant français, la fraude est divisée par deux ou trois, et les données sont totalement sécurisées, non revendues et non externalisées. L'intérêt du cobadging CB, qui évite que les données partent à l'étranger et permet d'activer le système Visa ou Mastercard si CB était en panne, ou inversement, doit être réaffirmé, comme le prévoit le plan du Comité national des moyens de paiement.* » [(1)]

La situation est différente dans les autres États membres. Seuls l'Allemagne (Girocard), la Belgique (Bancontact), l'Italie (Bancomat) et le Portugal (MutliBanco) ont développé une initiative similaire. La majorité des autres États membres (seize sur vingt-et-un) ne disposent pas d'un réseau national significatif et les grands réseaux internationaux comme Visa et Mastercard sont dans une situation d'oligopole. « *Il est en effet alarmant de constater que 60 % des paiements européens ne sont plus souverains et que la majorité des pays n'ont plus le choix qu'entre Visa ou Mastercard. Pour rappel, en France, ce sont les commerçants qui choisissent la marque, et non les consommateurs.* »

La dépendance aux réseaux Visa et Mastercard s'impose également dans le cas des paiements transfrontière, y compris à l'intérieur de l'Union européenne. Par exemple, un touriste français qui effectue un achat par carte en Allemagne y a recours en l'absence d'interconnexion entre les réseaux nationaux.

Outre les sujets de vulnérabilité à des technologies et entreprises étrangères, la dépendance aux grands réseaux internationaux a également des conséquences économiques fortes : des frais de réseau appliqués par Visa et Mastercard sensiblement supérieurs à ceux pratiqués par CB, d'une part, des pratiques commerciales jugées peu transparentes par les commerçants (par exemple, l'application de pénalités), d'autre part.

En France, le recul des pratiques de cobadging et le développement du paiement mobile, sur lequel CB n'était pas présent jusqu'à récemment, ont conduit à une érosion de la place du réseau national depuis 2019.

Face à cette situation, plusieurs actions ont été menées pour réaffirmer l'importance et la place du GIE CB, coordonnées par le Comité national des moyens de paiement (CNMP) :

– un plan stratégique de modernisation du réseau CB pour l'adapter aux nouveaux modes de paiement, en particulier les paiements mobile.

---

*(1) M. Philippe Laulanie, table ronde sur les services de paiement, le mercredi 8 avril 2026.*

Selon M. Philippe Laulanie, « *CB est aujourd'hui présent dans l'ensemble des paiements : pour retirer du cash, pour payer en proximité avec ou sans contact, et pour payer par mobile. En effet, 90 % des transactions via des solutions comme Apple Pay sont en réalité des paiements par carte. Sur le plan de la sécurité, ces paiements digitaux profitent de toute l'histoire et de la robustesse du système CB (…). D'ici 2026, l'ensemble des banques françaises proposera Apple Pay, Samsung Pay et Google Pay, avec les avantages de la carte cobadgée en matière de coût, de fraude et de protection des données (…). Nous sommes donc agnostiques et la carte française cobadgée CB est polyvalente, ce qui n'est absolument pas le cas dans les autres pays européens. En revanche, si le logo CB n'apparaît pas sur une carte, l'intégralité des données de transaction échappe à notre écosystème* ».

– les engagements récents de certaines banques pour refaire du cobadging des cartes la norme. Selon M. Erick Lacourrège, directeur général des moyens de paiements de la Banque de France [(1)] *:* « *Les six grands groupes bancaires français se sont engagés à cobadger toutes les cartes qu'ils émettent, et la Banque de France veille, en tant que régulateur, que les nouveaux entrants s'y engagent également. Il s'agit d'un sujet stratégique, car les grands acteurs américains disposent d'une base installée mondiale et d'une rentabilité leur permettant de mener une politique commerciale très dynamique, qui leur assure des parts de marché importantes* ». Toutefois, il convient de noter l'absence des discussions de certaines banques en ligne : *« Concernant le cobadgeage CB des banques en ligne, nous incitons tous les acteurs à cobadger, mais leur participation à cette stratégie du GIE CB supportée par la Banque de France reste volontaire. Un certain nombre de banques en ligne restent effectivement à convaincre, mais leur volonté ne fait pas de doute* ».

– Dans le cadre de la stratégie nationale des moyens de paiement, la souveraineté constitue un impératif stratégique pour l'écosystème. Notre stratégie s'articule également autour du principe directeur du libre choix du moyen de paiement pour les utilisateurs. L'action du CNMP vise donc à éclairer le grand public sur les implications du choix des différents moyens de paiement.

– le renforcement de l'information du public. Elle porte notamment sur le choix de la marque lors des paiements par carte : le règlement 2015/751, aussi appelé règlement IFR, donne aux consommateurs la possibilité de choisir le réseau de paiement qu'ils utilisent dans leurs transactions en magasin et en ligne. En pratique, les consommateurs détenant une carte cobadgée ont la possibilité de choisir le réseau de carte CB pour leurs paiements. L'information sur la localisation des données de paiement doit également être renforcée.

*(1) Table ronde sur les services de paiement, le mercredi 8 avril 2026.*

### *b. Le développement de nouveaux outils de paiement : le paiement instantané et, à terme, l'euro numérique*

Au-delà du maintien de la place du GIE CB, la préservation de la souveraineté sur les moyens de paiement passe 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. Son déploiement a commencé en 2024 pour les paiements entre particuliers et devrait s'étendre aux paiements auprès des commerçants et à l'e-commerce dès la fin de l'année 2026. Mme Martina Weimart, directrice générale d'EPI décrit Wero de la façon suivante [(1)] : « *L'idée est de créer un portefeuille électronique, un wallet, qui peut contenir différents moyens de paiement comme le paiement instantané, qui offre un lien direct avec le compte bancaire du consommateur, mais également des cartes, des tickets-restaurants ou, demain, l'euro numérique. L'objectif est de donner le choix au consommateur et de permettre les transactions instantanées chez les commerçants (…). Nous avons commencé par le paiement de personne à personne (P2P), mais nous visons aujourd'hui les professionnels et les petits commerçants qui peuvent accepter des paiements par téléphone mobile ou par QR code. Notre solution, disponible dans notre propre application, est également intégrée dans les applications bancaires ».*

La société EPI vise une expansion de l'utilisation de la solution à l'échelle européenne, soit directement soit via des accords commerciaux. En effet, des solutions similaires étant développées dans d'autres pays européens (par exemple, Bizum en Espagne), un rapprochement entre ces solutions domestiques – réunies au sein du consortium EuroPA – et EPI a été initié l'an dernier afin de construire une interopérabilité entre ces solutions.

« *Nous avons commencé avec trois pays, en comptons désormais cinq – la France, l'Allemagne, la Belgique, les Pays-Bas et le Luxembourg – et préparons notre expansion vers l'Autriche et d'autres marchés. Nous avons également conclu un accord d'interopérabilité pour étendre notre couverture géographique. L'objectif est d'offrir une forme européenne de paiement instantané, basée sur un standard et des règles européennes dont nous avons la maîtrise totale, et qui correspond à l'ère numérique où tout doit être immédiat (…).*

« *Le nombre de clients inscrits, aujourd'hui de 53 millions, est en forte expansion. Ainsi, 15 millions d'utilisateurs néerlandais vont migrer de leur solution nationale, iDEAL, vers Wero, car ils avaient besoin d'une solution plus moderne couvrant davantage de cas d'usage, notamment le commerce physique, l'intégration de cartes nationales ou internationales, ou le paiement de factures. Au Luxembourg, par exemple, 86 % des factures sont payées via un QR code. Le plus*

*(1) Table ronde sur les services de paiement, le mercredi 8 avril 2026.*

*important, pour nous, est d'offrir le choix au consommateur tout en lui garantissant un contrôle total de ses données.*

« *Au-delà du cadre national et européen, nous devons utiliser les marges de manœuvre qu'offre le paiement de compte à compte pour les paiements à l'international. Nous comptons aujourd'hui, dans le monde, 64 initiatives comme la nôtre. PIX au Brésil, ou UPI en Inde, sont très appréciés des consommateurs en raison du lien entre le compte bancaire et le téléphone mobile. PIX a même dépassé Visa au Brésil.*

« *Wero se déploie progressivement, marché par marché, et cas d'usage par cas d'usage. Ce mois-ci, les premières transactions e-commerce seront possibles en France, après l'Allemagne et la Belgique. Grâce à notre coopération avec d'autres solutions, nous sommes déjà capables de couvrir 130 millions de consommateurs sur 13 marchés. Cela nous permettra de couvrir rapidement l'Europe et d'être un partenaire crédible pour les coopérations internationales, car la prochaine étape est l'interopérabilité mondiale* ».

Preuve de l'omniprésence des *hyperscalers* et de la difficulté à développer une offre intégralement souveraine, *l'European Payments Initiative*, le consortium portant l'initiative Wero, a reconnu auprès de netzpolitik.org qu'une partie des données de Wero transitait par des serveurs d'Amazon (1).

Enfin, en complément des initiatives mentionnées précédemment, se prépare également le lancement de l'**euro numérique**. Ce projet, qui est porté par l'Eurosystème (2) 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. Selon la Banque de France (3), « *le Conseil a adopté une position en soutien du projet en décembre 2025 et les négociations sont en cours au Parlement européen avec un vote attendu en mai 2026. Si les colégislateurs s'accordent sur le fondement juridique de l'euro numérique cette année, cela signifie qu'un pilote restreint verra le jour en 2027, sera étendu en 2028 et que, suite à une décision de la BCE des gouverneurs de la zone euro réunis au Conseil des gouverneurs de la BCE, une entrée de l'euro numérique pour les citoyens et les commerçants en Europe verrait le jour en 2029* ».

La stratégie de réduction de la dépendance aux acteurs européens menée par les acteurs du secteur repose sur la diversification des options offertes au consommateur. Comme le décrit la Banque de France : « *Les études que nous*

---

*(1) Daniel Leisegang,* Europäischer Bezahldienst Wero nutzt Amazon-Server, *Netzpolitik.org, avril 2026 https://netzpolitik.org/2026/uneingeloestes-versprechen-auf-digitale-souveraenitaet-europaeischer-bezahldienst-wero-nutzt-amazon-server/#netzpolitik-pw*

*(2) 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.*

*(3) Réponses écrites au questionnaire de la rapporteure*

*menons au sein de la Banque de France sur l'évolution des usages des moyens de paiement montrent que les habitudes de paiement sont marquées par une forte inertie et évoluent de manière progressive. Il est donc très probable que ces différentes formes de paiement coexistent dans les prochaines années, avec la poursuite de tendances structurelles : la diminution de l'usage des espèces à des fins transactionnelles, même si celles-ci continueront à jouer un rôle clé dans les paiements du quotidien en raison de la singularité de leurs caractéristiques (p.ex. anonymat, inclusion) ; le maintien de la carte à un niveau élevé, avec une accélération de son usage via le mobile ; le développement du virement instantané lié (i) au plein effet de l'entrée en vigueur du règlement sur les virements instantanés et (ii) à l'arrivée sur le marché d'offres fondées sur ce type de paiement (p.ex. Wero) ; l'arrivée probable de l'euro numérique, qui permettra de disposer d'un équivalent numérique du billet pour accompagner la numérisation des usages.*

« *Tous ces différents moyens de paiement constituent des réponses complémentaires qui visent à répondre à notre besoin de souveraineté et de résilience dans les paiements de détail.* »

*
* *

Confirmant les constats qui avaient présidé à la création de la commission d'enquête, les travaux menés par la rapporteure conduisent à conclure à une dépendance avérée aux solutions et fournisseurs de logiciels et de cloud déployés par des entités américaines :

– Dans le domaine de la bureautique et des systèmes d'exploitation, la dépendance aux produits Microsoft est généralisée, créant de ce fait une vulnérabilité à grande échelle. Tous les acteurs sont concernés, administrations comme entreprises privées

– Dans le domaine des logiciels « tertiaire », certaines solutions portant sur la virtualisation ou le traitement des bases de données constituent le socle de l'ensemble du parc applicatif des systèmes d'information des entités publiques et privées gérant des volumes de données importantes. Ces solutions sont substituables, mais à la condition d'efforts de migration longs et coûteux.

– La situation est contrôlée dans le domaine des SI industriels des entreprises opérant des services essentiels, ainsi que pour les applications qui constituent le cœur des services publics.

L'utilisation de services cloud au sein des administrations, cadrée par la doctrine Cloud au centre, se traduit par le recours quasi-exclusif à des clouds internes ou des fournisseurs labellisés SecNumCloud. Des cas de non-conformité à la doctrine ont toutefois été identifiés. Les opérateurs d'importance vitale se

trouvent dans une situation de vulnérabilité plus forte, ayant davantage recours à des solutions de clouds américains.

– Le point de vulnérabilité le plus critique concerne le secteur privé, qui fait aujourd'hui majoritairement appel à des solutions américaines pour le déploiement des solutions de cloud, et en particulier sous la forme d'offres SaaS. La prise en compte de cette problématique est très récente au sein des entreprises.

# 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 raison de la moindre importance politique du sujet jusqu'à un passé récent, la mesure de la contribution réelle des grands acteurs américains à l'économie française a fait l'objet de peu de travaux de mesure. Dans le fonctionnement de ces entreprises multinationales, l'essentiel de la valeur ajoutée est créé hors de France et les produits sont simplement commercialisés sur le marché local.

L'omniprésence de solutions étrangères sur certains segments du marché conduit également à restreindre l'espace économique des acteurs nationaux du numérique. La rapporteure a souhaité mesurer les conséquences potentielles de ce phénomène, pour les entreprises françaises du secteur du numérique, mais aussi pour les administrations et l'ensemble du tissu économique.

Cette préoccupation rejoint les alertes tirées lors de plusieurs auditions devant la commission. Mme Catherine Mayenobe, directrice générale déléguée de la Caisse des dépôts déclarait ainsi : « *Le diagnostic que nous posons est proche de celui qui a motivé la création de votre commission : il est alarmant. En tant que groupe public financier, nous constatons une urgence claire à agir pour faire face aux dépendances technologiques héritées des dernières décennies. Cet héritage est d'autant plus préoccupant qu'il s'inscrit dans un contexte de double révolution. La première est technologique, avec l'arrivée de l'intelligence artificielle (IA) générative, qui pose en des termes nouveaux et encore plus inquiétants le diagnostic de notre dépendance aux solutions de cloud. Cette révolution redéfinit de façon drastique la chaîne de valeur des grands acteurs économiques. Au-delà des constats que vous avez vous-mêmes établis sur la part très importante des produits numériques consommés en France provenant de zones extra-européennes – le chiffre de 80 % reste d'actualité –, les conséquences sont lourdes : fuites de données stratégiques, perte de valeur économique estimée à près de 265 milliards d'euros par an pour l'Union européenne en achats de solutions, selon une étude du club informatique des grandes entreprises françaises (Cigref) commanditée auprès du cabinet Asterès, et une exposition majeure à des risques géopolitiques croissants* ». [(1)]

*(1) Audition, ouverte à la presse, de Mme Catherine Mayenobe, directrice générale déléguée de la Caisse des dépôts, directrice des opérations et du pilotage de la transformation opérationnelle, le 18 mars 2026.*

Mme Cristina Caffara, économiste, représentant le collectif Eurostack, pointait également le risque d'un décrochage économique, conséquence d'une cannibalisation de la valeur par les acteurs américains entraînant elle-même une réaction en chaîne sur les investissements :

« *L'Europe a longtemps considéré que l'infrastructure cloud était une infrastructure passive, à l'instar de l'eau ou de l'électricité, et que nous ne laisserions d'ailleurs pas des acteurs étrangers gérer à notre place. Or, le cloud n'est pas passif ; il constitue la rampe de lancement à partir de laquelle se déploie un large éventail de services numériques, de gestion des données et d'applications commerciales qui nous ont rendus dépendants, à tous les niveaux, y compris les entreprises, les administrations et la vie quotidienne. L'Europe ne peut plus rester dans cette position de vulnérabilité extrême, qui n'est pas acceptable.*

« *De mon point de vue, il ne s'agit pas seulement d'une question de sécurité ou de résilience, mais de croissance économique. En effet, si vous ne captez pas la chaîne de valeur sur laquelle reposent vos services, vous envoyez des montants considérables à l'étranger que vous auriez pu investir en Europe. Nous savons tous que la productivité européenne croît beaucoup plus lentement que celle des États-Unis, essentiellement en raison du manque d'investissement technologique. Dans ce domaine, nos investissements sont bien plus faibles, et si nous poursuivons dans cette voie, l'écart va continuer à se creuser.*

« *Pourtant, nous sommes un continent riche : nous épargnons deux fois plus que les États-Unis et nous envoyons chaque année environ 300 milliards d'euros vers des sociétés de capital américain. Nous devons donc utiliser nos capacités propres, qui sont considérables, d'autant plus que l'Europe dispose également de nombreux talents.* » [(1)]

Ce chapitre présente les éléments recueillis permettant de répondre aux questions suivantes :

– quelle place occupent les acteurs états-uniens dans le secteur du numérique en France ? quelle est leur part de marché dans les logiciels, et plus particulièrement dans les administrations ? Comment se comparent-ils aux acteurs français ?

– quelle valeur créent-ils ? La richesse créée en France est-elle importante ? Quelles sont les retombées en matière fiscale ?

*(1) Audition, ouverte à la presse, de l'association Eurostack, représentée par Mme Cristina Caffarra, économiste, et M. Yann Lechelle, le 26 mars 2026.*

## A. ACTEURS FRANÇAIS ET AMÉRICAINS DU NUMÉRIQUE : UN DÉSÉQUILIBRE FLAGRANT

La commission d'enquête s'est concentrée sur trois domaines : le logiciel, la publicité en ligne et le cloud. Bien que les dynamiques et la structuration des trois secteurs soient très différentes, la comparaison des chiffres d'affaires réalisés en France par les Big Tech avec ceux des entreprises nationales révèle un déséquilibre flagrant.

### 1. Secteur des logiciels : les filiales françaises de Microsoft et Oracle dans le Top 5 des éditeurs français

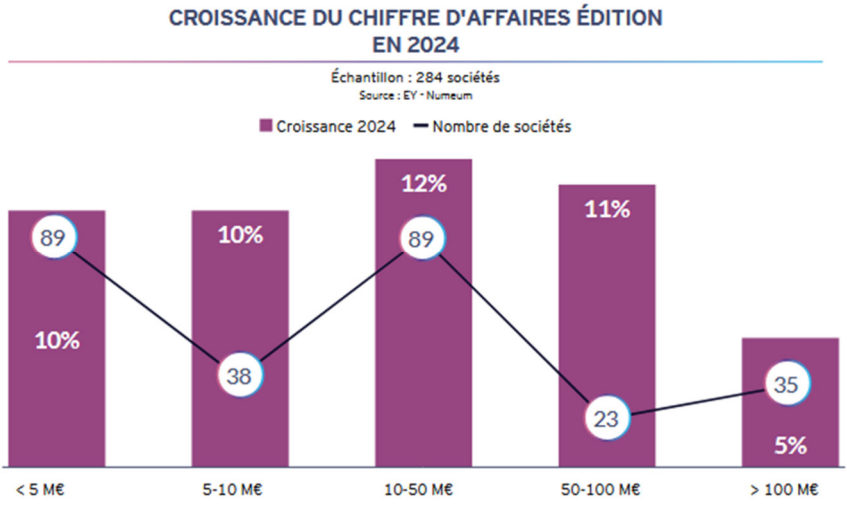
L'étude réalisée par Numeum sur les 250 plus grands éditeurs de logiciels français [(1)] comporte des données très précises sur le positionnement économique des acteurs nationaux. L'intérêt de l'étude est qu'elle se concentre sur les sociétés ayant déclaré ne pas être une filiale d'un groupe étranger. L'étude dresse le constat suivant :

– le chiffre d'affaires réalisé par les développeurs de logiciels *pure players* (hors activités de conseil) était de 23,1 milliards d'euros en 2024. Parmi eux, les éditeurs sectoriels représentent 14,4 milliards de chiffre d'affaires (62 %), contre 5,5 pour les éditeurs dits horizontaux et 3,2 milliards pour le segment des logiciels aux particuliers et des jeux vidéo ;

– les effectifs employés par les éditeurs français s'élevaient à 219 000 salariés, dont 115 000 spécifiquement dans le domaine du développement de logiciels ;

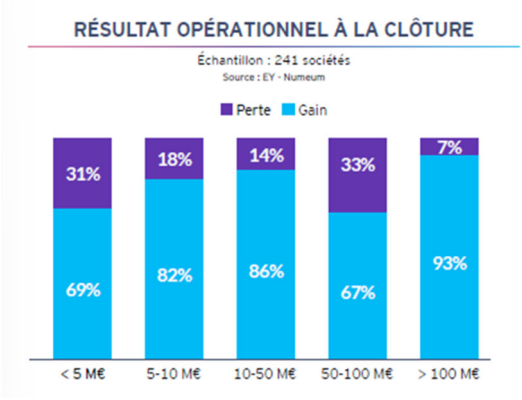
– le secteur compte trente-cinq sociétés réalisant un chiffre d'affaires supérieur à 100 millions d'euros. Trois d'entre elles ont un chiffre d'affaires supérieur à 1 milliard : Dassault Systèmes (5,6 milliards sur le développement de logiciels et 6,2 milliards au total), Ubisoft (1,9 milliard) et Criteo (1,8 milliard). Dassault systèmes et Criteo sont qualifiées d'éditeurs sectoriels, Ubisoft opère dans le domaine des jeux vidéo. Les deux premiers éditeurs horizontaux sont Cegid (967 millions de chiffre d'affaires) et 74Software, ex-Axway software (690 millions) ;

(1) *Numeum, EY,* Panorama Top 250 des éditeurs de logiciels français, *15ème édition, novembre 2025* https://numeum.fr/economie-marche/panorama-top-250-des-editeurs-de-logiciels-francais-15eme-edition-lia-entre-au-coeur-du-modele-des-editeurs-francais/




*Source : Numeum.*

– la rentabilité des éditeurs pose question : si 79 % ont réalisé un bénéfice d'exploitation en 2024, c'est le cas de 93 % des éditeurs de plus de 100 millions d'euros de chiffres d'affaires, mais de seulement 66 % des éditeurs de chiffre d'affaires compris entre 50 et 100 millions. Ces chiffres sont à comparer à ceux de l'ensemble des entreprises françaises : la part des PME et des ETI déclarant un bénéfice était de 78 % en 2021, et celle des grandes entreprises de 76 % [(1)] ;

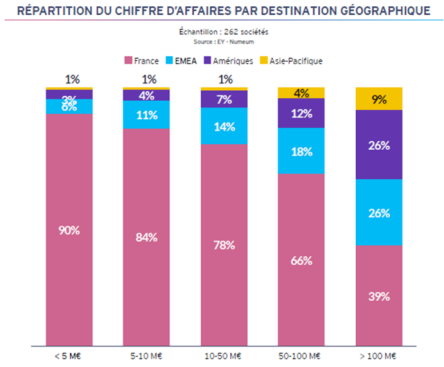



*Source : Numeum.*

– le crédit d'impôt recherche est au cœur du modèle des éditeurs, puisque 73 % des éditeurs y ont recours, notamment chez les éditeurs réalisant plus de 100 millions de chiffre d'affaires (86 %) ;

*(1) Insee, Impôt sur les sociétés, décembre 2023 https://www.insee.fr/fr/statistiques/7678564*

– 55 % du chiffre d'affaires des éditeurs français était réalisé à l'international, soit 12,7 milliards d'euros. Cependant, comme l'indique l'étude, « *ce chiffre cache toutefois de fortes disparités : l'internationalisation repose surtout sur quelques géants. Les trois premiers éditeurs du classement — Dassault Systèmes, Criteo et Ubisoft — contribuent fortement à l'internationalisation du secteur avec près de 9 milliards d'euros de chiffre d'affaires réalisés à l'international* ». Le niveau d'internalisation décroît fortement avec la taille des entreprises ;




*Source : Numeum.*

La France est le premier marché pour 91 % des fournisseurs. La Belgique et la Suisse sont le second marché pour 15 % d'entre eux, et l'Allemagne pour 12 %.

Le SaaS est le modèle économique dominant, représentant 64 % de l'activité. Les éditeurs hébergent leurs données 50 % chez un fournisseur cloud, seulement 35 % d'entre eux recourant directement à un opérateur de data center et 13 % hébergeant leurs données en propre.

Ces chiffres sont à comparer avec ceux des entreprises leaders mondiales de l'édition du logiciel, sur le périmètre de leur activité française. Le tableau ci-dessous indique le chiffre d'affaires réalisé en France par cinq entreprises leaders mondiales : Microsoft, SAP, Oracle, VMWare et Red Hat. Il les positionne sur ce critère dans le classement réalisé par Numeum sur le périmètre des éditeurs français.

Parmi les entreprises françaises du secteur, seule Dassault Systèmes réalise un chiffre d'affaires supérieur à celui de Microsoft France. Oracle France se situe à la cinquième place. VMWare et Red Hat sont de taille inférieure, mais tout de même à la vingt-cinquième et trente-troisième place.

**CHIFFRE D'AFFAIRES RÉALISÉ EN FRANCE DES SOCIÉTÉS LEADERS MONDIALES DE L'ÉDITION DE LOGICIELS**

| Éditeur | Chiffre d'affaires (M€) | Nombre de salariés | Rang Top 250 Éditeurs français |
|---|---|---|---|
| Microsoft France | 4 744 | 2 021 | 2 |
| SAP France | 1 376 | 1 658 | 4 |
| Oracle France | 972 | 922 | 5 |
| VMWare France | 159 | 422 | 25 |
| Red Hat | 115 | 419 | 33 |

*Source : DGFIP, réponse aux questionnaires de la rapporteure.*

*Note : chiffre d'affaires réalisé en France, incluant les exportations.*

Ces sociétés occupent les premières places du classement en France mais aussi sur le marché américain et fort probablement dans l'ensemble des États membres de l'Union européenne. Bien que très dynamiques, les entreprises françaises du secteur du logiciel et de l'édition sont insuffisamment positionnées dans d'autres zones géographiques. L'activité générée par les principales d'entre elles est comparable à l'activité des leaders mondiales sur leur seul périmètre français.

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

L'Insee chiffre le marché de la régie publicitaire de médias, tous médias confondus (catégorie « M73Z2 Régies publicitaires de médias »), à 5,2 milliards d'euros [(1)].

Le tableau ci-dessous présente les chiffres de l'activité réalisée en France par les acteurs internationaux, comparés à ceux de la plateforme française Dailymotion. L'activité des sociétés Google France, Facebook France et Amazon online France SAS est celle de régie publicitaire de médias (l'activité logistique d'Amazon n'est donc pas comptabilisée). Le nombre d'acteurs français positionnés sur le segment de la plateforme en ligne étant limité, seule la société Dailymotion a été incluse dans l'analyse.

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.

**CHIFFRE D'AFFAIRES RÉALISÉ EN FRANCE PAR LES PLATEFORMES EN LIGNE**

| Plateforme | Chiffre d'affaires (M€) | Nombre de salariés | Ratio chiffre d'affaires / salariés (M€) |
|---|---|---|---|
| Google France | 1 747 | 971 | 1,8 |
| Facebook France | 1 022 | 389 | 2,6 |
| Amazon online France SAS | 983 | 205 | 4,8 |
| Tiktok France | 78 | 263 | 0,3 |
| Linkedin France | 65 | 159 | 0,4 |
| Dailymotion | 54 | 239 | 0,2 |
| Twitter France | 9 | 24 | 0,4 |

*Source : DGFIP, réponse aux questionnaires de la rapporteure.*

*(1) Les services marchands en 2024,* Insee Documents de travail, n° 2025-14, juin 2025 https://www.insee.fr/fr/statistiques/8596787

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.

### 3. Cloud : OVH, un chiffre d'affaires comparable à celui des *hyperscalers*, dans un modèle d'affaires opposé

Le secteur du cloud, hors logiciels SaaS, est très concentré. Le tableau ci-dessous compare les chiffres d'activité des *hyperscalers* à ceux des acteurs français du cloud. Les chiffres de l'activité cloud de Microsoft ne sont pas disponibles, car non isolés au sein de l'activité de Microsoft France.

**COMPARAISON DE L'ACTIVITÉ DES ACTEURS FRANÇAIS ET AMÉRICAINS DU CLOUD SUR LE PÉRIMÈTRE 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 [(1)] ; pour Outscale, comptes sociaux [(2)] ; pour AWS, GCD et OVH, DGFiP (réponse aux questionnaires de la rapporteure).*

Ces éléments montrent que les sociétés AWS et Google cloud réalisent, sur le périmètre de la France, des chiffres d'affaires encore très supérieurs à ceux des acteurs français. OVH constitue un cas à part, du fait de son modèle intégrant la maîtrise de la chaine de production (conception production, maintenance, réutilisation, recyclage) et la gestion opérationnelle des data centers, qui se retrouve dans le nombre de salariés (plus de 2 000). OVH et Scaleway ne réalisent pas de bénéfices qui pourraient être réinvestis dans l'activité.

Sur les trois segments étudiés, l'édition de logiciels, le cloud et les plateformes en ligne, les chiffres disponibles confirment la différence de taille entre les entreprises leaders mondiales et les acteurs français. Parmi ces derniers, peu atteignent le volume d'activité réalisé par les Gafam sur leur seul périmètre français.

*(1) Communication financière du groupe Iliad, avril 2026, Iliad URD 2025*

*(2) Comptes annuels 2025, avril 2026, Outscale - Comptes sociaux 2025 29-05-2026.pdf*

## B. FAIBLE VALEUR AJOUTÉE, RECETTES FISCALES MINIMES : LES CONSÉQUENCES D'UNE ACTIVITÉ OFFSHORE

### 1. Un taux de valeur ajoutée très bas, témoignant de la contribution réduite des Gafam à l'activité économique nationale

La rapporteure a souhaité mesurer la valeur ajoutée de l'activité réalisée en France pour mesurer leur contribution réelle à l'économie. À partir des chiffres transmis par la DGFIP sur les entreprises Microsoft, Google, Amazon, Facebook et Oracle, une estimation de la valeur ajoutée (VA) a été calculée de la façon suivante :

Valeur ajoutée = Total du chiffre d'affaires généré en France (y.c. pour les exportations) – Autres achats et charges externes ou achats de marchandises. L'estimation de valeur ajoutée ainsi calculée a été comparée aux chiffres agrégés du secteur en 2022 fournis par l'Insee (1). Ces éléments sont repris dans le tableau ci-après.

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

(*) Catégorie Edition de logiciels.

(**) Catégorie Traitement des données, hébergement et activités connexes, portail.

Pour l'ensemble des sociétés identifiées, le taux de valeur ajoutée est bien plus faible que la moyenne du secteur, notamment pour Microsoft (18 % contre 49 % en moyenne dans l'édition de logiciels), Facebook et Amazon online (19 % et 9 % contre 42 % en moyenne pour l'activité de traitement de données). Par comparaison, ces taux sont de 65 % pour Outscale et 42 % pour OVH.

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.

(1) *Insee,* Activité économique des entreprises du secteur du numérique, *octobre 2025,* https://www.insee.fr/fr/statistiques/8616853?sommaire=8616883

### 2. Des recettes d'impôt sur les sociétés très faibles compensées par l'existence de la taxe sur les services numériques

La rapporteure a souhaité disposer d'informations sur les retombées fiscales tirées de l'imposition des filiales des entreprises américaines du secteur du numérique. Ces informations lui ont été transmises par la DGFIP au titre des pouvoirs qui sont conférés au rapporteur d'une commission d'enquête.

Dans le respecter du secret fiscal, la rapporteure présente non pas des chiffres individualisés mais un ratio entre le montant d'impôt des sociétés acquitté et le chiffre d'affaires.

**RECETTES FISCALES GÉNÉRÉES PAR LES ENTREPRISES AMÉRICAINES DU SECTEUR DU NUMÉRIQUE**

| | Impôt sur les sociétés / chiffre d'affaires |
|---|---|
| **Cloud** | 0,7 % |
| **Plateformes** | 1,0 % |
| **Logiciels** | 2,0 % |

Elle tire les constats suivants des éléments recueillis :

– **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.

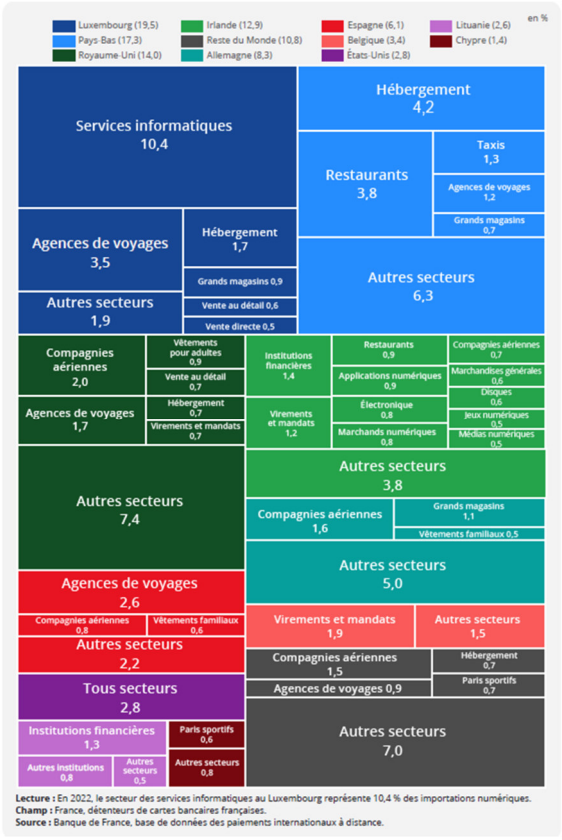
– le taux de contribution des entreprises de logiciels est plus élevé que celui des acteurs des deux premières catégories.

### 3. Le rôle joué par l'Irlande et le Luxembourg

La Banque de France a mené une étude sur la consommation en ligne des ménages français à partir des données de paiement par carte bancaire [(1)]. Cette étude permet de **quantifier l'activité économique générée par les plateformes de commerce en ligne localisées à l'étranger, autrement dit les importations numériques.** L'étude de la Banque de France **fait ressortir l'importance prise par quelques États membres, dont l'activité d'exportation de services numériques traduit l'implantation de sièges sociaux européens de grandes plateformes mondiales**. Ainsi que l'indique l'étude, « *le siège d'Airbnb et le siège européen d'Amazon se trouvent au Luxembourg, ceux de Meta et Google à Dublin en Irlande et ceux de Booking.com et d'Uber à Amsterdam* ». Le graphique ci-dessous illustre la part de chaque pays dans les importations numériques françaises.

*(1) NUM25.pdf , Le Commerce numérique et les consommateurs français dans la mondialisation, p. 28 et sq.*

**RÉPARTITION DES IMPORTATIONS NUMÉRIQUES EN FRANCE PAR PAYS ET SECTEUR (2022)**




*Source : Banque de France, base de données des paiements internationaux à distance.*

**Le Luxembourg représente à lui seul 19,5 % du volume total des importations numériques françaises**, dont 10,4 % pour les services informatiques. Cette sous-catégorie, dont on peut supposer qu'elle est fortement liée à l'activité d'Amazon en France, représente à elle seule un montant d'activité de 5,6 milliards d'euros.

L'étude du cabinet Asterès « La dépendance technologique aux software et cloud services américains : une estimation des conséquences économiques en Europe » [(1)] montre que sur les 25,7 milliards d'euros d'importations françaises dans le domaine du numérique (*computer services)* comptabilisées par l'OMC, 7,4 milliards proviennent d'Irlande et 2,4 milliards des États-Unis.

---

*(1) Asterès,* La dépendance technologique aux softwares & cloud services américains : une estimation des conséquences économiques en Europe*, avril 2025*
*https://www.cigref.fr/la-dependance-technologique-aux-softwares-cloud-services-americains-une-estimation-des-consequences-economiques-en-europe*

**Ces chiffres témoignent d'un modèle dans lequel l'essentiel de la valeur ajoutée est localisée offshore.** La société Microsoft France SAS agit par exemple comme un agent commercial, et non comme une société de développement logiciel à proprement parler : « *La société Microsoft France SAS a une activité d'agent commercial des sociétés Microsoft Ireland Opération Ltd (MIOL) et Microsoft Corporation, pour ses activités de représentation commerciale, de promotion et de supports techniques, réalisées sur le territoire français. À ce titre, Microsoft France perçoit des commissions, dont le mode de calcul n'a pas été modifié au cours de l'exercice. Ces commissions sont calculées selon les termes des contrats signés avec Microsoft Ireland Operation Ltd (MIOL) et Microsoft Corporation en France. Cette rémunération correspond à la refacturation de la totalité des coûts, complétés par un pourcentage des ventes réalisées par MIOL et Microsoft Corporation sur le territoire français. Depuis Février 2017, l'activité principale de Microsoft France a été étendue pour inclure la distribution en direct de logiciels et de matériel informatique sur le territoire français. Microsoft France exerce cette activité dans le cadre d'un modèle de "Distributeur à risque limité", dont les termes sont définis dans un accord de distribution et de services inter-sociétés signé avec MIOL.* » (1)

Concernant Facebook France, « *l'activité de la société au cours de l'année 2024 a été de : fournir un soutien aux ventes, des services de marketing et un soutien technique au groupe Meta, vendre des espaces publicitaires auprès de certains clients français.* » (2)

Enfin, le modèle économique est sensiblement le même pour Google France : « *Le revenu correspond au montant des frais payés en respect des prestations de services réalisées pendant l'année à Google Ireland Limited et à Google LLC. Depuis novembre 2022, la société a conclu un autre accord de service avec Google Ireland Limited, et, en vertu de cet accord, elle génère des revenus provenant de la revente et d'autres services d'assistance liés à la publicité sur les propriétés de Google ou sur les propriétés des membres du réseau Google. L'entreprise comptabilise les revenus de la vente de publicité en tant que revenus de tiers dans le compte de résultat »,* même s'il convient de noter que : *« Dans le cadre de son contrat avec Google LLC, Google France réalise une activité de recherche et développement en France. Ces dépenses en 2024 ont été comptabilisées pour un montant de €148,770,639 vs €152,024,247 en 2023.* » (3)

*(1) Microsoft, Comptes annuels 2024*

*(2) Facebook France, Comptes annuels 2024*

*(3) Google France, Comptes annuels 2024*

### C. LES DÉPENSES DE LOGICIELS : 1,5 MILLIARD D'EUROS PAR AN AU PROFIT DES ACTEURS EXTRA-EUROPÉENS, 1 MILLIARD DE DÉPENSES SUBSTITUABLES DÈS AUJOURD'HUI

En avril 2025, le cabinet Asterès publiait une étude remarquée pour le compte du Cigref, qui concluait que les entreprises américaines représentaient 80 % des achats de cloud-logiciel en France [(1)]. Aucune étude similaire n'avait été conduite pour les administrations.

Combien l'État dépense-t-il chaque année en licences auprès de Microsoft ? Quelle est la part des logiciels américains dans les achats des administrations ? Aussi simples que soient ces questions, aucun chiffre, ne serait-ce qu'estimatif, n'existait avant le démarrage de cette commission d'enquête.

Afin d'établir un diagnostic étayé, la commission d'enquête a souhaité disposer d'informations précises sur les montants dépensés par les administrations publiques pour l'achat de licences logiciels, et a ainsi collecté des données par trois canaux différents :

– les réponses aux questionnaires adressés directement aux administrations sollicitées. Ces dernières devaient lister dans un tableau les dépenses de développement et de maintien en conditions opérationnelles de leurs applications métiers ainsi que les dépenses de licences de leurs logiciels support ;

– un recensement effectué par le gouvernement dans le temps de la commission d'enquête, avec l'appui de l'Ugap, de la Dinum et de la direction des achats de l'État (DAE) ;

– les chiffres des achats réalisés par l'Ugap pour le compte des administrations publiques.

Ces trois sources ont ainsi permis de disposer de la vision la plus consolidée possible des achats effectués et de la part des logiciels extra-européens dans les solutions déployées au sein des administrations publiques.

#### 1. Dépenses de l'État dans le domaine du numérique : vision globale

Le recensement opéré par le gouvernement couvre un montant agrégé de 2,3 milliards d'euros, inférieur au montant des dépenses numériques de l'État déclaré par les différentes personnes auditionnées par la commission d'enquête (4,2 milliards). Ce recensement n'est donc pas exhaustif, mais donne toutefois une vision globale de la répartition des achats par poste de dépense et de la part des fournisseurs extra-européens sur chacun des postes.

*(1) Asterès, ibid.*

**POSTES DE DÉPENSES NUMÉRIQUES DES ADMINISTRATIONS ET PART DES FOURNISSEURS EXTRA-EUROPÉENS**

| Poste de dépenses | Montant annuel | Part des fournisseurs extra-européens |
|---|---|---|
| Études informatiques et conseil en urbanisation | 981 | 19 % |
| Prestations de développement et maintenance informatique | 750 | 23 % |
| Logiciels pour les DSI | 219 | 64 % |
| Logiciels pour l'environnement de travail | 142 | 90 % |
| Logiciels de cybersécurité | 103 | 24 % |
| Cloud | 93 | 1 % |
| Logiciels et services d'IA | 10 | 59 % |

*Source : Ministère de l'action et des comptes publics et ministère délégué chargé de l'intelligence artificielle et du numérique*

Le tableau ci-dessus montre que les principales dépenses réalisées concernent les prestations d'assistance à maîtrise d'ouvrage et de conseil (981 millions) et les prestations de développement et de maintenance informatique (750 millions). Pour ces deux postes, la dépendance aux fournisseurs extra-européens est faible (respectivement 19 % et 23 %). Ces chiffres rejoignent les constats réalisés précédemment : le développement d'applications à façon et le maintien en conditions opérationnelles des systèmes sont les principales sources de dépense des administrations. Or, ces activités sont réalisées par des entreprises de services du numérique (ESN) principalement localisées en France. Néanmoins cela ne prend pas en compte l'intégration potentielle de technologies extra-européennes dans les produits développés par les ESN.

Concernant les dépenses de logiciels, bien que les montants soient moins importants, le constat d'une prédominance des fournisseurs extra-européens se confirme. Cette part est de 64 % pour les logiciels pour les directions des systèmes d'information (DSI) et de 90 % pour les logiciels pour l'environnement de travail (bureautique et systèmes d'exploitation).

Au total, les fournisseurs extra-européens représentent une part minoritaire de l'ensemble des achats réalisés (29 % sur le périmètre considéré, soit une dépense annuelle de 658 millions d'euros), mais occupent une position très forte sur le segment des logiciels support.

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

#### *a. Données des administrations d'État*

L'estimation des dépenses de logiciels des administrations publiques d'État repose sur deux sources :

– les réponses aux questionnaires recueillies par la rapporteure. Le périmètre est celui des administrations d'État, auquel s'ajoutent quatre établissements publics à caractère administratif (France Travail, la Cnam, la Cnav et la CAF) et l'AP-HP, établissement public de santé. Ce périmètre n'est pas exhaustif mais couvre les principales administrations opérant les services publics

nationaux. Certaines administrations sollicitées ont toutefois transmis des chiffres selon des périmètres incomplets (ministère de l'intérieur : direction générale de la police nationale uniquement) ;

– les chiffres transmis par la Dinum sur les achats publics ; ils comptabilisent les dépenses réalisées auprès de l'Ugap ou renseignées dans le logiciel Chorus. Le périmètre, qui couvre exclusivement les administrations et exclut les opérateurs de l'État, est donc moins large que celui couvert par la commission d'enquête.

Les dépenses de logiciels reflètent les dépendances techniques constatées. 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 sur le périmètre de la commission d'enquête (98 millions sur le périmètre Dinum).

Les solutions VMWare et Oracle représentent une dépense de 34,1 et 23,1 millions d'euros (respectivement 22 et 32 millions au périmètre Dinum). Moins généralisés, Red Hat et IBM représentent néanmoins 17,1 et 12,6 millions d'achats en 2025. Le constat d'une dépendance critique à des solutions extra-européennes est corroboré par les chiffres d'achats, ces fournisseurs étant d'origine américaine.

Parmi les sept plus gros fournisseurs des administrations, les européens SAP (Allemagne) et Sopra HR (France) sont également des fournisseurs de premier plan pour les solutions de gestion du SIRH et de la comptabilité.

## DÉPENSES DE LOGICIELS AUPRÈS DES PRINCIPAUX FOURNISSEURS DES ADMINISTRATIONS NATIONALES

| En M€ | Microsoft Syst. exploitation | | Microsoft Suite bureautique | | Total Microsoft | | | Oracle | | | VM Ware | | | SAP | | Red Hat | | | SOPRA HR | | IBM | | | Total | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2025 | Moy 2023 - 2025 | 2025 | Moy 2023 - 2025 | 2025 | Moy 2023 - 2025 | DINUM 2025 | 2025 | Moy 2023 - 2025 | DINUM 2025 | 2025 | Moy 2023 - 2025 | DINUM 2025 | 2025 | Moy 2023 - 2025 | 2025 | Moy 2023 - 2025 | DINUM 2025 | 2025 | Moy 2023 - 2025 | 2025 | Moy 2023 - 2025 | DINUM 2025 | 2025 | Moy 2023 - 2025 |
| **Ministères sociaux** | | | | | | | | | | | | | | | | | | | - | - | - | - | | 3,7 | 4,7 |
| **MAASA** | | | | | | | | | | | | | | | | | | | - | - | - | - | | 0,9 | 0,8 |
| **AP-HP** | | | | | | | | | | | | | | | | | | | | | - | - | | 23,1 | 19,3 |
| **MEF** | | | | | | | | | | | | | | | | | | | | | | | | 41,0 | 38,8 |
| **CNAF** | | | | | | | | | | | | | | | | | | | - | - | | | | 11,5 | 3,8 |
| **CNAV** | | | | | | | | | | | | | | | | | | | | | | | | 17,0 | 6,0 |
| **CNAM** | | | | | | | | | | | | | | | | | | | | | | | | 23,2 | 12,0 |
| **CULTURE** | | | | | | | | | | | | | | | | | | | - | - | - | - | | 3,4 | 1,9 |
| **DEFENSE** | | | | | | | | | | | | | | | | | | | - | - | - | - | | 28,1 | 28,2 |
| **MTE** | | | | | | | | | | | | | | | | | | | - | - | - | - | | 1,5 | 1,5 |
| **Edu Nat** | | | | | | | | | | | | | | | | | | | | | | | | 9,5 | 10,1 |
| **Gend nat** | | | | | | | | | | | | | | | | | | | - | - | - | - | | 1,0 | 0,8 |
| **Justice** | | | | | | | | | | | | | | | | | | | - | - | - | - | | 40,3 | 28,5 |
| **MEAE** | | | | | | | | | | | | | | | | | | | - | - | - | - | | 3,5 | 2,8 |
| **Intérieur - DGPN** | | | | | | | | | | | | | | | | | | | | | - | - | | 19,4 | 17,8 |
| **France Travail** | | | | | | | | | | | | | | | | | | | - | - | - | - | | 16,8 | 11,6 |
| **Total** | **45,8** | **34,5** | **66,3** | **49,1** | **115,3** | **86,3** | **98** | **23,1** | **19,6** | **32** | **34,1** | **27,6** | **22** | **28,7** | **24,4** | **17,1** | **12,5** | **15** | **13,0** | **10,5** | **12,6** | **7,5** | **8** | **244,0** | **188,0** |

| *< 1 million (M€)* | *[ 1 M€ - 4 M€ ]* | *[4 M€ - 7 M€ ]* | *[7 M€ – 10 M€ ]* | *[ 10 M€ - 15 M€ ]* | *> 15 M€* |
|---|---|---|---|---|---|

*Source : réponses aux questionnaires, DINUM.*

### *b. Ensemble du secteur public*

Par son positionnement auprès de l'ensemble des administrations, l'Ugap dispose d'une vision panoramique des achats numériques. Lors de son audition devant la commission d'enquête, M. Edward Jossa, président de l'Ugap, dressait un tableau plutôt optimiste de la pénétration des logiciels souverains dans les achats publics, qui serait dû notamment aux efforts de son organisation pour les promouvoir : « *Nous travaillons sur les outils de distribution. Avant même les commissions d'enquête, nous avons créé un arbre de choix numériques qui permet d'identifier les solutions souveraines, notamment sur le marché cloud. Sur les logiciels, nous avons complété des fiches produit de logiciels pour indiquer si les éditeurs sont de nationalité française – au sens de leur présence en France, y compris la maison mère. Nous travaillons actuellement sur un outil d'intelligence artificielle d'aide à la décision pour que les clients puissent voir le logiciel qui correspond le mieux à leurs besoins. Les questions de sensibilité des données et de souveraineté seront bien sûr abordées.*

« *Quels sont les résultats de cette politique ? Sur le marché des multi-éditeurs, nous sommes passés de 2 150 à 2 700 éditeurs français et de 224 à 294 pour les autres éditeurs de l'Union européenne – ils comptent aussi en matière de souveraineté. Ce qui est important, c'est peut-être le volume des ventes : en volume, entre 2024 et 2025, nous sommes passés de 595 millions de ventes à 668 millions, et de 54 millions à 64 millions pour les Européens non français. S'agissant des logiciels, nous vendons des solutions souveraines à hauteur de 723 millions d'euros, soit 55,5 % des ventes totales de logiciels de l'Ugap – Microsoft et Oracle compris. Nous vendons du souverain, mais nous avons une croissance constante et régulière des ventes de logiciels non souverains.* »

M. David Amiel, ministre de l'action et des comptes publics, reprenait ces chiffres à son compte : « *54 % des commandes publiques de logiciels passées en 2025 par l'État et les collectivités par l'intermédiaire de l'Ugap – c'est donc un périmètre plus vaste que celui des 4,2 milliards d'euros – concernaient des éditeurs français ou européens.* » (1)

Les pourcentages de 55,5 % (audition de M. Jossa) et 54 % (audition de M. Amiel) étant en décalage avec l'étude menée par le cabinet Asterès pour le compte du Cigref, et, de manière générale, avec les constats qualitatifs convergents des auditions, la rapporteure a souhaité disposer d'informations plus précises sur le calcul de ce pourcentage.

Lorsqu'il s'est agi de fournir les détails du calcul, l'Ugap a fait valoir des erreurs de méthodologie dans la classification des nationalités des fournisseurs. La centrale d'achat a dû procéder à des traitements manuels pour corriger des

*(1) Audition commune, ouverte à la presse, de M. David Amiel, ministre de l'action et des comptes publics, et de Mme Anne Le Hénanff, ministre déléguée auprès du ministre de l'économie, des finances et de la souveraineté industrielle, énergétique et numérique, chargée de l'intelligence artificielle et du numérique, 20 mai 2026.*

incohérences identifiées. Certains éditeurs de logiciel étaient ainsi considérés à tort comme européens car la tête de groupe internationale était localisée en Europe (Irlande), alors qu'une analyse plus fine et manuelle révélait que les sociétés étaient bien des filiales d'entreprises non européennes.

Quel est le résultat final des calculs ?

Nous ne disposons finalement pas d'un chiffre global pour l'ensemble des achats logiciels de l'Ugap. Compte tenu de l'imprécision de la classification automatique par nationalité des éditeurs, cette information est disponible seulement pour les seuls cinquante plus gros fournisseurs de logiciels.

Le tableau ci-dessous présente les dix fournisseurs de logiciels les plus importants en termes de chiffre d'affaires réalisé. **Microsoft se situe en première 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 de chiffre d'affaires. Parmi les dix principaux fournisseurs, huit sont américains et deux sont français : Docaposte et Cegid (actionnaire français, mais la tête de groupe est localisée au Luxembourg).

**DIX PRINCIPAUX FOURNISSEURS DE LOGICIELS PAR MONTANT DE CHIFFRE D'AFFAIRES RÉALISÉ AUPRÈS DE L'UGAP (2025)**

| En M€ | Ministères | Collectivités territoriales | Établissements publics | Santé | Caisses et entreprises | Total |
|---|---|---|---|---|---|---|
| MICROSOFT | 85 | 87 | 50 | 0 | 71 | 293 |
| ORACLE | 4 | 32 | 7 | 2 | 23 | 69 |
| VMWARE FRANCE | 18 | 3 | 19 | 3 | 20 | 62 |
| RED HAT INC | 13 | 1 | 1 | 0 | 10 | 25 |
| SALESFORCE | 6 | 1 | 8 | 0 | 7 | 22 |
| BUREAU VAN DIJK EDITIONS | 15 | 0 | 0 | 0 | 0 | 15 |
| ADOBE | 3 | 6 | 3 | 1 | 1 | 15 |
| PEGASYSTEMS FRANCE | 0 | 0 | 12 | 0 | 3 | 14 |
| DOCAPOSTE | 4 | 2 | 5 | 0 | 1 | 12 |
| CEGID | 2 | 3 | 2 | 0 | 4 | 11 |
| Autres fournisseurs | 214 | 211 | 223 | 49 | 98 | 795 |
| Total | 363 | 346 | 330 | 56 | 239 | 1 333 |

Les deux tableaux ci-après présentent les résultats pour les cinquante fournisseurs de logiciels les plus importants en termes de chiffre d'affaires réalisé pour les années 2024 et 2025.

**PART DES ACHATS DE LOGICIELS PAR NATIONALITÉ DU FOURNISSEUR RÉALISÉS AUPRÈS DE L'UGAP - TOP 50 FOURNISSEURS**

| | États-Unis | | France | | Autres | | Total |
|---|---|---|---|---|---|---|---|
| | M€ | % | M€ | % | M€ | % | |
| 2024 | 507 | 81 % | 82 | 13 % | 35 | 6 % | 624 |
| 2025 | 609 | 79 % | 127 | 17 % | 33 | 4 % | 770 |
| Croissance 2025/2024 | 20 % | | 17 % | | 4 % | | |

Note : les chiffres prennent en compte les achats réalisés auprès des 50 principaux fournisseurs en termes de chiffre d'affaires réalisé auprès de l'Ugap.

**Sur le périmètre des cinquante principaux fournisseurs, les seuls pour lesquels nous disposons 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 Asterès**.

Peut-on en déduire un chiffre pour l'ensemble des achats réalisés par l'Ugap pour le compte des administrations ? En faisant l'hypothèse, très conservatrice, qu'aucun fournisseur hors du Top 50 n'était américain, on aboutirait à une part dans le total des achats de l'Ugap de 46 %. Avec une hypothèse raisonnable de 50 % (1), cette part serait de 73 %.

Quant aux fournisseurs français, leur chiffre d'affaires auprès de l'Ugap est bien en forte augmentation. **Toutefois, au vu des chiffres disponibles pour le Top 50 (17 %), il est fort probable que les pourcentages de 54 et 55,5 % mentionnés par M. Jossa et M. Amiel lors des auditions soient erronés**.

### 3. 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. Ce choix pose triplement question au regard du bon usage des deniers publics :

– les achats réalisés contribuent-ils à soutenir les acteurs français et européens du numérique ?

– dans quelle mesure le paiement de ce type de licences est-il évitable, grâce à l'utilisation de logiciels libres de droit ?

– les choix de logiciels effectués conduisent-ils à des situations de *vendor lock-in*, c'est-à-dire de dépendance à des solutions propriétaires, dans lesquelles les fournisseurs seraient à même de dicter leurs conditions commerciales ?

*(1) Le recensement auprès des administrations d'État a fait apparaître un nombre important de fournisseurs américains en complément des principaux identifiés, pour des solutions de cybersécurité, etc.*

### *a. Montant des dépenses logicielles des administrations au profit des acteurs extra-européens : tentative d'estimation globale*

Ainsi que la rapporteure l'a expliqué précédemment, les dépenses de logiciel constituent le principal poste de dépendance à des acteurs extra-européens. Pour les administrations d'État, en 2025, ces dépenses sont estimées à :

– 244 millions d'euros sur le périmètre des administrations sollicitées par la commission d'enquête, dont 202 millions auprès de fournisseurs américains (83 %) [(1)] ;

– 361 millions d'euros d'après le recensement du gouvernement, dont 268 millions auprès de fournisseurs extra-européens (74 %) [(2)] ;

**Pour l'ensemble des administrations (incluant les collectivités territoriales, les établissements publics et les établissements de santé)**, les seuls chiffres disponibles sont ceux de l'Ugap. Ces données ne permettent pas un chiffrage exhaustif puisqu'il existe d'autres centrales d'achat davantage tournées vers les collectivités comme la Centrale d'achat du numérique et des télécoms (Canut), ou vers les établissements de santé comme l'Union des hôpitaux pour les achats (UniHA). Ils permettent cependant de donner une tendance, c'est-à-dire d'illustrer l'importance des dépenses auprès des acteurs non-européens. De plus, l'Ugap a communiqué à la rapporteure une estimation de sa part de marché sur le segment des achats de logiciels pour les administrations. En 2024, l'Ugap a enregistré 1,174 milliard d'euros de commandes dans les logiciels, pour une taille de marché estimée à 2,950 milliards d'euros par l'entreprise Exaegis, soit **une part de marché pour l'Ugap qui peut être estimée à 40 %.**

Le montant des achats via l'Ugap auprès des entreprises américaines en 2025 était au minimum de 609 millions d'euros après vérification manuelle de la nationalité des groupes présents dans le top 50 des fournisseurs, soit 79 %. **Considérant que la part de marché de l'Ugap représente 40 %, on peut estimer le montant minimal d'achats auprès des entreprises américaines à 1,5 milliard d'euros environ.**

### *b. Montant des dépenses logicielles substituables*

Les principales solutions achetées disposent d'alternatives en open source, au moins partielles. Les réponses aux questionnaires des administrations et des opérateurs font ainsi état de transitions engagées ou en réflexion vers les solutions suivantes :

– pour les solutions de bureautique : les solutions libres de type LibreOffice, ou les produits développés par la Dinum ;

---

*(1) Ces chiffres couvrent les sept principaux fournisseurs uniquement, les autres fournisseurs n'ont pas été comptabilisés en raison d'un trop grand nombre de références différentes.*

*(2) Chiffre obtenu par moyenne pondérée.*

– pour les systèmes d'exploitation : le système d'exploitation Linux ;

– pour la virtualisation (VMWare) : les solutions Openstack, Proxmox ou Kubernetes :

– pour la gestion de bases de données (Oracle, IBM) : PostgreSQL, Tomcat.

Ces solutions alternatives couvriraient une grande part des achats en volume auprès des principaux fournisseurs extra-européens. Les dépenses annuelles additionnées de licences pour les produits Microsoft, Oracle, VMWare et IBM s'élèvent à :

– 160 millions d'euros d'après le recensement du gouvernement ;

– 185 millions d'euros sur le périmètre des administrations sollicitées par la commission d'enquête ;

– 423 millions d'euros sur le périmètre des achats de l'Ugap, couvrant tous types d'acteurs publics

– **1 060 milliards d'euros pour l'ensemble des achats des administrations publiques,** en faisant l'hypothèse que la structure des achats de l'Ugap est représentative de celle de l'ensemble des achats de l'administration.

**DÉPENSES AUPRÈS DES FOURNISSEURS EXTRA-EUROPÉENS – TABLEAU DE SYNTHÈSE**

*(en M€)*

| Source | Périmètre et source | Dépenses 2025 | Part extra – UE total | Part extra – UE principaux fournisseurs | Part substituable |
|---|---|---|---|---|---|
| Commission d'enquête | Administrations d'État + France Travail, Cnav, Cnaf, AP-HP. 7 principaux fournisseurs uniquement | 244 | | 202 (83 %) des 7 principaux fournisseurs | 185 |
| Gouvernement | Ministères. Dépenses de logiciels « pour les DSI » et « environnement de travail » | 361 | 268 (74 %) | | 160 |
| Ugap | Achats logiciels Ugap | 1 333 | | 609 sur 769 (79 %) pour le top 50 fournisseurs | 423 |
| Extrapolation Ugap | Ensemble des administrations à partir de taille de marché de l'UGAP | 3 300 | | 1 500 | 1 060 |

*Note : la part substituable est définie ici comme l'addition des dépenses pour des solutions fournies par Microsoft, VMWare, Oracle, et IBM, pour lesquelles des solutions de substitution ont été expressément identifiées lors des auditions.*

Les témoignages des directeurs de l'Anfsi et de la DGFIP fournissent une vision complémentaire.

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,

dont 0,7 million pour la solution SAP. La commission d'enquête a auditionné le directeur de l'Anfsi, afin de disposer d'éléments sur les économies réalisées grâce au basculement vers des solutions open source. **Elles sont estimées à 534 millions en cumulé depuis 2004**.

« *[Sur] le plan financier, nous avons évalué les économies générées par cette stratégie, qu'il s'agisse des postes de travail ou de nos smartphones professionnels, équipés d'un système d'exploitation souverain. Ce choix technique nous protège d'ailleurs efficacement : les téléphones des directeurs généraux de la gendarmerie et de la police nationales ont ainsi été préservés de l'infiltration par le logiciel Pegasus. Depuis 2004, ces dépenses évitées s'élèvent précisément à 534 millions d'euros. Dans un contexte de budgets contraints, c'est un argument de poids.* » (1)

Le basculement vers des solutions open source entraîne des coûts de gestion de projet, au moment de la migration, et est susceptible d'accroître les besoins en main-d'œuvre en phase d'exploitation. En effet, les solutions ne sont généralement pas intégrées entre elles, et les services supports moins disponibles. Il conviendrait ainsi de vérifier que ces dépenses évitées comprennent bien les surcoûts associés.

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. Ainsi, pour la DGFIP, l'économie générée est de l'ordre de 10 millions par an. Selon le chef du service des systèmes d'information, « *bien que nous n'ayons pas réalisé d'étude sur les coûts évités grâce au logiciel libre, l'exemple de LibreOffice est révélateur puisque son coût annuel est quasi nul là où une suite propriétaire reviendrait à environ 10 millions d'euros par an. Pour un usage courant, nos enquêtes annuelles de satisfaction révèlent que les agents jugent ces deux solutions équivalentes* » (2).

Selon les estimations de la DSI du CNRS, la migration des solutions Microsoft vers des solutions open source pour les espaces collaboratifs permettrait également de réaliser des économies significatives. *« Pour le CNRS, cela représente environ 2,5 millions d'euros annuels uniquement pour la partie espaces collaboratifs SharePoint. Pour la messagerie, c'était, de mémoire, 3 millions d'euros annuels. En basculant chez Renater, cela nous coûtera 600 000 euros par an. Économiquement, il est extrêmement avantageux de passer sur du libre pour ces sujets.* » (3)

**Les dépenses de logiciel pour des produits propriétaires extra-européens représentent un montant annuel de l'ordre de 200 à 300 millions**

---

*(1) Audition du général de corps d'armée Marc Boget, directeur de l'agence du numérique des forces de sécurité intérieure (Anfsi), 7 mai 2026.*

*(2) Audition de M. Tomasz Blanc, chef du service des systèmes d'information de la direction générale des finances publiques (DGFIP), 7 mai 2026.*

*(3) Audition de Mme Marie-Pierre Fontanel, directrice des systèmes d'information du Centre national pour la recherche scientifique (CNRS), le mercredi 1er avril 2026.*

**d'euros pour les administrations d'État et les grands établissements publics, et de 1,5 milliard pour l'ensemble des administrations.**

**Les travaux de la commission le montrent, des solutions de substitution open source existent dans la très grande majorité des cas. 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.**

Comme cela a été mentionné précédemment, ces chiffres croisent des recensements effectués sur des périmètres différents, aucun d'entre eux n'étant exhaustifs. Une analyse approfondie devrait être conduite afin de disposer d'un recensement exact de l'utilisation des solutions propriétaires. De plus, pour disposer d'une vision complète permettant de calculer le retour sur investissement d'un basculement vers le logiciel libre, les économies potentielles de coûts de licence devraient être mises en regard des coûts supplémentaires liés à la migration : coûts initiaux et coûts de main-d'œuvre pour le fonctionnement.

**Au regard des économies substantielles qui pourraient être réalisées, ce travail est à réaliser par le gouvernement.**

### *c. Impact des choix de solutions logicielles sur la hausse des dépenses numériques des administrations*

La dépendance à des produits propriétaires rend les administrations vulnérables aux hausses tarifaires imposées par les fournisseurs dès lors que ces derniers sont en position de force : soit car dans de rares cas il n'existe aucune solution de substitution, soit parce que la transition vers une alternative est rendue longue ou coûteuse. Les travaux de la commission d'enquête montrent que de telles pratiques sont courantes.

**L'analyse de l'évolution des dépenses montre une hausse des dépenses de licences significative, bien au-dessus de l'inflation constatée dans les services.**

Le taux de croissance moyen des dépenses auprès des dix principaux fournisseurs de l'Ugap était de 74 %. Seul Oracle voit son chiffre d'affaires diminuer. Les dépenses en logiciels Microsoft sont en hausse de 26 %, celles pour les solutions VMWare sont multipliées par plus de deux (+ 113%).

**EVOLUTION DES DÉPENSES AUPRÈS DES 10 PRINCIPAUX FOURNISSEURS DE L'UGAP ENTRE 2024 ET 2025**

| Fournisseur | Chiffre d'affaires 2024 | Chiffre d'affaires 2025 | Taux de croissance |
|---|---|---|---|
| MICROSOFT | 233 | 293 | 26 % |
| ORACLE | 97 | 69 | – 29 % |
| VMWARE FRANCE | 29 | 62 | 113 % |
| RED HAT INC | 13 | 25 | 90 % |
| SALESFORCE COM FRANCE | 9 | 22 | 138 % |
| BUREAU VAN DIJK EDITIONS ELECTRONIQ | 5 | 15 | 201 % |
| ADOBE | 13 | 15 | 15 % |
| PEGASYSTEMS FRANCE | 6 | 14 | 150 % |
| DOCAPOSTE | 10 | 12 | 18 % |
| CEGID | 233 | 293 | 13 % |

*Source : Ugap.*

La commission d'enquête a examiné l'évolution des dépenses pour les six [(1)] principaux fournisseurs des administrations en comparant les dépenses 2025 à la moyenne des dépenses 2023 – 2025 [(2)].

D'après les chiffres transmis à la rapporteure par les administrations, les hausses constatées auprès des six principaux fournisseurs entre 2025 et la moyenne des dépenses 2023 – 2025 sont comprises entre +7 % (Oracle) et + 46 % (Red Hat). Concernant les dépenses Microsoft, les dépenses sont en augmentation de 27 % sur l'ensemble du périmètre considéré.

**EVOLUTION DES DÉPENSES AUPRÈS DES PRINCIPAUX FOURNISSEURS DES ADMINISTRATIONS**

| Fournisseur | Taux de croissance |
|---|---|
| MICROSOFT | 27 % |
| ORACLE | 7 % |
| VMWARE FRANCE | 37 % |
| RED HAT INC | 46 % |
| SOPRA HR | 24 % |
| SAP | 13 % |

*Source : réponses aux questionnaires.*

*Note : comparaison entre l'année 2025 et la moyenne des années 2023-2025.*

Ces hausses agrègent deux effets :

– une évolution du périmètre des services fournis, certains vendeurs accroissant les fonctionnalités offertes, tandis que d'autres voient leur champ d'action réduit ;

– des hausses des prix unitaires des services, de façon unilatérale ou à l'occasion de nouvelles versions ou encore de renégociation de contrats pluriannuels.

*(1) Les chiffres d'IBM ne sont pas analysés car non significatifs (impact très fort du contrat auprès de la Cnav).*

*(2) L'utilisation de la moyenne des trois dernières années permet de neutraliser l'effet des contrats pluriannuels qui exigent le versement en une année de plusieurs années de frais de licences.*

La frontière entre les deux est parfois poreuse, lorsque les éditeurs pratiquent le *bundling*, et imposent ainsi à leurs clients des fonctionnalités dont ils n'ont pas besoin.

Les fortes hausses de prix, liées aux pratiques tarifaires des principaux acteurs du logiciel, ont bien été mises en évidence lors de la table ronde réunissant les directeurs des systèmes d'information de quatre grands organismes de recherche publics, le CEA, l'Inserm, le CNRS et l'Inrae.

« *Côté CEA, nous venons de renégocier notre contrat Microsoft pour trois ans. L'ordre de grandeur est de 6 millions d'euros par an. Microsoft demande de ne pas communiquer sur les augmentations, mais je peux vous dire qu'entre le contrat précédent et celui-ci, l'augmentation est à deux chiffres, de l'ordre de 20 % sur trois ans, ce qui est bien supérieur à l'inflation. De plus, ils pratiquent la vente liée (bundle) en incluant des produits que nous n'utilisons pas. C'était le cas de Teams, que nous n'avons jamais déployé mais que nous étions obligés de payer. Une décision de la Commission européenne les a contraints à sortir Teams du lot, mais ils ne lui ont pas affecté son vrai prix. L'augmentation globale sur trois ans est bien supérieure au retrait de ce petit élément.*

« *L'autre éditeur qui nous a créé des difficultés est VMware, qui a été racheté par Broadcom. Les changements de prix ont été très significatifs et pèsent sur le budget de l'État* » [(1)].

« *Vous posiez la question des migrations auxquelles on pourrait renoncer à cause du coût. Je reprends l'exemple de VMware. Quand ils ont annoncé une augmentation de 50 % ou 60 % des coûts du jour au lendemain, nous nous sommes posé la question de changer. Mon DSI avait évalué le coût de l'accompagnement de la migration à 1 000 jours-hommes. Nous avons commencé à diversifier un peu nos solutions en introduisant une solution de virtualisation open source, car nous ne pouvions pas mettre tous nos œufs dans le même panier. Mais nous n'avons pas été capables d'absorber une migration complète du jour au lendemain et avons donc dû subir cette hausse de coût* » [(2)].

« *Côté CNRS, en revanche, ce n'est pas du tout en marche. Nous sommes entièrement sur VMware. Contrairement à nos collègues, nous n'avons pas subi d'augmentation lors du passage à Broadcom, car je pense que nous payions déjà le maximum. Une sortie de VMware au CNRS est inenvisageable à moyen terme, cela nous coûterait extrêmement cher. C'est un peu la même chose pour SAP, même si ce n'est pas un acteur américain. Sortir de SAP quand on l'utilise depuis vingt ans, avec des développements spécifiques, est extrêmement compliqué. Le verrouillage n'est pas lié qu'aux constructeurs américains* » [(3)].

---

*(1) Audition de M. Baptiste Grigy, directeur des systèmes d'information du Commissariat à l'énergie atomique et aux énergies alternatives (CEA), le 1er avril 2026.*

*(2) Audition de M. Damien Rousset, directeur général délégué à l'administration de l'Institut national de la santé et de la recherche médicale (Inserm), le 1er avril 2026.*

*(3) Audition de Mme Marie-Pierre Fontanel, directrice des systèmes d'information du Centre national pour la recherche scientifique (CNRS), le 1er avril 2026.*

Le constat est partagé par M. Thomas Jan, directeur général adjoint en charge de l'innovation et de la stratégie numérique de l'UniHA [(1)] : « *Le rachat de VMware par Broadcom en octobre 2024 a éveillé les consciences. Dans le secteur des établissements de santé, nous avons eu connaissance d'une proposition faite à un CHU (centre hospitalier universitaire) dont le prix, à besoins constants, avait augmenté non de 20 % mais de 800 %. Cet effet a été ressenti dans tous les secteurs. (…) Idem pour le contrat avec Microsoft : une augmentation de 20 % est malheureusement ce qu'on peut avoir avec un renouvellement tous les quatre ans.* »

Les chiffres agrégés comme les témoignages des DSI des administrations montrent que la **dépendance à des produits propriétaires installées au cœur des systèmes crée de fortes vulnérabilités économiques. Non seulement les dépenses en logiciels pourraient être évitées avec l'utilisation de solutions open source, mais elles sont en hausse en raison des pratiques commerciales des principaux fournisseurs des administrations.** L'ensemble des acteurs économiques sont également vulnérables à des hausses de prix unilatérales. Plus un produit propriétaire est intégré au fonctionnement d'une institution ou d'une entreprise plus cette vulnérabilité est grande.

### D. HAUSSES DES PRIX : UNE MENACE CROISSANTE POUR L'ENSEMBLE DES ENTREPRISES FRANÇAISES

Les phénomènes auxquels sont confrontées les administrations sont généralisables à l'ensemble des acteurs économiques. C'est la conclusion d'une étude menée par le cabinet Asterès pour le compte du Cigref [(2)].

L'étude effectue tout d'abord une revue de littérature, dont ressortent les éléments suivants :

– les logiciels sont le premier poste de contribution à la hausse des dépenses numériques mondiales entre 2020 et 2026 : ils représentent 40 % du total des hausses, contre 34 % pour les services IT, 21 % pour le hardware et 6 % pour les appareils ;

– les entreprises françaises sont confrontées à des hausses de tarif importantes, supérieures à l'inflation, et ces hausses peuvent être reliées aux stratégies de *vendor lock-in* des éditeurs de logiciel, consistant à proposer des prix de licence bas pour les premiers contrats pour imposer leurs solutions propriétaires et s'assurer ensuite des revenus récurrents : « *concernant les hausses de prix facial, l'enquête Vanson Bourne – Asterès, conduite en 2022, a révélé que près de 90 % des entreprises françaises étaient touchées, avec des hausses de 3 % à 6 % par an, selon l'hypothèse de durée du contrat, soit supérieures de plusieurs points à l'inflation. Ces résultats corroboraient les témoignages recueillis par le Pr. Jenny, selon lesquels les prix des licences des logiciels sont " initialement compétitifs "*

*(1) Table ronde sur les acheteurs publics, le 9 avril 2026.*

*(2) Asterès, « De la dépendance technologique à la captation économique : ce que les hausses tarifaires du cloud-logiciel coûtent à l'Europe », mai 2026.*

*mais presque systématiquement augmentés au moment du renouvellement (*vendor lock-in*)* ».

– prises dans des négociations déséquilibrées, les entreprises clientes se voient imposer des fonctionnalités non désirées via des offres groupées, qui contribuent à la hausse constatée des tarifs :

« *Concernant les ventes groupées, l'enquête Vanson Bourne – Asterès, conduite en 2022, a révélé que 70 % des entreprises françaises s'étaient déjà vues proposer une offre groupée, avec un différentiel de coût de 26 % en moyenne et pouvant atteindre jusqu'à 80 % pour certains répondants. Ces résultats sont confortés par l'analyse du Pr. Jenny qui, en analysant les politiques de licence de certains fournisseurs, a quantifié des majorations pouvant atteindre 90 % pour Office 365 et 300 % pour SQL Server, ainsi que par celle du cabinet Elée, qui illustre ce type de pratique avec l'exemple de VMWare : « la fusion de milliers de références en une centaine de packs a provoqué des hausses brutales, régulièrement supérieures à 40 %, et parfois jusqu'au double* ».

Le cabinet Asterès dévoile ensuite les résultats d'une enquête réalisée auprès de 54 entreprises et administrations publiques françaises, belges et néerlandaises, membres ou partenaires du Cigref [(1)], qui confirment la vulnérabilité de ces dernières aux pratiques commerciales des principaux éditeurs de logiciels :

« ***Les répondants déclarent une hausse moyenne du coût de leurs services de cloud-logiciel de 8,7 % par an sur les trois dernières années, et anticipent une hausse de 12 % par an sur les cinq prochaines année****s. La hausse la plus importante lors d'un renouvellement atteint 51 % en moyenne, avec des cas extrêmes déclarés à 100 %, voire 200 à 300 % pour certains répondants. Ces données confirment l'accélération de l'inflation tarifaire depuis la première enquête Asterès – Vanson Bourne de février 2022, qui évaluait alors les hausses à 5,8 % par an. Le rythme d'inflation a ainsi progressé de près de trois points en quatre ans, et les anticipations des DSI pour les cinq prochaines années s'inscrivent dans la continuité de cette trajectoire (…). Les hausses les plus importantes concernent en premier lieu les logiciels de productivité et de collaboration et les logiciels de socle technique et sécurité (…).* ***Ces hausses s'appuient sur des pratiques commerciales potentiellement abusives :*** **vendor lock-in** ***(40 % des répondants s'en disent victimes au cours des trois dernières années), l'IA by-design (32 %), l'obsolescence programmée (30 %), la bundlisation (26 %) ou encore la réduction de métriques (21 %).*** »

L'étude du cabinet Asterès prolonge l'analyse en décrivant les impacts potentiels de telles hausses sur les budgets numériques des grandes organisations, et de manière générale sur leur activité : « *les hausses tarifaires se traduisent dans*

*(1) Le cabinet Asterès relève un potentiel biais de sélection induit par l'enquête :* « les entreprises les plus concernées par les hausses tarifaires sont vraisemblablement les plus enclines à répondre, ce qui peut conduire à une surestimation de l'ampleur des hausses observées. La concordance avec d'autres enquêtes et d'autres données conforte alors l'analyse du questionnaire ».

*la grande majorité des cas par une réduction d'autres postes de dépenses. Le budget numérique représente 4,1 % du chiffre d'affaires des organisations privées interrogées (ou de leur contribution au Produit National Brut, pour les administrations). 28 % de ce budget est consacré au cloud-logiciel, et selon la trajectoire inflationniste tendancielle actuelle, cette proportion pourrait monter à 42 % à l'horizon 2030. Cette dépense est fortement concentrée : les cinq premiers fournisseurs captent à eux seuls 53 % du budget cloud-logiciel des répondants, Microsoft étant cité par la quasi-totalité d'entre eux. Les hausses tarifaires du cloud-logiciel modifient profondément la structure des budgets numériques des organisations sur les cinq dernières années, avec la part moyenne des OPEX portée à 50 %, ce qui constitue une " forte augmentation " selon les répondants. Pour absorber ces hausses, 47 % des répondants déclarent réduire leurs autres dépenses numériques, 33 % augmentent leur budget numérique global, 14 % réalisent des gains de productivité et 6 % en répercutent le coût sur les clients (…) Pour les organisations augmentant leur budget numérique, les autres dépenses réduites en priorité sont la R&D et l'investissement productif (32 %), la trésorerie et les marges (26 %), le recrutement (21 %) et les augmentations de salaires (12 %)* ».

*
* *

La rapporteure a souhaité rassembler l'ensemble des chiffres montrant la domination des entreprises extra-européennes dans le domaine du logiciel et la perte de valeur que cela représente.

La France compte des acteurs dynamiques dans le domaine du logiciel, positionnés surtout sur le segment des outils sectoriels. En revanche, les logiciels transverses, présents dans tous les systèmes d'information, et les services de cloud, qui constituent là encore des briques de base, sont entre les mains d'une poignée d'acteurs, quasi-intégralement américains. La concurrence française, en train de s'organiser, est toutefois loin d'atteindre le même volume d'activité, et son degré d'ouverture à l'international demeure insuffisant.

Cette situation engendre des vulnérabilités économiques constatées du côté des utilisateurs des solutions, confrontés à l'insuffisance de la concurrence. L'ensemble des administrations publiques recourent de manière massive à des achats de logiciels fournis par des entreprises extra-européennes, au détriment de solutions développées en Europe. Sur le périmètre de l'État, a minima 268 millions de dépenses auprès de fournisseurs extra-européens ont été identifiées, et 609 millions d'euros pour l'ensemble des administrations. L'extrapolation des chiffres de l'Ugap à l'ensemble des achats de l'État conduit à une estimation de **dépenses auprès des fournisseurs extra-européens de l'ordre de 1,5 milliard d'euros par an.**

L'utilisation de logiciels open source, techniquement possible, pourrait représenter des **économies annuelles de frais de licences.** Les dépenses directement identifiées par la commission d'enquête sont de 185 millions d'euros sur le périmètre de l'État et 423 millions d'euros sur le périmètre de l'ensemble des administrations. **L'extrapolation des chiffres de l'Ugap conduit à une estimation d'économies de dépenses annuelles de 1 milliard d'euros.**

Les dépenses auprès d'acteurs extra-européens n'apportent aucun bénéfice particulier à la collectivité, ne génèrent que très peu d'activité sur notre territoire, et sont donc des pertes nettes.

Pour les acteurs privés, l'utilisation de solutions propriétaires les expose à des hausses tarifaires parfois brutales, imposées par des éditeurs en position de force du fait de l'absence d'alternative ou des coûts de migration.

Enfin, le modèle particulier des plateformes doit conduire à mettre en place des dispositifs fiscaux spécifiques, sans quoi la valeur générée en France ne pourra pas contribuer au financement des services publics et de la protection sociale. **La taxe sur les services numériques, qui génère 542 millions d'euros de recettes auprès des grandes plateformes extra-européennes, est absolument nécessaire pour contrebalancer leur modèle tourné vers l'activité offshore. En l'absence de dispositif similaire pour le cloud, cette activité ne génère pour le moment aucun retour pour la collectivité, si elle est le fait d'un acteur extra-européen.**

## CHAPITRE 4 – ATTEINTE 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. Selon le directeur général de l'Anssi, M. Vincent Strubel, cela constitue une menace directe pour la souveraineté européenne, à savoir la capacité à « *appliquer notre droit et nos règles telles que nous les avons choisies dans l'expression de la souveraineté définie par notre Constitution, et de ne pas subir les règles définies par d'autres, sur lesquelles nous n'aurions pas voix au chapitre, ce qui renvoie à toute la question du droit extraterritorial*. » Si l'adoption du RGPD en 2016 a marqué un tournant, en imposant le respect de standards de sécurité et de confidentialité élevés aux entreprises étrangères qui opèrent au sein de l'Union européenne, il est encore largement contourné par des plateformes qui fondent leur enrichissement sur la collecte massive de données personnelles et leur commercialisation à travers la publicité ciblée.

### 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, comme l'ont montré les décisions successives de la Cour de justice de l'Union européenne concernant les transferts de données transatlantiques.

#### 1. Des transferts transatlantiques invalidés à plusieurs reprises par le juge européen en raison des risques d'atteinte aux droits fondamentaux

Conformément à l'article 25 de la directive du 24 octobre 1995 relative à la protection des données personnelles, **les données à caractère personnel de résidents européens ne peuvent être transférées vers un pays tiers que s'il assure un niveau de protection adéquat**. Si la Commission européenne constate qu'un pays tiers ne garantit pas un tel niveau de protection, les États membres doivent prendre les mesures nécessaires pour empêcher toute transmission de données personnelles vers le pays en cause. En revanche, lorsqu'elle constate qu'un pays tiers assure un niveau de protection adéquat, en raison de sa législation interne ou d'engagements internationaux pris dans le cadre des négociations avec l'Union européenne, la Commission peut autoriser les transferts de données vers ledit pays par une décision d'adéquation.

La **décision d'adéquation du 26 juillet 2000 dite *Safe Harbour*** a ainsi permis, pendant quinze ans, que les données personnelles de citoyens européens soient transférées vers les États-Unis, avant qu'elle ne soit jugée invalide par la Cour de justice de l'Union européenne au motif que la protection des données des citoyens européens n'était pas garantie par le cadre américain.

**En 2013, les alertes d'Edward Snowden ont, de fait, révélé l'existence d'un vaste réseau de surveillance établi par les États-Unis en 2007**. Sur le fondement de la section 215 du Patriot Act*,* adopté en 2001, la National Security Agency était en mesure d'accéder à toutes les données hébergées sur le cloud américain par les *hyperscalers* et de surveiller ainsi les informations échangées sur le territoire américain ainsi que l'ensemble des flux dirigés vers l'extérieur, sans disposer de mandat d'un juge. Selon Mme Marie-Laure Denis, « *a été alors mis en lumière le fait que les géants du numérique disposaient de pans entiers de notre vie privée, mais également que nos données étaient massivement exploitées à notre insu, au détriment de nos intérêts et de nos droits* » (1).

Par l'**arrêt du 6 octobre 2015 *Maximillian Schrems c/ Data Protection Commissioner***, la Cour de justice de l'Union européenne (CJUE) a estimé que l'existence d'une réglementation autorisant les autorités américaines à accéder de manière généralisée au contenu de communications électroniques devait être considérée comme portant atteinte au droit fondamental au respect de la vie privée, tandis que l'absence de voie de recours pour permettre aux justiciables d'accéder à leurs données à caractère personnel, ou d'en obtenir la rectification ou la suppression, violait le droit fondamental à une protection juridictionnelle effective.

La Commission a engagé de nouvelles négociations avec les États-Unis, qui ont abouti, le 12 juillet 2016, à une **nouvelle décision d'adéquation, dite *Privacy Shield*,** qui apportait des garanties supplémentaires. Elle renforçait notamment les voies de recours à disposition des citoyens européens et conférait à la Federal Trade Commission le pouvoir de sanctionner les entreprises qui ne respectaient pas leurs obligations de protection des données découlant de l'accord. L'administration américaine s'était également engagée à ce que la surveillance de masse soit limitée à la protection de la sécurité nationale, et à mettre en place un *ombudsman*, un médiateur chargé de suivre les plaintes des citoyens européens à propos des programmes de surveillance des États-Unis.

Cette décision a de nouveau été invalidée par la Cour de justice de l'Union européenne, par **l'arrêt du 16 juillet 2020, *Data Protection Commissioner / Maximilian Schrems et Facebook Ireland***. Elle a jugé que la collecte des données par les services de renseignement n'offrait pas de garanties de proportionnalité équivalentes à celles requises en Europe, et que les voies de recours étaient insuffisantes, relevant notamment le manque d'indépendance de l'ombudsman et l'absence de contrôle juridictionnel effectif sur les activités de renseignement américaines.

---

*(1) Audition de Mme Marie-Laure Denis, présidente de la Cnil, le 15 avril 2026.*

L'arrêt de la Cour a marqué un tournant, selon la présidente de la Cnil, Mme Marie-Laure Denis : *« en considérant que la législation américaine portait une atteinte disproportionnée à la vie privée des Européens, la Cour a remis en question l'ensemble des transferts de données vers ce pays et de facto vers les fournisseurs de services numériques soumis au droit états-unien. Les conséquences opérationnelles de cette décision ont mis en lumière l'extrême dépendance de nos administrations et des entreprises à l'égard de ces acteurs à tous les niveaux – hébergement, services d'informatique en nuage, outils de cybersécurité, outils bureautiques ou d'analyse de donnée* » (1).

### 2. Le *Data Privacy Framework* : un nouveau cadre toujours fragile

**Par l'*executive order* 14086 du 7 octobre 2022, le président des États-Unis Joe Biden a renforcé les garanties de protection de la vie privée dans le cadre des activités de renseignement des États-Unis**. Le décret a notamment établi un nouveau mécanisme de recours pour les Européens qui allèguent de la collecte et de l'utilisation illicite de leurs données personnelles par les services de renseignement à des fins de sécurité nationale. Il est prévu que la plainte soit transmise par les autorités européennes de protection des données au Civil Liberties Protection Officer du Bureau du directeur du renseignement national américain, qui sera chargé de vérifier si les garanties prévues ont été violées et, le cas échéant, de déterminer les mesures correctives contraignantes appropriées. Il est possible de contester cette décision devant la DPRC, créée par un règlement du Procureur général du 7 octobre 2023 et composée de juges fédéraux indépendants. Sur cette base, la Commission européenne a adopté une nouvelle décision d'adéquation le 10 juillet 2023, dite *Data Privacy Framework.*

**Ce nouveau cadre est cependant considéré comme très insuffisant par les associations de protection des données**.

De fait, il « ***repose largement sur des garanties extralégislatives américaines*** *– des courriers, des décrets présidentiels, et ainsi de suite –,* explique Max Schrems. *Car en pratique, comme me le signalait un parlementaire américain, il serait impossible de faire adopter au Congrès américain une loi visant à accroître les droits des étrangers, pour des raisons politiques »* (2). Il est donc susceptible d'évoluer très rapidement, en fonction des changements politiques, sans que l'administration ait besoin d'obtenir l'appui du Congrès.

Il marque d'ailleurs **peu de progrès substantiels par rapport au précédent accord conclu par la Commission**. *« Sur le plan des relations publiques, la Commission européenne a géré ces questions de manière très habile, se contentant de mentionner dans ses communiqués de presse la signature de nouveaux décrets, sans préciser que ceux-ci n'étaient souvent rien de plus qu'une copie directe de ceux signés sous la présidence de Barack Obama, dont les cours*

*(1) Audition de Mme Marie-Laure Denis, présidente de la Cnil, le 15 avril 2026.*

*(2) Audition de M. Max Schrems, fondateur de l'association Noyb, le 26 mars 2026.*

*de justice avaient signalé l'insuffisance. Il a souvent fallu un long travail d'analyse pour mesurer combien l'apport de nouveaux décrets était faible. Par exemple, la Commission européenne s'est félicitée que les États-Unis introduisent un principe de proportionnalité sur le modèle de celui prévu dans le droit européen, avec l'idée que cela permettrait d'interdire la surveillance de masse, dès lors que celle-ci est jugée disproportionnée par les tribunaux. Or ce n'est pas le cas. Interrogés sur ce point,* ***les États-Unis expliquent ne pas avoir la même définition de la proportionnalité que l'Union européenne****. Ainsi, les deux parties se sont accordées sur l'usage d'un terme, mais pas sur son sens.* » (1)

Dans le rapport qu'il a rendu en novembre 2024 sur le *Data Privacy Framework* (2), le Comité européen de la protection des données (CEPD) a noté qu'il restait encore à garantir l'effectivité du mécanisme de recours, compte tenu du faible nombre de plaintes constaté jusqu'à présent. Il a également appelé la Commission européenne à contrôler la mise en œuvre des principes de nécessité et de proportionnalité par les autorités américaines, et de suivre les évolutions futures liées à la loi américaine sur la surveillance du renseignement étranger.

Pour ces motifs, **le député Philippe Latombe, président de la commission d'enquête, a introduit un recours devant le Tribunal de l'Union européenne en vue d'obtenir l'annulation de la décision d'adéquation**. Sa requête s'appuie, d'une part, sur le manque d'impartialité et d'indépendance de la DPRC, qui a été créée par décret et non par une loi du Congrès, maintenant sa subordination au ministère de la justice ; d'autre part, sur la collecte massive de données personnelles de citoyens européens par les agences de renseignement des États-Unis, sans contrôle préalable par un juge ou une administration (3). Le Tribunal a rejeté la requête, le 3 septembre 2025, marquant un assouplissement des exigences par rapport à la décision *Schrems II* : il estime notamment qu'il n'est pas nécessaire d'obtenir une autorisation préalable systématique pour des collectes de données en masse, mais qu'un contrôle juridictionnel *a posteriori* peut suffire (4). Le contentieux est toujours pendant, M. Latombe ayant introduit un pourvoi devant la CJUE.

Sur ce point, la présidente de la Cnil a assuré à la rapporteure interroger régulièrement la Commission européenne sur son analyse de la situation et sur les mesures qu'elle entendait prendre pour garantir la protection des données dans le cadre transatlantique. Elle a relevé que l'administration américaine n'avait pour l'instant pas donné de signe qu'elle souhaitait abroger *l'executive order* de 2022 sur lequel repose le *Data Privacy Framework.*

---

*(1)* Ibid.

*(2) Rapport du Comité européen de protection des données sur la mise en œuvre par la Commission européenne de la décision d'adéquation dans le cadre du Data Privacy Framework, adopté le 4 novembre 2024.*

*(3) Belot,Emma et al., « Le contrôle du data privacy framework par le tribunal de l'Union européenne : une validation sous le signe de la fragilité de l'équilibre »,* PinCode, *2026/1 n° 26 , 2026.*

*(4) Arrêt du Tribunal de l'Union européenne du 3 septembre 2025 (T-443/23).*

**Le cadre établi se trouve cependant menacé par la diminution des compétences et des moyens de la DPRC**. Ce risque avait été pointé par Max Schrems lors de son audition : « *La Cour suprême américaine, désormais très conservatrice, doit se prononcer dans les prochains mois sur les garanties d'indépendance dont dispose la Federal Trade Commission. Sa décision va probablement marquer la fin de toutes les autorités indépendantes aux États-Unis – alors que l'Union européenne s'est beaucoup appuyée sur leurs décisions pour assurer la protection des données de millions d'Européens. Les fondements des garanties actuelles pourraient être réduits à néant du jour au lendemain* » [(1)]. La DPRC a, en outre, connu une réduction de ses effectifs, susceptible de fragiliser sa capacité à remplir ses missions.

Le 29 juin 2026, 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) [(2)]. En autorisant le limogeage de Rebecca Slaughter, la Cour valide la stratégie présidentielle de politisation des agences d'État indépendantes. En remettant en cause l'indépendance de la DPRC, cette décision rend 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.

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

### B. UNE EXPLOITATION MASSIVE DES DONNÉES PERSONNELLES PAR LES GÉANTS DU NUMÉRIQUE, EN VIOLATION DU DROIT EUROPÉEN

Les géants du numérique, notamment les réseaux sociaux et les moteurs de recherche, ont fondé leur modèle économique sur une collecte massive de données personnelles à des fins de monétisation à travers la publicité ciblée. Cela les a conduits à largement contourner pendant des années le RGPD pour augmenter leur patrimoine de données et renforcer leur position dominante. Si elles se sont désormais mises partiellement en conformité, elles utilisent désormais les données accumulées pour développer leurs modèles d'intelligence artificielle, sans avoir recueilli au préalable le consentement des utilisateurs.

*(1) Audition de M. Max Schrems, fondateur de l'association Noyb, le 26 mars 2026.*

*(2) Cour suprême des États-Unis,* Trump, président des États-Unis et al. *v.* Slaughter, 29 juin 2026 (n° 25-332)

### 1. Un modèle fondé sur une collecte massive de données personnelles

Le **modèle économique de monétisation des données personnelles adopté par les grandes plateformes** a bien été mis en valeur par l'ensemble des chercheurs, associations et ONG auditionnés par la commission d'enquête. Les recherches réalisées par Amnesty International sur l'impact du fonctionnement des grandes plateformes numériques sur les droits européens, et notamment sur X, sur Google et sur Facebook, ont montré « *l'existence d'un modèle économique commun, fondé sur un profilage intrusif, une collecte massive de données personnelles et le recours à la publicité ciblée, qui constitue le moteur du fonctionnement de ces plateformes. Ce schéma se retrouve de manière constante puisque les plateformes cherchent en permanence à accroître la quantité de données collectées afin d'élaborer des profils toujours plus précis, destinés à être commercialisés auprès des annonceurs, tandis qu'elles recourent, dans le même temps, à des algorithmes sophistiqués pour déduire des centres d'intérêt, voire des indicateurs de bien-être, comme c'est le cas de TikTok. L'objectif poursuivi consiste à personnaliser les contenus, à maintenir les utilisateurs en ligne le plus longtemps possible et à remporter cette guerre de l'attention, souvent au détriment des droits humains* » (1).

Ce ciblage repose le plus souvent 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.

**Grâce à leur écosystème de services intégrés, les *Big Tech* disposent en effet de volumes considérables de données**. Google est en mesure de collecter des données personnelles grâce à son moteur de recherche Google Search, son navigateur Google Chrome, son application de géolocalisation Google Maps, ou l'application d'édition de contenus vidéos Youtube. De même, Meta a accès aux données personnelles de millions d'utilisateurs à travers ses services de messagerie et de réseau social WhatsApp, Messenger et Facebook. La possibilité de croiser les données entre les différents services proposés, grâce à l'identifiant unique de l'utilisateur, leur permet d'établir des profils extrêmement précis. Ils peuvent ensuite être commercialisés auprès des annonceurs afin de choisir le contenu publicitaire le plus susceptible de faire interagir la personne.

C'est cet accès privilégié aux données qui **permet à Google de fonder sa domination sur le marché de la publicité en ligne, auquel il participe à la fois en tant que régie publicitaire et que vendeur d'espace publicitaire**, comme l'a expliqué M. Robin Berjon : « *avoir accès aux recherches effectuées par les personnes et à leur navigation internet – Chrome traque tout ce que nous faisons -, à leurs données de localisation physique et à de nombreux autres paramètres en grand volume permet de deviner ce qu'elles s'apprêtent à acheter. Il est ainsi possible de leur présenter une publicité correspondante et de se prévaloir d'un lien de causalité entre la publicité et l'achat. Le fait d'avoir montré la publicité n'a*

*(1) Audition de Mme Katia Roux, chargée de plaidoyer pour Amnesty International, le 25 mars 2026.*

*apporté aucune valeur à l'annonceur mais les grands acteurs peuvent se targuer d'offrir davantage de conversions que les autres.* ***Tout le système est organisé pour acheminer le maximum de données vers les grands acteurs***. » (1)

**La masse de données détenues permet également aux entreprises de personnaliser très finement l'édition des contenus, à travers leur algorithme de recommandations**, au risque de créer des biais discriminatoires ou d'engendrer des pratiques addictives. La commission d'enquête n'a cependant pas traité la question des risques sur la santé et les droits fondamentaux de ces modèles algorithmiques, d'ores et déjà démontrés par de nombreux travaux.

**Ce profilage peut également être utilisé par des gouvernements afin de limiter l'exercice des droits et libertés, si les grandes plateformes coopèrent à la mise en œuvre de dispositifs de surveillance de la population**. Meredith Whittaker, présidente de la fondation Signal, a notamment évoqué, lors de son audition, la communication par Facebook de messages privés aux autorités du Nebraska dans le cadre d'une enquête sur un avortement illégal : « *aux États-Unis, une femme a été incarcérée après que Meta a pris connaissance d'un échange de messages sur Facebook entre elle et sa fille, dans l'État du Nebraska, après que cet État a restreint l'accès aux soins reproductifs après la décision Dobbs. Ces messages privés montraient qu'elle avait aidé sa fille à accéder à l'avortement ; elle est désormais en prison. Cet exemple nous est connu parce qu'il a été relayé par les médias, mais le problème excède très largement ce seul cas. Des entreprises détiennent des informations, alors même que des qualifications telles que « terroriste » ou « menace pour le pays » sont, par nature, mouvantes. Ce qui est légal aujourd'hui peut devenir illégal demain.* » (2)

### 2. Des violations répétées du cadre européen de protection des données

**Au lendemain de l'affaire Snowden, les colégislateurs européens ont adopté le RGPD, le 27 avril 2016, afin d'assurer aux citoyens un meilleur contrôle sur leurs données personnelles**. Le règlement requiert que les traitements de données personnelles fassent l'objet d'un **consentement libre, spécifique, univoque et volontaire**, tout en consacrant également le droit d'accès à ses données, le « droit à l'oubli » et le droit à la portabilité de ses données. Il impose la protection des données dès la conception et par défaut, en responsabilisant l'ensemble des acteurs de traitement. Disposant d'une portée extraterritoriale, il a vocation à s'appliquer à toutes les entreprises qui traitent des données personnelles de citoyens européens, même si elles sont situées en dehors de l'UE. En cas d'infraction, les entreprises s'exposent à des **amendes allant jusqu'à 20 millions d'euros ou 4 % de leur chiffre d'affaires mondial**. Si le règlement a abrogé la directive du 24 octobre 1995 sur la protection des données à caractère personnel, la directive dite e-privacy du 12 juillet 2002 demeure applicable pour le dépôt des traceurs, ou *cookies*. Elle exige le consentement préalable de l'utilisateur avant le

*(1) Audition de M. Robin Berjon, directeur de l'agence Supramundane, le 10 mars 2026.*

*(2) Audition de Mme Meredith Whittaker, présidente de la fondation Signal, le 25 mars 2026.*

stockage d'informations sur son terminal ou l'accès à des informations déjà stockées sur celui-ci, sous le contrôle des autorités de protection des données nationales.

Selon la présidente de la Cnil, **le RGPD constitue « *un outil de souveraineté normative par lui-même* » : « *son champ d'application ne se limite pas aux sociétés européennes, mais couvre tous les acteurs dès lors qu'ils proposent des biens ou des services à des personnes dans l'Union européenne*.** *En exigeant un haut niveau de protection des données, notamment en matière de sécurité ou d'encadrement des transferts, le RGPD constitue un levier favorable à l'affirmation d'une souveraineté européenne*. » [(1)].

**Le cadre européen de protection des données est cependant largement contourné, aussi bien la directive e-privacy que le RGPD.**

Plusieurs enquêtes de la Cnil ont montré que les géants du numérique avaient adopté des pratiques contraires à la législation sur les cookies**.** De fait, **sur les 953 millions d'euros d'amendes prononcées par l'autorité sur le fondement de la directive e-privacy depuis 2019, 903 millions l'ont été à l'encontre des plus grandes plateformes étrangères**, « *non parce qu'elles sont étrangères mais en raison de leur impact sur la protection des droits de nos concitoyens »* explique Mme Marie-Laure Denis.

**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, avril 2026 (https://www.cnil.fr/fr/les-sanctions-prononcees-par-la-cnil)*

En 2020, la Cnil a infligé de premières amendes, respectivement de 100 millions et de 35 millions d'euros, à Google et Amazon [(2)], qui déposaient automatiquement des cookies à finalité publicitaire sur le terminal des utilisateurs dès leur arrivée sur la page, sans qu'ils aient donné leur consentement. La Cnil avait

*(1) Audition de Mme Marie-Laure Denis, président de la Cnil, le 15 avril 2026.*

*(2) Cnil, délibérations SAN-2020-012 et SAN-2020-013 du 7 décembre 2020*

justifié le montant des sanctions par le poids considérable de ces acteurs – 90 % du marché de la recherche en ligne pour Google et 20 % du commerce en ligne pour Amazon –, dont les manquements affectaient par conséquent des dizaines de millions d'utilisateurs. L'autorité avait souligné, en outre, les bénéfices considérables tirés par Google des données collectées par ces cookies du fait de sa position dominante sur toute la chaîne de valeur de la publicité en ligne.

En 2021 et 2022, la Cnil a sanctionné Google à hauteur de 150 millions d'euros d'amende, Facebook à hauteur de 60 millions [(1)], et Microsoft à hauteur de 60 millions également [(2)], pour ne pas avoir permis à leurs utilisateurs de refuser les cookies aussi facilement que de les accepter, plusieurs clics étant nécessaires pour ce faire.

Google a été sanctionné une troisième fois, en 2025, d'une amende record de 325 millions d'euros, notamment pour avoir déposé des cookies lors de la création de comptes Google sans le consentement valide des utilisateurs : ces derniers n'étaient pas clairement informés que l'accès aux services de Google était conditionné au dépôt de cookies, et étaient incités à choisir les traceurs liés à l'affichage de publicités personnalisées plutôt que ceux liés à l'affichage de publicités génériques. La société Shein a également été sanctionnée d'une amende de 150 millions en raison d'un dépôt de traceurs dès l'arrivée des utilisateurs sur le site, sans consentement préalable, d'un manque d'informations sur la finalité publicitaire des traceurs, et d'un mécanisme de refus du consentement défaillant [(3)].

**Ces sociétés ont également été reconnues responsables de nombreuses violations au RGPD par les autorités de protection des données européennes compétentes.**

En 2021, l'autorité luxembourgeoise a ainsi infligé une **amende de 746 millions d'euros à Amazon** pour avoir collecté les données personnelles des utilisateurs de sa plateforme de e-commerce en se fondant sur l'intérêt légitime, et non, comme elle aurait dû, sur leur consentement.

*(1) Cnil, délibérations SAN-2021-023 et SAN-2021-024 du 31 décembre 2021.*

*(2) Cnil, délibération SAN-2022-023 du 19 décembre 2022.*

*(3) Cnil, délibérations SAN-2025-004 et SAN-2025-005 du 1er septembre 2025.*

**SANCTIONS PRONONCÉES PAR LA DATA PROTECTION COMMISSION IRLANDAISE À L'ENCONTRE DES GRANDES ENTREPRISES EXTRA-EUROPÉENNES**

| Date | Société | Montant de l'amende (en millions d'euros) |
|---|---|---|
| **20/08/2021** | WhatsApp | 225 |
| **15/03/2022** | Meta (Facebook) | 17 |
| **02/09/2022** | Meta (Instagram) | 405 |
| **25/11/2022** | Meta | 265 |
| **31/12/2022** | Meta | 390 |
| **12/01/2023** | WhatsApp | 5,5 |
| **12/05/2023** | Meta | 1 200 |
| **01/09/2023** | TikTok | 345 |
| **26/09/2024** | Meta | 91 |
| **22/10/2024** | LinkedIn | 310 |
| **12 et 17/12/2024** | Meta | 251 |
| **30/04/2025** | TikTok | 530 |

*Source : Data Protection Commission, juin 2026 (https://dataprotection.ie/en/dpc-guidance/decisions/fines).*

**Meta a été sanctionné à huit reprises par l'autorité irlandaise, en lien avec le CEPD, pour un total de plus de 2,8 milliards d'euros d'amendes, en raison de multiples manquements à ses obligations de protection des données**.

En 2021, l'autorité lui a infligé une première amende de 225 millions d'euros pour son défaut de transparence sur le partage de données entre WhatsApp et d'autres filiales de Facebook et les possibilités de croisement. Une nouvelle amende de 405 millions a été infligée à Instagram pour avoir divulgué publiquement des adresses e-mail et des numéros de téléphones d'enfants utilisant un compte professionnel, et utilisé un paramétrage public par défaut pour des comptes personnels d'enfants, sans base légale.

En 2022, Facebook et Instagram ont été sanctionnés à hauteur de 390 millions pour avoir illégalement collecté des données personnelles à des fins de publicité ciblée depuis 2018 : alors que les deux réseaux sociaux avaient modifié leurs conditions générales pour conditionner l'accès à leurs services à l'acceptation des cookies, le CEPD a estimé que la publicité ciblée n'était en l'espèce pas nécessaire pour fournir le service et que Facebook et Instagram étaient tenus d'obtenir le consentement de leurs utilisateurs. Cette décision marque un jalon dans l'appréhension par le régulateur des *cookie walls*, ou murs de cookies.

**Les cookie walls**

Le terme *cookie wall* désigne le fait de conditionner l'accès à un service à l'acceptation du dépôt de cookies.

Dans sa déclaration sur la révision de la directive e-privacy, dénuée de portée normative, le Comité européen de protection des données avait considéré que la pratique consistant à bloquer l'accès à un site web ou à une application mobile aux personnes refusant les cookies n'était pas conforme au RGPD (1). La Cnil a repris cette position dans ses lignes directrices de 2020 en prévoyant que « *le consentement ne peut être valable que si la personne concernée est en mesure d'exercer valablement son choix et ne subit pas d'inconvénients majeurs en cas d'absence ou de retrait du consentement* » (2).

Par une décision du 19 juin 2020, le Conseil d'État a cependant invalidé ce raisonnement, en jugeant que l'exigence d'un consentement libre ne pouvait pas justifier une interdiction générale et absolue des *cookie walls*.

La Cnil apprécie donc la légalité des *cookie walls* au cas par cas, en tenant compte de l'existence d'alternatives réelles et équitables proposées en cas de refus des cookies (3). Elle indique par exemple que des services administratifs ne peuvent pas conditionner l'accès à une téléprocédure ou à un site d'information à l'acceptation des traceurs, puisqu'ils sont les seuls à proposer ce service. De même, l'instauration d'un *cookie wall* par un fournisseur de services dominant ou incontournable aurait pour conséquence de priver l'utilisateur d'un véritable choix.

L'alternative aux cookies peut consister dans le versement d'une contrepartie financière qui compenserait la perte de revenus publicitaires. Si cette pratique n'est pas interdite en soi, la Cnil veille à ce que le tarif soit raisonnable pour qu'il y ait un véritable choix. L'éditeur devra en outre démontrer que son cookie wall est limité aux finalités qui permettent une juste rémunération du service proposé (par exemple, la publicité ciblée), en demandant le consentement pour les autres finalités (personnalisation du contenu éditorial, etc.).

Une amende record de 1,2 milliard a été infligée à Meta en 2023 pour avoir continué, en 2020, à transférer les données de ses utilisateurs européens vers les États-Unis, en utilisant des clauses contractuelles types insuffisamment protectrices, malgré l'invalidation par la CJUE de la décision d'adéquation *Privacy Shield*.

Meta a également été sanctionnée plusieurs fois pour avoir manqué à son obligation de sécurisation des données de ses utilisateurs découlant de l'article 25 du RGPD : d'abord, en 2022, à hauteur de 265 millions, à la suite d'une collecte massive de données personnelles d'utilisateurs de Facebook par un tiers grâce aux techniques de *scrapping* ; puis en 2024, à hauteur de 91 millions et de 251 millions, pour le stockage de mots de passe non cryptés et la fuite de données de trois millions d'utilisateurs européens.

*(1) CEPD, Lignes directrices 05/2020 portant sur le consentement au sens du RGPD du 4 mai 2020, paragraphe 39.*

*(2) Cnil, Lignes directrices relatives aux cookies et aux traceurs du 4 juillet 2019.*

*(3) Cnil, « Cookie walls : la Cnil publie des premiers critères d'évaluation », 16 mai 2022.*

**Tiktok s'est également vue infliger des amendes, de 345 millions en 2023**, pour avoir rendu publics par défaut les profils d'adolescents, **et de 530 millions en 2025**, pour ne pas avoir offert de protection suffisante des données personnelles de ses utilisateurs européens, accessibles à distance par son personnel en Chine, alors que ce pays n'assure pas un niveau de protection équivalent à celui de l'Union européenne.

**Ces décisions successives ont conduit certaines plateformes à se mettre en conformité**, comme l'a salué la présidente de la Cnil lors de son audition : « *L'objectif premier de la régulation de la Cnil a été d'offrir la possibilité à l'utilisateur de refuser les cookies dès le premier écran. Cela a réclamé un travail de régulation méthodique mené durant trois ans en concertation avec les acteurs : publication de lignes directrices, puis, après avoir laissé un temps d'adaptation, lancement des contrôles et application des sanctions. Désormais, la plupart des sites se conforment aux règles : il est possible de refuser dès le premier écran – sur le téléphone portable, c'est l'option " continuer sans accepter ", en général en haut à droite de l'écran. Nos contrôles se tournent désormais vers les* ***interfaces trompeuses qui visent par exemple à noyer le " continuer sans accepter " dans d'autres informations.*** » (1)

**De fait, les *dark patterns*, ou interfaces trompeuses, sont utilisées par les opérateurs de sites web ou d'applications pour manipuler les utilisateurs et les conduire à faire des choix qu'ils n'auraient pas effectués autrement**. Il peut s'agir de demandes multiples de confirmation de choix qui rallongent le parcours pour les utilisateurs qui ne veulent pas renseigner certaines informations les concernant, de cases précochées, de sollicitations répétées pour amener l'utilisateur à consentir à l'utilisation de ses données personnelles, de comptes à rebours ou de messages d'urgence pour pousser à réaliser un achat… Comme l'a expliqué la directrice de recherche Mme Nataliia Bielova lors de son audition, « *de nombreuses recherches montrent que ces dark patterns influencent effectivement les décisions des utilisateurs. Nous avons mesuré leur impact sur le processus décisionnel de plus de 4 000 utilisateurs en France et avons conclu que* ***ces interfaces trompeuses modifient significativement la probabilité de consentement****. Nous avons également observé un effet d'exposition : des utilisateurs ayant déjà été confrontés à des dark patterns sont plus enclins à cliquer sur " Accepter " par la suite. De nombreux fournisseurs proposent par ailleurs des bandeaux de consentement avec des paramètres par défaut favorables au traçage. Or, nous connaissons bien la force de ces choix par défaut*. » (2)

Nombre de ces pratiques ne sont pas compatibles avec un consentement libre, éclairé et univoque, comme l'a estimé le CEPD dans ses lignes directrices

*(1) Audition de Mme Marie-Laure Denis, président de la Cnil, le 15 avril 2026.*

*(2) Table ronde sur la protection des données personnelles le 1er avril 2026.*

de 2022 sur les interfaces trompeuses [1]. **L'article 25 du règlement sur les services numériques (DSA) les a explicitement interdites.**

**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.

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

Le gouvernement devrait encourager la diffusion des outils développés par la Cnil auprès du grand public et des élèves, notamment l'application FantomApp et le site sur les apparences trompeuses, afin de mieux sensibiliser aux enjeux de protection des données personnelles.

### 3. Une exploitation massive des données personnelles détenues par les géants du numérique pour l'entraînement de leurs modèles d'IA

Les grandes plateformes étrangères utilisent désormais les volumes considérables de données qu'elles détiennent pour entraîner leurs modèles d'intelligence artificielle générative, alors que les modalités d'application du RGPD à l'entraînement et à l'utilisation de tels modèles ne sont pas encore stabilisées.

En mai 2025, Meta a annoncé son intention d'utiliser toutes les photos et messages publics de ses utilisateurs européens adultes de Facebook et d'Instagram pour entraîner ses systèmes d'intelligence artificielle. Les personnes qui souhaitent s'y opposer doivent alors modifier les paramètres de confidentialité de leur compte pour rendre ces informations privées.

Le patrimoine de données de Google permet à son modèle Gemini d'avoir accès à l'historique de requêtes, aux commentaires, aux vidéos, ou aux données de localisation de ses utilisateurs. Google assure que les contenus des emails, les photos et les historiques ne servent qu'à générer des réponses contextualisées pour personnaliser l'expérience des utilisateurs, sans être intégrés à l'entraînement des modèles.

Microsoft peut s'appuyer sur un corpus important pour entraîner ses propres modèles d'IA, grâce au rachat de la plateforme de référence des développeurs informatiques GitHub en 2018, et son moteur de recherche Bing.

*(1) CEPD, Lignes directrices 03/2022 relatives aux interfaces trompeuses dans les interfaces des plateformes de médias sociaux : comment les reconnaître et les éviter ?, version 2.0, adoptées le 14 février 2023.*

L'Autorité de la concurrence constatait ainsi, dès 2024 [1], que les *Big Tech* « *bénéficient également d'un accès privilégié à un large volume de données (ainsi, YouTube offre à Alphabet une source majeure de données d'entraînement pour les modèles d'IA producteurs de vidéos). Elles peuvent également accéder à des données associées à l'utilisation de leurs services. Elles peuvent aussi utiliser leur puissance financière pour conclure des accords avec des propriétaires de données tiers. Google s'est ainsi engagée à payer 60 millions de dollars (environ 55 millions d'euros) par an pour accéder aux données de Reddit, un site communautaire américain de discussions et d'actualités sociales* ».

En recourant au *web scraping*, ou l'extraction automatique de données accessibles sur le web, les grandes plateformes mettent en œuvre ce que Mme Mélanie Dulong de Rosnay, directrice de recherche au CNRS, appelle un « ***colonialisme des données*** », en référence aux travaux de Renata Avila, Nick Couldry et Ulises Mejias [2] : « [il s'agit d']*une nouvelle forme de vulnérabilité systématique (…) qui s'exerce sur tous les types de données numériques – personnelles, privées, publiques, techniques ou encore qui relèvent des communs numériques.* ***La vulnérabilité provient des conditions d'utilisation des plateformes, qui imposent des termes injustes et impossibles à négocier. Ces termes transfèrent tous les droits à la plateforme****. Les modèles économiques du numérique se fondent sur la captation de masses de données. La vulnérabilité vient aussi des limites et des effets secondaires des licences libres et des données ouvertes ayant placé les ressources dans des conditions proches du domaine public, ce qui est excellent du point de vue de leur diffusion, de la culture, de la démocratie et de l'innovation, mais qui autorise l'extraction et l'appropriation de la valeur de la donnée sans réciprocité ni soutien à la création ou à l'infrastructure, alors que les communs numériques sont produits grâce à des financements publics ou au travail bénévole de communautés. Nous sommes face au résultat d'une conception libérale de l'open data, revenant à offrir une manne réutilisable par tous y compris les grands acteurs du numérique, dès lors libres de les privatiser et d'en extraire la valeur – d'où la comparaison avec le colonialisme. La captation des investissements et du travail bénévole ne suppose ici aucune contribution aux communs* ».

**Ces traitements seraient, en outre, réalisés par les grandes plateformes sans garde-fous appropriés pour assurer la protection des données**, selon Meredith Whittaker [3] : « *Les pratiques dominantes consistent à agréger de vastes volumes de données, issues par exemple d'Alexa ou de Gmail, ainsi que des données provenant du web et de vos appareils connectés, pour les injecter dans un modèle, qui est ensuite ajusté par des travailleurs, généralement faiblement rémunérés et localisés dans les pays du Sud. Dans un tel cadre, et au regard des contraintes de*

---

*(1) Avis 24-A-05 de l'Autorité de la concurrence relatif au fonctionnement concurrentiel du secteur de l'intelligence artificielle générative du 28 juin 2024*

*(2) Audition de Mme Mélanie Dulong de Rosnay, directrice de recherche au Centre national de la recherche scientifique (CNRS), co-fondatrice du Centre internet et société (CIS) du CNRS, le 31 mars 2026.*

*(3) Audition de Mme Meredith Whittaker, présidente de la fondation Signal, le 25 mars 2026.*

*coûts qui pèsent sur ces entreprises, rien n'est véritablement conçu pour préserver l'intégrité des données face à des attaques d'empoisonnement*. »

**Le RGPD et la directive e-privacy continuent pourtant de s'appliquer et de pouvoir seuls servir de base légale au traitement des données à caractère personnel par les fournisseurs et les développeurs de systèmes d'IA**. En adoptant le règlement sur l'intelligence artificielle de 2024, les législateurs européens n'ont pas entendu « *modifier l'application du droit de l'Union régissant le traitement des données à caractère personnel* » comme il est précisé dans l'exposé des motifs [(1)]. Il y est ajouté que « *les personnes concernées continuent de jouir de tous les droits et garanties qui leur sont conférées par le droit de l'Union* ».

**Contestant l'idée selon laquelle le RGPD ne serait pas adapté aux nouveaux enjeux soulevés par l'intelligence artificielle, M. Max Schrems défend au contraire sa pleine applicabilité** [(2)] : « *On entend souvent dire que le RGPD n'a pas prévu ces développements et qu'il est donc nécessaire d'adapter la loi à ces nouvelles technologies. Or, les vieux hommes blancs qui, en 1981, ont établi les principes qui structurent le RGPD, évoquaient déjà la possibilité que, dans le futur, les données personnelles soient réutilisées de diverses façons alors inconnues et servent à alimenter de gros algorithmes qui prendraient des décisions étranges, dont plus personne ne serait en mesure de comprendre l'origine. C'est exactement pour cette raison que nous avons le droit d'accéder aux données collectées, de les faire supprimer ou de faire corriger de fausses informations : le sentiment dominant, à l'époque, était déjà que ces algorithmes étaient susceptibles de produire des erreurs. Nous y sommes : aujourd'hui, on appelle ces fausses informations des " hallucinations " et on constate que les données recueillies pour alimenter des IA ou des LLM (Large Language Models, ou grands modèles de langage) sont rassemblées dans de grands réservoirs sans qu'on sache ce qu'elles y deviennent. Une partie importante du RGPD a été rédigée précisément pour gérer ces situations*. »

**Les autorités européennes de protection des données ont néanmoins adopté une position moins exigeante**. Par un avis du 18 décembre 2024, le CEPD a d'abord précisé cette applicabilité en établissant qu'un modèle d'IA peut être considéré comme anonyme s'il est très peu probable d'identifier directement ou indirectement les personnes dont les données ont été utilisées pour créer le modèle, et d'extraire ces données personnelles du modèle par le biais de requêtes. La Cnil a précisé les opérations que doivent réaliser les développeurs de modèles d'IA pour déterminer si ceux-ci sont anonymes ou non et si le RGPD trouve à s'y appliquer.

Les autorités européennes de protection des données font cependant état de difficultés spécifiques soulevées par l'IA générative. La Cnil observe ainsi que

---

*(1) Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) no 300/2008, (UE) no 167/2013, (UE) no 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle)*

*(2) Audition de M. Max Schrems, fondateur de l'association NOYB (None of your business), le 26 mars 2026.*

**« *recueillir le consentement est souvent impossible en pratique* », notamment lorsque les systèmes sont entraînés à partir des données accessibles en ligne, par la pratique du *web scraping***, ou moissonnage [1].

Les développeurs sont amenés à s'appuyer sur l'intérêt légitime, prévu à l'article 6, point f) du premier alinéa du RGPD. Cela suppose de réunir trois conditions : l'intérêt doit être légal au regard du droit et déterminé de façon suffisamment claire et précise ; le traitement de données personnelles doit être nécessaire, c'est-à-dire qu'il ne doit pas y avoir d'autres moyens moins intrusifs ; et l'utilisation des données ne doit pas porter une atteinte disproportionnée à la vie privée des personnes. En pratique cependant, **les mesures prises par les développeurs des grands modèles d'IA générative sont insuffisantes pour limiter les risques d'extraction ou de régurgitation des données personnelles qui ont servi à leur entraînement**.

S'agissant des droits des personnes, **la Cnil considère que « *l'exercice des droits sur un modèle d'IA n'est pas absolu* »** [2]. Le droit de rectifier ses données, de les faire effacer et de s'opposer à leur traitement implique en effet de réentraîner le modèle d'IA, à défaut de pouvoir retirer certains éléments de sa base de données d'entraînement. La Cnil reconnaît également la possibilité pour les développeurs de ne pas donner suite à une demande d'accès aux données au motif qu'ils ne peuvent pas identifier la personne au sein de leur base de données.

Ainsi, selon Mme Ramya Chandrasekhar, chercheuse au centre internet et société du CNRS, « ***la législation en vigueur dans l'Union européenne (dont les lois sur le copyright ou sur la protection des données) se voit ainsi contournée pour laisser place à l'idée selon laquelle nos données sont tout simplement là pour être exploitées*** ».

M. Schrems relève lui aussi une forme de **renoncement des autorités de protection des données à appliquer le droit aux modèles d'IA, au risque de laisser se généraliser de graves atteintes à la vie privée** : « *quand l'IA est arrivée, nous avons constaté que tous les régulateurs européens, y compris la Cnil – qui était habituellement un régulateur très fort sur bien des sujets – ont cédé, estimant qu'il fallait tout autoriser, de peur de prendre du retard dans ce secteur. De ce fait,* ***nous faisons maintenant face à 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****. Une de nos affaires en cours concerne par exemple un ressortissant norvégien dont l'intelligence artificielle d'OpenAI prétend qu'il a assassiné ses enfants, maltraité sa femme et commis toute une série d'actes aussi horribles que fictifs. Or, quand nous demandons à OpenAI de corriger ces informations produites par son algorithme, l'entreprise explique être techniquement incapable de le faire. De nombreuses personnes témoignent de cas*

---

*(1) Cnil, « Développement des systèmes d'IA : les recommandations de la CNIL pour respecter le RGPD », 22 juillet 2025 (https://www.cnil.fr/fr/developpement-des-systemes-dia-les-recommandations-de-la-cnil-pour-respecter-le-rgpd)*

*(2) Ibid.*

*similaires. Il s'agit souvent de journalistes qui, parce que leur nom apparaît en tête d'articles qu'ils ont consacrés à des affaires criminelles, sont mêlés par l'IA avec le contenu desdits articles et se retrouvent ainsi accusés d'avoir tué des dizaines d'enfants ou d'avoir commis des agressions sexuelles. Que des compagnies de la Big Tech, qui engrangent des milliards, affirment n'avoir aucun moyen de corriger ces erreurs ou de traiter le problème est affligeant. C'est précisément pour ces raisons que nous nous sommes dotés des principes qui figurent dans le RGPD*. » (1)

## C. UN ÉCOSYSTÈME DE CAPTATION ET DE MONÉTISATION DES DONNÉES

Plus largement, c'est l'ensemble de l'architecture numérique qui s'est construite sur une captation des données personnelles à des fins de monétisation, par la constitution de chaînes d'intermédiaires complexes et opaques.

### 1. Une captation massive et opaque des données personnelles, intermédiée par les *data brokers*

**L'enquête réalisée par le journal *Le Monde* et huit médias partenaires (2), 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. Contrairement aux grandes plateformes numériques, qui exploitent directement les données qu'elles collectent, ces acteurs 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), ou encore historique de navigation sur internet.

« *En réalité,* ***quasiment toutes les applications sont concernées par la collecte de données publicitaires****. La quasi-totalité des applications et des services qu'elles proposent étant gratuits, les outils sont financés par la publicité. Ils embarquent donc des dispositifs pour en afficher et collecter des données afin de les cibler* », a expliqué le journaliste M. Martin Untersinger devant la commission d'enquête (3).

**Les données sont également recueillies par des entreprises tierces, via les briques logicielles (*software development kit – SDK)* qu'elles fournissent**. Mme Nataliia Bielova, également auditionnée, observe ainsi : « *Ce que l'on observe aujourd'hui est un système plus vaste de chaînes d'inclusion, dans lequel de nombreuses entreprises intègrent et dépendent des services des autres. D'un point de vue technique, cette situation est liée à la nature dynamique du contenu web. Des composantes peuvent être chargées par des bibliothèques JavaScript à l'insu de*

---

*(1) Audition de M. Max Schrems, président de l'association Noyb, le 26 mars 2026.*

*(2) 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.*

*(3) Audition de M. Martin Untersinger, journaliste au Monde, et MM. Antoine Schirer et Sébastien Bourdon, journalistes indépendants, le jeudi 26 mars 2026.*

*l'opérateur du site web, ce qui permet l'introduction de traceurs cachés. (…) Par exemple, un service fournissant une carte à un site web peut inclure des cookies liés à une entreprise publicitaire, sans que l'utilisateur du site puisse réellement les éliminer. S'agissant des technologies spécifiques utilisées pour le traçage en ligne massif, l'industrie s'est historiquement appuyée sur les cookies tiers, qui permettent la constitution de profils utilisateurs à partir des sites visités »* (1). Elle estime que **les traceurs seraient présents sur environ 90 % du web.**

**Certains *data brokers* collectent également des informations dans le cadre des enchères en temps réel** organisées pour attribuer les encarts publicitaires qui s'affichent sur l'écran d'un internaute. Selon la Cnil, parmi les dizaines, voire centaines, d'annonceurs qui reçoivent des informations sur le profil de l'internaute, certains décident de les conserver pour les revendre, sans qu'il soit facile de les identifier.

### 2. Des risques importants pour la sécurité intérieure et les droits fondamentaux

**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. À partir de la base de données vendue par le *data broker* américain Datastream Group, les journalistes du *Monde* sont parvenus à identifier des policiers, des militaires, des employés d'industries stratégiques, des gardes du corps du Président de la République, ou encore des agents de la direction générale de la sécurité extérieure (DGSE), dont l'identité est pourtant protégée par la loi :

« *Lorsqu'on se penche sur les déplacements des officiers de la DGSE, on les voit évidemment boulevard Mortier ; le long des lignes de métro qui les amènent à la gare du Nord ; sur les quais des trains de la gare du Nord qui desservent leurs lieux d'habitation ; devant chez eux, etc. C'est d'une grande finesse. Donc les risques sont nombreux. Les données sont en elles-mêmes inoffensives, mais dans la mesure où elles sont reliées au domicile, au lieu de travail et à tous les lieux qui permettent d'identifier la personne et ses activités habituelles, elles constituent une menace.* » (2)

Une fois établis, **ces fichiers de données sont vendus à une grande diversité d'acteurs économiques**. Les entreprises déclarent sur les places de marché revendre les données à des fins de mesure d'audience, d'information sur des lieux, de prise d'information sur les concurrents,etc. Mais les fichiers peuvent

---

*(1) Table ronde sur la protection des données personnelles, avec Mme Nataliia Bielova, directrice de recherche au centre Inria de l'université Côte d'Azur, et M. Julien Rossi, maître de conférences en sciences de l'information et de la communication à l'UFR Culture et communication et au Cemti de l'université Paris 8, le 1er avril 2026.*

*(2) Audition de M. Martin Untersinger, journaliste au Monde, et MM. Antoine Schirer et Sébastien Bourdon, journalistes indépendants, le jeudi 26 mars 2026.*

également être acquis par des acteurs étatiques. M. Martin Untersinger décrit l'« ***industrie de la surveillance étatique*** » qui *« s'est greffée au secteur publicitaire » : « Une quinzaine ou une vingtaine de sociétés achètent des données, notamment et vraisemblablement auprès de courtiers, pour fournir des outils de géolocalisation et de pistage à des services de renseignement ou de police ».*

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**. Mme Bielova atteste que « *les utilisateurs peuvent être facilement manipulés ou discriminés sur la base de ces profils extrêmement précis, par exemple par le refus d'accès à certains services, à des offres d'emploi, ou encore par la proposition de prix différenciés pour des prêts, y compris des prêts immobiliers ».*

### 3. Un cadre réglementaire largement contourné en pratique

Interrogée par la commission d'enquête sur la prolifération de telles pratiques, la présidente de la Cnil a confirmé qu'elles n'étaient **pas conformes au cadre réglementaire de protection des données** : « *Sur le plan juridique, la réutilisation et la revente de données, même si elles ne sont pas illégales, sont strictement encadrées. En effet, le RGPD et la loi " informatique et libertés " prévoient que les personnes doivent être informées de la collecte et des usages de leurs données, et donner leur consentement en cas de traitement de celles-ci à des fins publicitaires et de revente.* » (1) Or, les conditions d'un consentement libre, éclairé, univoque et spécifique ne sont manifestement pas remplies en l'espèce. Mme Bielova remarquait que même les opérateurs de site web qui accueillent des traceurs « *ne savent pas précisément qui collecte les données des utilisateurs, à quelles fins, ni dans quelles conditions ».*

**Ce cadre réglementaire est pourtant largement contourné, en raison de la complexité et de l'opacité des chaînes d'intermédiaires**, qu'il est délicat de reconstituer. Les contrôles conduits par la Cnil en 2022 sur la prospection commerciale, et notamment sur les pratiques des courtiers en données, ont mis en évidence deux obstacles principaux qui rendent l'instruction particulièrement chronophage (2).

D'une part, « ***la complexité technique des chaînes de collecte et de revente rend difficile la traçabilité des données et l'identification des responsables*** » (3).

---

*(1) Audition de Mme Marie-Laure Denis, présidente de la Cnil, le 15 avril 2026.*

*(2) La Cnil a cependant été en mesure de rendre plusieurs sanctions à l'encontre de courtiers en données qui collectent des informations personnelles via des jeux concours et les revendent à des fins commerciales sans consentement valide, dont notamment le 31 janvier 2024 et le 15 mai 2025. En 2025, elle a également consacré une thématique prioritaire de contrôle aux applications mobiles, qui constituent l'un des principaux vecteurs de la collecte de données.*

*(3) Audition de Mme Marie-Laure Denis, présidente de la Cnil, le 15 avril 2026.*

Les entreprises ne sont en effet pas les destinataires finaux et uniques de ces données, mais les revendent à une multitude d'intermédiaires. Reprenant une image de ses collègues allemands, M. Untersinger compare le marché des données publicitaires mobiles à « *la lave à l'intérieur des lampes* » : « *elle bouge, se divise, se rapproche. Autrement dit, c'est un marché en mouvement permanent. Les données s'échangent, se revendent, sont modifiées, recoupées, etc. par des dizaines et des dizaines d'acteurs différents, sans qu'il soit vraiment possible de suivre leur cheminement.* » (1)

D'autre part, les acteurs qui revendent les données sur les places marchandes « *sont pour la plupart de* ***petites structures, qui n'ont aucun établissement en Europe, ne sont pas pérennes, ou changent souvent de nom*** », ce qui empêche de les sanctionner effectivement, a expliqué Mme Denis (2). M. Untersinger illustre ce dernier point avec le cas d'une start-up française, qui avait été sanctionnée par Google pour ne pas avoir respecté les bonnes pratiques de sa régie publicitaire : « *Cette start-up récupérait des données personnelles pour les revendre, notamment dans des outils de surveillance proposés à des États. Une fois blacklistée par Google, cette société a disparu. Son PDG en a immédiatement recréé une autre et si je n'ai pas d'informations à son sujet, il n'y a, à mon sens, guère de suspense quant à son activité* ».

**En bout de chaîne, ce sont néanmoins les grandes plateformes qui tirent parti de cette économie dans la mesure où elles constituent un point incontournable de la monétisation des contenus publicitaires**. M. Robin Berjon, informaticien et directeur de l'agence Supramundane, a souligné la forte concentration du marché publicitaire, qui permet aux *Big Tech* de « *maintenir une opacité absolue sur le fonctionnement des réseaux publicitaires, par lesquels transitent pourtant des centaines de milliards de dollars par an.* » (3).

#### 4. Les données de géolocalisation

Compte tenu de leur rôle clé dans la réidentification des personnes, la rapporteure s'est particulièrement intéressée à l'opportunité de **mieux encadrer la collecte des données de géolocalisation.**

Une autre enquête réalisée par *Le Monde*, consacrée aux *StravaLeaks* (4), a confirmé la sensibilité de ces données et les vulnérabilités que leur diffusion engendre. Sur cette application américaine qui permet de partager ses performances

---

*(1) Audition de M. Martin Untersinger, journaliste au Monde, et MM. Antoine Schirer et Sébastien Bourdon, journalistes indépendants, le jeudi 26 mars 2026.*

*(2) Audition de Mme Marie-Laure Denis, présidente de la Cnil, le 15 avril 2026.*

*(3) Table ronde réunissant M. David Chavalarias, directeur de recherche au CNRS, M. Robin Berjon, informativien et directeur de l'agence Supramundane, et Mme Maud Quessard, directzrice du domaine « Europe, espace transatlantique, Russie » à l'Irsem, le 10 mars 2026.*

*(4) Asia Balluffier, Sébastien Bourdon, Liselotte Mas et Antoine Schirer, «* StravaLeaks *: le porte-avions Charles-de-Gaulle localisé en temps réel par* Le Monde *grâce à l'application de sport »,* Le Monde, *le 19 mars 2026.*

sportives en ligne, il est possible d'accéder en direct à la position de nombreux utilisateurs. Cela a permis aux journalistes, là encore, de retrouver des militaires ou des gardes du corps de chefs d'État, et donc d'identifier, non seulement leur domicile, mais aussi des bases de l'armée française, la position du porte-avions *Charles de Gaulle*, ou les hôtels où devait séjourner le président de la République, avec des risques opérationnels manifestes.

M. Sébastien Bourdon, journaliste indépendant, revient également sur de précédents travaux sur l'opération Barkhane au Mali : *« La plupart des Maliens n'utilisant pas Tinder, les seuls profils que nous voyions apparaître étaient ceux de militaires français en poste dans cette base. L'application indique si la personne se situe à 1, 2, 3 ou 4 kilomètres, sachant qu'avec un système de triangulation, on peut même obtenir une localisation très précise, à quelques mètres près ; ce n'est pas très compliqué à faire. Et comme il s'agit d'une application de rencontres, les utilisateurs ajoutent nécessairement des informations personnelles : nom, âge, photos, y compris en uniforme ou avec des armes dans le cas des militaires.*

*« S'il est possible de faire cela au Mali, on peut aussi y parvenir en France métropolitaine. Il ne faut que trois clics pour se localiser sur l'île Longue sur Tinder et cela permettrait certainement d'identifier des dizaines, voire des centaines de militaires français ».*

Selon lui « *les personnes n'ont pour beaucoup d'entre elles, pas conscience de ce qu'implique le fait d'appuyer sur un bouton sur une montre connectée ou sur un téléphone – ce faisant, elles mettent en ligne des données. Je le répète,* ***le profil créé sur Strava est par défaut public, ce qu'ignore l'immense majorité de ses utilisateurs*** » (1). Malgré les recommandations transmises depuis par l'armée aux personnels pour leur faire prendre conscience des risques liés aux réseaux sociaux, la situation s'est toujours reproduite, révélant son caractère systémique.

Sur ce point, la Cnil a rappelé, dans ses réponses écrites, que le RGPD impose de recueillir le consentement des utilisateurs pour collecter et utiliser la donnée de géolocalisation lorsqu'elle n'est pas strictement nécessaire pour faire fonctionner l'application, comme c'est le cas pour les usages publicitaires. Par ailleurs, les acteurs doivent respecter le principe de minimisation des données, en privilégiant une géolocalisation approximative lorsque c'est suffisant. Il doit également être possible de désactiver techniquement l'accès aux données par une application au sein du téléphone.

**Les enquêtes sur les *StravaLeaks* ou sur les *data brokers* révèle les limites d'un modèle de protection des données qui repose sur la responsabilité individuelle, plutôt que sur celle des éditeurs,** en laissant aux utilisateurs le soin de modifier les paramètres de confidentialité pour restreindre les informations partagées, par défaut publiques. Mme Ophélie Coelho dénonce une « *forme de*

*(1) Audition de M. Martin Untersinger, journaliste au Monde, et MM. Antoine Schirer et Sébastien Bourdon, journalistes indépendants, le jeudi 26 mars 2026.*

*déresponsabilisation réglementaire qui individualise le droit : c'est à l'utilisateur de gérer sa propre sécurité* » [(1)].

À cet égard, il pourrait être pertinent d'**imposer plus systématiquement la désactivation par défaut de l'accès à la géolocalisation et le partage public des informations**. Comme l'a observé M. Florent Della Valle, chef du service de l'expertise technologique de la Cnil, « *l'article 25 du RGPD impose déjà que le paramétrage par défaut soit le plus protecteur de la vie privée. Ce principe est donc reconnu au niveau européen. Il doit toutefois être décliné dans différents contextes. Dans le secteur des applications mobiles, nous avons ainsi souhaité expliquer concrètement aux acteurs comment l'appliquer, pour mieux protéger la vie privée des personnes ».*

Les applications mobiles devenant l'un des principaux moyens d'accès aux contenus et services numériques, la Cnil a publié le 18 juillet 2024 des recommandations relatives aux applications mobiles [(2)]. L'ensemble de ces recommandations démontrent qu'il existe un cadre permettant d'avoir accès de manière plus sécurisée à de multiples applications mobiles.

### D. UNE APPLICATION INÉGALE DU RGPD

Lors de son audition, M. Max Schrems a raconté : « *Un jour, le responsable d'une autorité de protection des données est venu me voir à l'issue d'une conférence pour me dire combien ce serait drôle si les mesures que j'avais exposées étaient mises en œuvre. Quand on songe qu'il s'agissait précisément des lois qu'il était chargé de faire appliquer, c'est ahurissant ! C'est comme si une agence de lutte contre la drogue déclarait : " Ce serait drôle de faire quelque chose pour empêcher le trafic de cocaïne, non ? " Telle est la réalité avec laquelle nous devons composer sur le terrain. Il est vrai que les chiffres disponibles à l'échelle européenne montrent que moins de 1,3 % des plaintes débouchent sur une amende.* »

#### 1. Le rôle bloquant de l'Irlande

Afin d'assurer une application cohérente du règlement sur le territoire européen, **l'article 60 du RGPD prévoit une procédure de guichet unique pour les traitements de données transfrontaliers**, c'est-à-dire les traitements mis en œuvre par une entreprise établie dans plusieurs États européens ou qui affectent sensiblement des personnes d'au moins un autre État européen. La plainte doit dès

---

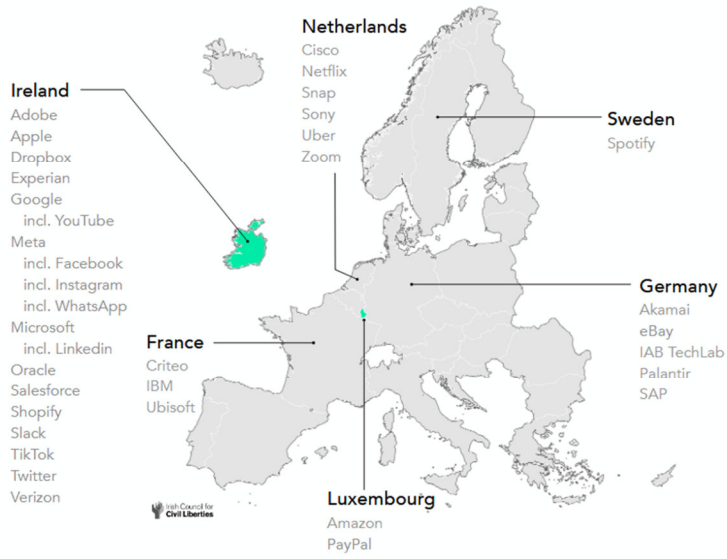
*(1) Table ronde, ouverte à la presse, sur les infrastructures numériques, réunissant, le 2 avril 2026 : Mme Ophélie Coelho, chercheuse associée à l'Institut des relations internationales et stratégiques (Iris), doctorante au CIS et au centre d'analyse et de recherche interdisciplinaires sur les médias (Carism-Paris-Assas) ; Data for Good : Mme Lou Welgryn, secrétaire générale, et Mme Alexandra Lutz, chargée de plaidoyer ; et Mme Francesca Musiani, directrice de recherche au CNRS, co-fondatrice et directrice du CIS.*

*(2) Délibération n° 2025-024 du 27 mars 2025 portant modification de la recommandation relative aux applications mobiles et abrogeant la délibération n° 2024-061 du 18 juillet 2024 portant adoption de la recommandation relative aux applications mobiles*

lors être prise en charge par l'autorité cheffe de file, qui est l'autorité de protection des données du pays où se trouve l'établissement principal de l'entreprise.

Cette règle a pour effet de **diriger une part importante des plaintes émises contre les grandes plateformes vers les trois États européens qui en concentrent les sièges, en raison de leur cadre fiscal favorable : l'Irlande, les Pays-Bas et le Luxembourg**. En 2025, la Cnil a ainsi transmis plus de 260 plaintes transfrontalières à un homologue, dont 51 % à la seule autorité de protection des données irlandaises (Data Protection Commission – DPC*)*.

**AUTORITÉS CHEFFES DE FILE DES PRINCIPALES ENTREPRISES TECHNOLOGIQUES.**




*Source : ICCL, 2023.*

Or, **de nombreuses organisations auditionnées par la commission d'enquête ont pointé le manque de fermeté de la DPC irlandaise dans la bonne application du RGPD**, ainsi que la durée particulièrement longue des procédures et l'impossibilité pour les plaignants d'avoir accès aux pièces du dossier. Un rapport publié par l'ONG *Irish Council for Civil Liberties (ICCL)* en 2023 relevait que, sur 55 dossiers transfrontaliers instruits entre 2018 et 2022, la DPC avait choisi de conclure des accords amiables dans 46 cas, comme le lui permet le droit irlandais, ne rendant de décision que dans les 9 cas restants [(1)]. À titre de comparaison, les autorités allemande et française avaient rendu respectivement 60 et 54 décisions sur

*(1) Irish Council for Civil Liberties,* 5 years : GDPR's crisis point, mai 2023 (https://www.iccl.ie/wp-content/uploads/2023/05/5-years-GDPR-crisis.pdf)

la même période. Aucune des plaintes déposées par La Quadrature du Net en 2018, qui relevaient de la compétence de la DPC, n'ont donné lieu à des sanctions.

**Cela s'expliquerait en partie par des ressources insuffisantes face à l'augmentation des plaintes reçues**. La présidente de la Cnil a ainsi reconnu qu'« *au début de la mise en œuvre du RGPD, l'autorité irlandaise a mis un peu de temps à se mettre en route et à décider des sanctions, pour des raisons qu'il lui reviendrait d'expliquer et aussi parce qu'il y avait certainement une montée en charge très importante des plaintes et des contrôles* » (1). De fait, le budget alloué à la DPC n'était que de 4,7 millions d'euros en 2016 ; il a depuis été multiplié par six, pour atteindre 29 millions en 2025 (2) – à titre de comparaison, le budget de la Cnil s'élevait à 30,2 millions la même année (3).

**Les sanctions prononcées par la DPC mettent plusieurs années à s'appliquer en raison du caractère suspensif des recours à leur encontre**. Les amendes ne deviennent exigibles qu'après avoir été confirmées par un tribunal : même si aucun recours n'est formé contre la décision de la DPC, celle-ci doit saisir la *Circuit Court* pour faire confirmer sa décision. « *Le recouvrement de l'amende ne peut donc avoir lieu qu'à l'issue de tous les contentieux consécutifs à la sanction, ce qui fait qu'un certain nombre d'amendes dont le montant est élevé n'ont pas encore été recouvrées* » a expliqué Mme Marie-Laure Denis. Le problème est amplifié par les **procédures dilatoires intentées par les grandes plateformes**, qui attaquent systématiquement en justice les sanctions qui les visent.

De fait, **seulement 0,6 % des sanctions prononcées par la DPC entre le 1er janvier 2020 et le 31 décembre 2024 ont été recouvrées**. Plusieurs amendes, d'un montant cumulé de 2 485 millions d'euros, infligées à Meta entre 2021 et 2023, n'ont toujours pas été perçues, du fait de recours encore en instance. Les 875 millions d'amendes infligés à TikTok n'ont pas non plus été recouvrés.

**RECOUVREMENT DES AMENDES PRONONCÉES PAR LA CNIL ET LA DATA PROTECTION COMMISSION IRLANDAISE**

| | Amendes prononcées (2020-2024) | Amendes recouvrées (2020-2024) | Taux de recouvrement |
|---|---|---|---|
| **DPC** | 3 507 481 500 | 19 952 000 | 0,6 % |
| **Cnil** | 598 260 100 | 570 986 038 | 95 % |

*Source : Assemblée nationale à partir de DPC, mai 2026 (https://www.dataprotection.ie/en/dpc-guidance/decisions/fines) ; Cnil, avril 2026*

M. Schrems dénonce des « ***procédures judiciaires irlandaises (…) extrêmement longues, complexes et onéreuses, au point qu'un citoyen lambda n'a aucune chance de faire valoir ses droits*** » (4). L'importance des frais à engager prive

*(1) Audition de Mme Marie-Laure Denis, présidente de la Cnil, le 15 avril 2026.*

*(2) ICCL, mai 2023*

*(3) Cnil, Rapport annuel 2025, mai 2026*

*(4) Audition de M. Max Schrems, fondateur de l'association Noyb, le 26 mars 2026.*

en pratique les citoyens de la faculté d'exercer leurs droits : « *si, en tant que citoyen français, votre cas est transféré en Irlande, vous avez théoriquement la possibilité de poursuivre le régulateur irlandais pour son inaction, mais votre démarche n'a en réalité aucune chance d'aboutir si vous n'avez pas au moins 100 000 euros sur votre compte en banque. À l'issue de l'affaire Schrems II – j'étais alors poursuivi par le régulateur –, les frais juridiques se sont établis à environ 10 millions d'euros. Si j'avais perdu, j'en aurais été personnellement redevable et j'aurais été déclaré en faillite. Il se trouve que j'avais raison d'accuser le régulateur de ne pas avoir fait son travail et que j'ai gagné, mais la plupart des gens ne prendraient pas un tel risque.* »

**Le fonctionnement interne de l'autorité de protection des données irlandaise serait également en cause selon les organisations et ONG auditionnées**. M. Bastien Le Querrec, juriste membre de la Quadrature du Net, a dénoncé lors de son audition une autorité « *notoirement incapable de faire face aux* Big Tech », « *marquée par des phénomènes de pantouflage et un turnover élevé, qui entravent le traitement des plaintes et les investigations* » [(1)]. Dans le même sens, M. Max Schrems a évoqué la récente nomination de Mme Niamh Sweeney comme commissaire de la DPC, qui avait travaillé pendant six ans comme lobbyiste pour Meta, chez Whatsapp puis chez Facebook.

Comme mentionné dans la première partie de ce rapport, les revenus liés à l'activité numérique, et plus particulièrement à l'immatriculation des filiales des géants américains, représentent près de 35 % du PIB irlandais. **Le traitement par l'Irlande des plaintes concernant des acteurs majeurs de son activité économique relève, pour la rapporteure, d'un conflit d'intérêt majeur et ne peut perdurer**.

La rapporteure appelle ainsi les autorités françaises à défendre la suppression de la règle du guichet unique pour transférer la compétence de contrôle et de sanction au titre du RGPD au CEPD de pour les plus grandes plateformes.

C'est seulement ainsi qu'il sera possible de surmonter le verrou de l'Irlande et d'assurer une application effective des sanctions aux Big Tech qui y ont leur siège, le CEPD ayant démontré, à l'occasion de l'adoption de ses décisions contraignantes, sa plus grande fermeté. Son organisation collégiale, associant l'ensemble des autorités européennes compétentes, facilitera l'adhésion des États membres.

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

*(1) Table ronde sur le thème de la protection des données personnelles le 25 mars 2026.*

### 2. Des sanctions insuffisamment dissuasives ?

Le RGPD a renforcé le pouvoir de sanction des autorités de protection des données personnelles, avec des **amendes qui peuvent désormais s'élever jusqu'à 4 % du chiffre d'affaires mondial** pour une entreprise, ou 20 millions d'euros en l'absence de chiffre d'affaires. **Les amendes prononcées atteignent cependant rarement ces plafonds, ce qui peut conduire à douter de leur caractère dissuasif à l'égard des géants du numérique**.

L'article 83 du RGPD répertorie un certain nombre d'éléments dont il convient de tenir compte pour déterminer le montant de l'amende, parmi lesquels : la nature, la gravité et la durée de la violation ; le fait que la nature ait été commise délibérément ou par négligence ; les catégories de données à caractère personnel concernées par la violation ; ou toute autre circonstance aggravante ou atténuante, telle que les avantages financiers obtenus ou les pertes évitées du fait de la violation. La méthode de calcul a été précisée par des lignes directrices du CEPD adoptées le 24 mai 2023(1).

La présidente de la Cnil a fait observer à la commission d'enquête qu'il était « *plus compliqué de définir des critères très précis lorsque l'on défend un droit fondamental tel que la protection de la vie privée. Combien rapporte un biais de consentement ? Combien rapporte le refus d'accès à des données ? Ce n'est pas tout à fait la même chose que dans le domaine de la concurrence, l'Autorité de la concurrence ayant publié une grille indiquant des critères de sanction précis en fonction du préjudice causé et des sommes rapportées*. (…) ***Tout le problème est d'arriver à concilier la proportionnalité*** *– il est heureux que cette exigence s'applique dans un État de droit, où les décisions de la Cnil peuvent faire l'objet d'un recours devant le Conseil d'État –* ***et le rôle dissuasif de la sanction***. » (2)

**La procédure de résolution des litiges prévue par le RGPD a permis au CEPD d'imposer à plusieurs reprises un relèvement du montant des amendes prononcées par l'autorité cheffe de file irlandaise dans le cas des traitements transfrontaliers**. L'article 60 du RGPD prévoit en effet des mécanismes de coopération pour les traitements transfrontaliers, et notamment la possibilité pour les autorités nationales concernées de présenter des observations sur le projet qui leur est soumis par le chef de file, afin de parvenir à une décision consensuelle. En cas de désaccord persistant entre autorités, le CEPD est habilité à régler le litige, sur le fondement de l'article 65. Cette décision est contraignante pour l'autorité cheffe de file, qui peut être amenée à changer son projet de décision. Elle ne peut s'y opposer qu'en portant l'affaire devant la Cour de justice de l'Union européenne.

C'est notamment l'intervention du CEPD (3) qui a imposé que l'amende sanctionnant Meta pour avoir continué à transférer des données personnelles

*(1) CEPD, Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD, version 2.1., adoptées le 24 mai 2023.*

*(2) Audition de Mme Marie-Laure Denis, présidente de la Cnil, le 15 avril 2026.*

*(3) CEPD, décision contraignante du 13 avril 2023*

d'Européens vers les États-Unis en violation du cadre légal européen soit d'au moins 20 % du plafond légal, ce qui a ouvert la voie à la sanction de 1,2 milliard d'euros finalement prononcée par la DPC – le plafond était alors de 4 milliards selon Noyb. Entre 2018 et 2022, 75 % des projets de décision irlandais ont été invalidés par le CEPD [(1)].

**À l'inverse, des tribunaux nationaux ont pu invalider des amendes importantes prononcées par une autorité de protection des données, au nom du respect du principe de proportionnalité**. La Cour administrative du Luxembourg a ainsi cassé, le 12 mars 2026, la décision de la Commission nationale pour la protection des données luxembourgeoise, qui avait infligé en 2021 une amende historique de 743 millions d'euros contre Amazon. Comme l'a détaillé M. Thomas Dautieu, directeur de l'accompagnement juridique de la Cnil, « *la Cour a validé les manquements relevés par l'autorité luxembourgeoise, mais elle a annulé la décision car le montant de la sanction n'était pas justifié par les manquements. L'autorité de protection des données luxembourgeoise doit donc reprendre le travail pour justifier le montant initial en fonction des manquements*. » [(2)]

Les législateurs nationaux et européens doivent clairement affirmer le souhait d'utiliser pleinement l'ensemble des outils règlementaires existants, notamment par l'application de sanctions véritablement dissuasives.

*(1) ICCL, mai 2023.*

*(2) Audition de Mme Marie-Laure Denis, présidente de la Cnil, le 15 avril 2026.*

## CHAPITRE 5 – ESPIONNAGE 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

**La dépendance aux solutions d'hébergement américaines rend l'Europe particulièrement vulnérable à l'espionnage**, qu'Henri Verdier estime « *systématique* ». « *Dans le cas des États-Unis, cette pratique s'appuie sur un cadre juridique qui autorise les administrations américaines à accéder aux données sous juridiction américaine. Quant à la Chine, l'espionnage y relève d'un véritable sport national. Cette dépendance nous expose à des risques majeurs en cas de conflit et nous rend vulnérables à des opérations de manipulation de l'information* » (1), souligne-t-il.

#### 1. 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 **Fisa,** adopté en 1978, prévoit la collecte de données sur des personnes ou entités non américaines à des fins de sécurité nationale. S'il visait à l'origine la recherche d'informations ciblées sur des acteurs étatiques étrangers, il a été modifié en 2008 pour introduire un article 702 qui autorise le gouvernement américain à surveiller les communications électroniques de ressortissants étrangers hors du territoire américain, avec l'assistance des fournisseurs de services numériques qui relèvent des juridictions américaines.

Sur cette base, le procureur général et le directeur du renseignement national des États-Unis peuvent autoriser conjointement, pour une période maximale d'un an, le ciblage de personnes étrangères soupçonnées de se trouver hors des États-Unis. En vertu du quatrième amendement de la Constitution, qui requiert un mandat pour toute perquisition contre des citoyens américains, ces derniers ne peuvent être ciblés. La Cour de surveillance du renseignement étranger (Foreign Intelligence Surveillance Court – FISC*)* contrôle le programme judiciaire annuel pour vérifier de façon globale que la collecte ne concerne que des personnes non américaines à l'étranger, sans examiner précisément les informations demandées pour chaque individu. Les flux de données des *US persons* bénéficient ainsi « *d'une protection qui est à certains égards plus forte que celle prévue en Europe et leur surveillance est jugée inconstitutionnelle. Pour le reste, (…) le gouvernement américain peut faire ce qu'il veut »* a fait observer Max Schrems lors de son audition (2).

---

*(1) Audition de M. Henri Verdier, le 10 mars 2026.*

*(2) Audition de M. Max Schrems, fondateur de l'association Noyb, le 26 mars 2026.*

Dans son bilan annuel de 2025, la Cour de surveillance du renseignement étranger a déclaré avoir reçu 287 demandes : 179 ont été accordées, 91 ont été modifiées, 15 ont été partiellement rejetées, et 4 pleinement rejetées [(1)].

Adopté en 2018, le **Cloud Act** permet aux autorités américaines, disposant d'un mandat ou de l'autorisation d'un juge, d'accéder aux données hébergées, même à l'étranger, par des entreprises soumises au droit américain dans le cadre d'une enquête criminelle. Le texte vise ainsi à accélérer le temps de l'investigation, en obtenant la divulgation des données plus rapidement que ne le permettent les procédures d'entraide judiciaire internationale. Des données de citoyens européens peuvent ainsi être transmises sans que ce leur soit notifié et en dehors de tout contrôle des administrations ou tribunaux européens.

Ces législations ont pour effet de conférer aux États-Unis « *un accès total à toutes les données qui sont soit la propriété d'un fournisseur de cloud américain, soit sous sa garde ou sous son contrôle, sans limite géographique. Cet accès concerne donc n'importe quel serveur sur la planète, dès lors qu'une société américaine y a accès de quelque façon que ce soit* » conclut Max Schrems.

En Chine, la **loi sur le renseignement national**, adoptée en 2017, prévoit, en son article 7, que « *toutes les organisations et tous les citoyens doivent soutenir, assister et coopérer aux efforts des services de renseignement nationaux conformément à la loi* » et, en son article 10, que « *les services nationaux de renseignement doivent utiliser les moyens, les tactiques et les canaux nécessaires pour mener à bien leurs activités de renseignement, tant à l'intérieur qu'à l'extérieur du pays* ». La combinaison de ces deux articles pourrait ainsi obliger les entreprises chinoises à communiquer aux services de renseignement les données de citoyens européens qu'elles détiennent.

Il s'agit d'une **menace directe pour la souveraineté et l'intelligence économique**. Par l'application de ce droit extraterritorial, les services de renseignement de pays tiers seraient susceptibles d'accéder aux données sensibles des États, aux secrets industriels d'entreprises stratégiques, ou encore à des résultats de recherche de pointe hébergés sur des infrastructures étrangères.

**Ces menaces sont largement sous-estimées par les grandes entreprises françaises**. M. Henri Verdier l'a illustré par l'exemple de M. Guillaume Poupard, qui a dirigé le pôle Sécurité des systèmes d'information du ministère des armées puis pendant quasiment dix ans l'Anssi : « *Il m'a rapporté une conversation avec le dirigeant d'une entreprise du CAC40 à qui il conseillait de ne pas héberger ses données chez Amazon Web Services, en raison des risques d'espionnage. Son interlocuteur lui avait alors répondu qu'il n'avait pas de preuves. Cela illustre bien l'état d'esprit qui prévaut : on tend à considérer le numérique comme une simple*

*(1) Rapport du directeur du bureau administratif des tribunaux américains sur les activités de la Cour de surveillance du renseignement étranger pour 2025.*

*fonction support, un peu ingrate, au même titre que l'immobilier ou la cantine, alors qu'il s'agit d'une fonction éminemment stratégique.* » (1)

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

#### *a. L'obligation pour les entreprises américaines de répondre aux demandes des autorités fédérales*

**La commission d'enquête a interrogé les représentants de Microsoft, d'Amazon Web Services et de Google sur les suites qu'ils donnaient aux requêtes émises par les autorités américaines**.

Mme Corine de Bilbao, présidente de Microsoft France, a assuré que les services juridiques de Microsoft vérifiaient toujours la légalité de la demande qui leur était transmise, et notamment si elle n'était pas « *imprécise, excessive, ou en conflit avec le droit d'un autre pays* ». Microsoft affirme s'être par ailleurs, « *engagé contractuellement à contester systématiquement les demandes devant les tribunaux, qu'elles relèvent du Cloud Act ou du Fisa* ». S'agissant d'AWS, M. Arnaud David, directeur des affaires publiques, a indiqué que la société essayait de rediriger les demandes vers ses clients : « *Nous considérons en effet que nous n'avons pas de légitimité pour y répondre, dans la mesure où nous n'avons pas d'accès aux données. Les clients sont plus à même de le faire – prenons le cas d'un opérateur de forums ou de réseaux sociaux, qui a une relation directe avec ses utilisateurs finaux* » (2).

Ces procédures internes et recours juridiques ne permettent cependant que de retarder la réponse aux injonctions américaines. À la question de la rapporteure « *si un juge, après contestation, valide la demande d'accès du gouvernement américain à des données françaises, publiques ou privées, avez-vous l'obligation légale de les transmettre ?* », les auditionnés ont refusé ostensiblement d'apporter une réponse claire, à l'exception de M. Frédéric Geraud de Lescazes, directeur des affaires publiques de Google France, qui a déclaré : « *Google Cloud respecte l'État de droit : si un juge allemand, canadien, chilien, américain ou français nous demande de coopérer, nous le faisons* ». **Étant soumis au droit américain, les *hyperscalers* ont de fait l'obligation juridique de transférer les informations demandées par les agences fédérales**.

Cela confirme les propos tenus par un représentant de Microsoft devant la commission d'enquête sénatoriale sur la commande publique qui l'interrogeait sur

---

*(1) Audition de M. Henri Verdier le 10 mars 2026.*

*(2) Table ronde, ouverte à la presse, réunissant des représentants en France des Gafam, le 13 mai 2026 :*
- *Mme Corine de Bilbao, présidente de Microsoft France, et M. Philippe Limantour, directeur technologie et cybersécurité ;*
- *M. Sébastien Missoffe, directeur général de Google France et M. Frédéric Geraud de Lescazes, directeur des affaires publiques de Google Cloud ;*
- *M. Julien Lépine, représentant en France d'Amazon Web Services Europe, Moyen-Orient, Afrique (AWS EMEA), et M. Arnaud David, directeur des affaires publiques France et Union européenne de AWS.*

sa capacité à garantir que les données des citoyens français hébergées par Microsoft France ne seraient jamais transmises à des autorités étrangères sans l'accord des autorités françaises. M. Anton Carniaux, directeur des affaires publiques et juridiques, avait reconnu sous serment : « *Non, je ne peux pas le garantir* » [(1)]. Il avait été licencié quelques jours plus tard – sans qu'il n'y ait « *absolument aucun lien* » avec son audition selon la présidente de Microsoft France [(2)].

Mme de Bilbao affirme que « *Microsoft n'a jamais divulgué de données d'un client du secteur public français à des autorités étrangères, y compris américaines* ». Elle a cependant dû reconnaître avoir transmis les données d'une entreprise européenne au gouvernement américain : « *Pour les entreprises privées, nous avons un cas dans les trois dernières années* ». S'agissant d'Amazon, M. Arnaud David a déclaré qu'« *aucune demande adressée à AWS n'a été suivie d'une transmission au gouvernement américain de données appartenant à des entreprises ou des gouvernements et situées hors des États-Unis* ».

**Ces déclarations, outre qu'elles ne sont pas vérifiables, n'offrent qu'une vision partielle de l'ensemble des communications de données réalisées par ces entreprises.**

Les rapports de transparence publiés par Microsoft [(3)], Google [(4)] et Amazon [(5)] témoignent de la réception de nombreuses demandes d'informations sur leurs utilisateurs, provenant de l'ensemble des autorités gouvernementales du monde, le plus souvent dans le cadre d'enquêtes criminelles. La localisation géographique des personnes morales ou physiques ciblées n'est cependant pas spécifiée. Au deuxième semestre 2025, il est possible de relever les éléments suivants :

– AWS indique avoir reçu 1 870 demandes gouvernementales, dont 444 des États-Unis ;

– Microsoft fait état de 5 587 requêtes émanant du gouvernement américain sur des utilisateurs, dont 75 % ont donné lieu à la transmission d'informations – du contenu pour 16 % et des métadonnées pour 59 %. 115 de ces demandes visaient à obtenir des données de contenu stockées en dehors des États-Unis – le nombre de requêtes concernant des métadonnées n'est pas indiqué ;

---

*(1) Rapport fait au nom de la commission d'enquête sur les coûts et les modalités effectifs de la commande publique et la mesure de leur effet d'entraînement sur l'économie française, par M. le sénateur Dany Wattebled, enregistré à la présidence du Sénat le 8 juillet 2025.*

*(2) Table ronde, ouverte à la presse, réunissant des représentants en France des Gafam, le 13 mai 2026 :*
*– Mme Corine de Bilbao, présidente de Microsoft France, et M. Philippe Limantour, directeur technologie et cybersécurité ;*
*– M. Sébastien Missoffe, directeur général de Google France et M. Frédéric Geraud de Lescazes, directeur des affaires publiques de Google Cloud ;*
*– M. Julien Lépine, représentant en France d'Amazon Web Services Europe, Moyen-Orient, Afrique (AWS EMEA), et M. Arnaud David, directeur des affaires publiques France et Union européenne de AWS.*

*(3) https://www.microsoft.com/en-us/corporate-responsibility/reports/government-requests/customer-data*

*(4) https://transparencyreport.google.com/user-data/overview*

*(5) https://d1.awsstatic.com/onedam/marketing-channels/website/aws/en_US/whitepapers/compliance/Amazon_AWS_Information_Request_Report_H2_2025.pdf*

– Google indique avoir reçu en moyenne 287 000 demandes d'informations, dont 60 000 émanant du gouvernement américain – 89 % de ces dernières ont donné lieu à des divulgations.

**S'agissant spécifiquement de la transmission d'informations relatives à des personnes ou des entités européennes, les rapports contiennent des éléments qui contredisent les déclarations d'intention des *hyperscalers***. Si le rapport d'Amazon se borne à indiquer qu'il n'y a eu aucune « *divulgation au gouvernement américain de données de contenu d'entreprise ou de gouvernement situés en dehors des États-Unis »,* Microsoft déclare avoir reçu trois « ***mandats émis par les autorités américaines ayant donné lieu à la divulgation de contenu de données d'entreprises stockées en dehors des États-Unis*** », **dont une entreprise européenne**. **Au premier semestre 2025, la société déclarait déjà avoir accédé à ce type de demande pour cinq entreprises non-américaines, dont une européenne, « *sous-traitant du gouvernement américain* ».**

**Ces déclarations sont, par ailleurs, très lacunaires, laissant supposer que les cas de transmissions de données de citoyens européens pourraient être bien plus nombreux que ce qui est allégué. Il convient de relever notamment trois limites.**

Tout d'abord, elles **ne portent que sur les « *data content* »,** ou contenu de données – c'est-à-dire des textes, des courriels, des photos ou des vidéos – **sans inclure les métadonnées –** le destinataire, l'expéditeur, le journal d'activités –**,** qui sont pourtant aussi recensées par les rapports de transparence. Or, ces métadonnées sont tout aussi sensibles, comme l'a rappelé M. Martin Untersinger lors de son audition : « *Je me souviens d'un ancien chef de la NSA, l'Agence nationale de sécurité américaine, qui avait dit : " Nous tuons des gens en nous basant sur les métadonnées. " Il est donc absolument crucial de les protéger. En effet, le secret des sources, ce n'est pas tant garder confidentiel ce que vous a dit quelqu'un, mais avec qui vous avez discuté.* » (1)

**Elles ne portent que sur les entreprises, et non sur les utilisateurs particuliers**. Rien n'est donc dit sur les transmissions aux autorités américaines de données ou de métadonnées de citoyens européens.

**Enfin, il n'y a aucune transparence sur les requêtes émises en vertu du Fisa ou de *National Security Letters***. Les lois relatives à la sécurité nationale interdisent en effet aux entreprises américaines de communiquer ces éléments autrement que sous la forme de fourchettes très larges. Elles ne sont pas davantage autorisées à notifier la divulgation à leurs clients, comme l'a confirmé M. Geraud de Lescazes : « *le cadre réglementaire américain ne nous permet pas, à nous, entreprise américaine, de communiquer sur ces éléments ».* Au premier semestre 2025, les rapports de transparence donnaient l'aperçu suivant :

---

*(1) Audition de M. Martin Untersinger, journaliste au* Monde, *et MM. Antoine Schirer et Sébastien Bourdon, journalistes indépendants, le jeudi 26 mars 2026.*

– Amazon indique seulement que ses réponses « *à ces demandes dépendent de la nature de la demande. Amazon communique le nombre de ces demandes dans certaines fourchettes autorisées par la loi. (...) La fourchette de déclaration est comprise entre 0 et 249 pour toutes les demandes relatives à la sécurité nationale adressées à Amazon (y compris AW*S) » ;

– Google indique pour sa part avoir reçu en vertu de la loi Fisa, au niveau mondial, entre 0 et 499 demandes portant sur le contenu (messages, photos, vidéos), concernant de 177 500 à 177 900 comptes, et entre 0 et 499 demandes portant sur les métadonnées, concernant de 75 500 à 75 999 comptes ;

– Microsoft fait état de 0 à 499 demandes de divulgation de contenus sur la base du Fisa, concernant 33 500 à 33 999 comptes.

***b. Des barrières techniques à l'efficacité non démontrée***

Les *hyperscalers* auditionnés ont tous revendiqué la mise en place de solutions techniques rendant matériellement impossible l'accès par leur personnel aux données des clients, et *de facto* leur transmission aux autorités américaines.

M. Arnaud David, directeur des affaires publiques d'AWS a ainsi déclaré : « O*n ne peut communiquer des données sur une base légale qu'à partir du moment où on peut techniquement y avoir accès. Or nous utilisons un certain nombre de technologies qui ne permettent pas d'accéder aux données des clients* ». La représentante de Microsoft a défendu la même position : « *Microsoft est dans l'impossibilité de fournir les données lorsque les clés de chiffrement ont été utilisées et que celles-ci sont dans le coffre du client, dans le cadre du* confidential computing, *ou lorsqu'elles sont hébergées dans un* cloud *sécurisé, certifié SecNumCloud* » (1).

La première garantie de confidentialité consisterait dans le chiffrement systématique des données des clients, au repos ou en transit. M. Vincent Strubel, directeur général de l'Anssi, a néanmoins souligné que « ***l'argument souvent avancé par certains acteurs du cloud est insuffisant car même si les données sont chiffrées, leur traitement implique que la clé de déchiffrement soit présente dans le cloud, aux côtés des données, ce qui permet au prestataire d'y accéder*** » (2).

Le ***confidential computing***, ou informatique confidentielle, vise à remédier à cette limite, en créant des environnements isolés et étanches, qui fonctionnent indépendamment du système d'exploitation hôte et auxquels même les administrateurs ne pourraient pas accéder. Les données entrent et sortent chiffrées, et l'application ne s'exécute qu'à l'intérieur de l'espace sécurisé. Cela permettrait de protéger les données et leur traitement à l'encontre des fournisseurs de cloud.

---

*(1) Table ronde réunissant des représentants en France des Gafam le 13 mai 2026.*

*(2) Audition de M. Vincent Strubel le 30avril 2026.*

Microsoft a mis au point sa technologie de calcul confidentiel en 2014, avant de la rendre opérationnelle dans Azure en 2017. M. Philippe Limantour a expliqué que « *les clés de chiffrement font l'objet d'une hiérarchie. Au sommet se trouve la possibilité pour le client de gérer sa propre clé, dont il est le seul détenteur – s'il perd sa clé, il perd ses données. Les clés peuvent être stockées dans un coffre muni d'un mécanisme de calcul confidentiel, provenant de l'un de nos trois fournisseurs ; ces mécanismes nous empêchent physiquement et techniquement d'accéder à la clé.* » (1)

Google Cloud a également mis en place un système de chiffrement reposant sur une gestion externalisée des clés de chiffrement, appelé EKM (*external key management)*. Les entreprises clientes peuvent ainsi choisir de déposer leurs clés chez l'un de leurs partenaires, notamment Thalès.

Enfin, AWS a développé la solution AWS Nitro, intégrée directement à ses serveurs. Nitro permettrait de créer des enclaves, des machines virtuelles avec des processeurs et une mémoire isolée des instances du système. Invité à présenter la technologie, M. Julien Lépine a affirmé : « *Par défaut, Nitro permet à tous nos clients, quand ils lancent gratuitement des infrastructures, de bénéficier de l'isolation de leurs données, qu'elles soient en traitement, en transit ou en repos ; celles-ci sont soit chiffrées, soit complètement isolées, sans aucune possibilité d'accès pour les opérateurs. »* Les clés de chiffrement sont gérées par les services d'AWS ou stockées auprès de prestataires comme Devoteam ou Thales (2).

Ces solutions ne seraient cependant pas encore matures sur le plan technologique. Le directeur général de l'Anssi estime en effet que « ***les technologies de* confidential computing *(…) ne sont aujourd'hui ni suffisamment fiables ni généralisables, ce qui ne permet pas de se dispenser de la confiance accordée au prestataire*** » (3).

Il n'est par ailleurs pas certain que l'argument d'une impossibilité technique suffise à supprimer le risque juridique, en exonérant les fournisseurs de cloud américains du respect des lois extraterritoriales américaines. Face à une injonction des États-Unis, les entreprises concernées pourraient se trouver contraintes de trouver un moyen technique de contourner ces verrous matériels. Le journaliste Mourad Krim relevait dans IT Social que « *la jurisprudence américaine a déjà démontré qu'elle pouvait ordonner la remise d'éléments techniques ou la modification de systèmes pour permettre l'accès, si la structure capitalistique l'autorise. Cette garantie ne saurait donc constituer, à elle seule, un bouclier contre le risque d'extraterritorialité.* » (4).

---

*(1) Table ronde réunissant des représentants en France des Gafam le 13 mai 2026.*

*(2) Ibid.*

*(3) Audition de M. Vincent Strubel le 30 avril 2026.*

*(4) Mourad Krim, « AWS European Sovereign Cloud : étanche technologiquement, perméable juridiquement »,* IT social*, 16 janvier 2026*

*c. Une nécessaire immunité au droit extraterritorial*

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**. « *Aucune réponse purement technologique ne permet de faire face à ces risques puisque le chiffrement ne protège pas du Cloud Act, et encore moins d'un* kill switch, observe le directeur général de l'Anssi. *Cette réalité conduit à s'interroger sur la nationalité des fournisseurs, sans pour autant s'en tenir à une lecture binaire, car c'est l'ensemble de la chaîne de valeur qu'il faut examiner* » (1).

**Le référentiel SecNumCloud élaboré par l'Anssi, tend ainsi à garantir l'immunité du fournisseur cloud au droit extraterritorial, en imposant des exigences capitalistiques, techniques et organisationnelles** (2) :

– **le prestataire qualifié doit être européen** : son siège doit être établi dans l'Union européenne et son capital ne doit pas être détenu, individuellement à plus de 24 %, et collectivement à plus de 39 %, par des entités tierces possédant leur siège, leur administration centrale ou leur établissement principal à l'extérieur de l'Union européenne. Les entités tierces ne doivent pas disposer d'un droit de veto, ni du droit de désigner la majorité des membres des organes d'administration, de direction ou de surveillance du prestataire ;

– s'il a recours à des **sous-traitants ou fournisseurs non européens**, le prestataire doit garantir que ces derniers **n'ont en aucun cas accès aux données de ses clients** ;

– **le prestataire doit être autonome dans l'exploitation de la solution**.

M. Vincent Strubel précise néanmoins que « *le SecNumCloud ne garantit pas la protection des données contre l'opérateur de cloud, mais par celui-ci contre des tiers* ».

## B. LA MENACE D'UNE COUPURE DES SERVICES NUMÉRIQUES

**Le durcissement des relations transatlantiques oblige à considérer l'éventualité où une décision du président américain imposerait une coupure des services numériques fournis à l'Union européenne, qu'elle soit générale ou ciblée sur certaines personnalités**. Une telle menace constitue un levier de pression considérable à l'encontre des pays européens.

**Cette menace s'est matérialisée avec le blocage des modèles d'intelligence artificielle Mythos 5 et Fable 5 d'Anthropic**. Le 12 juillet, l'entreprise a annoncé suspendre l'accès à ces deux modèles d'IA suite aux ordres

*(1) Audition de M. Vincent Strubel le 30 avril 2026.*

*(2) Anssi, Référentiel d'exigences pour les prestataires de services d'informatique en nuage (SecNumCloud), version 3.2 du 8 mars 2022.*

des autorités américaines de couper l'accès à tout ressortissant étranger, à l'intérieur ou à l'extérieur des États-Unis, y compris à ses propres « employés étrangers » (1).

### 1. Le ciblage de personnalités : le cas du juge Guillou

En réaction aux enquêtes ouvertes par la Cour pénale internationale (CPI) sur les crimes de guerre présumés de soldats américains en Afghanistan et du gouvernement israélien dans la bande de Gaza, **le président des États-Unis a pris l'*executive order* 14203 imposant des sanctions à la CPI**. Il est notamment prévu d'imposer aux personnes visées : l'interdiction de se rendre sur le territoire américain, pour elles et leur famille proche ; le gel de leurs avoirs détenus aux États-Unis ; et l'**interdiction pour toute personne physique ou morale américaine, y compris leurs filiales et leurs employés, de leur fournir des biens et services**. Aucun recours juridictionnel ne permet de contester la décision. Ces mesures sont mises en œuvre par l'Office of Foreign Assets Control (OFAC) du département du Trésor américain, qui tient une liste recensant les personnes physiques et morales sous sanctions économiques – essentiellement des terroristes, des trafiquants ou des personnes coupables de graves violations des droits de l'homme.

Comme l'indique le juge M. Nicolas Guillou, juge à la CPI (2) : « *Une des principales difficultés est que ce régime de sanction a été élaboré en commun par l'Europe et les États-Unis pour lutter contre le terrorisme. On ne s'est donc pas beaucoup posé ces questions au début : les sanctions ont été conçues comme émanant d'une décision de l'exécutif, quasiment sans contrôle du juge – la Cour de justice de l'Union européenne a imposé un contrôle du juge en 2008, par l'arrêt Kadi, mais c'est à peu près tout. Personne n'avait imaginé qu'un système visant ceux qui violent le droit international pourrait être retourné contre ceux qui sont censés le faire respecter.* »

Le décret ne visait à l'origine que le procureur de la CPI, Karim Khan, mais le secrétaire d'État Marco Rubio a progressivement étendu le champ des sanctions à dix autres magistrats de la CPI. Le décret du 20 août 2025 cible notamment le juge français Nicolas Guillou, pour avoir autorisé l'émission de mandats d'arrêt internationaux à l'encontre du Premier ministre israélien Benyamin Netanyahou et de l'ancien ministre de la défense israélien Yoav Gallant.

**Le juge Guillou a témoigné devant la commission d'enquête de l'ampleur des conséquences de ces sanctions américaines sur sa vie quotidienne en Europe**, particulièrement fortes dans deux domaines : les services numériques et les moyens de paiement, en raison de la prépondérance des acteurs américains. « ***Ma vie personnelle est devenue un laboratoire de la perte de souveraineté****,* a-t-il ainsi déclaré. *Ce qui m'arrive me fait réaliser l'ampleur de notre dépendance au quotidien :* ***tout ce qui ne fonctionne plus dans ma vie quotidienne, c'est de la dépendance***. »

---

*(1) https://www.anthropic.com/news/fable-mythos-access*

*(2) Audition de Nicolas Guillou, juge à la Cour pénale internationale, le mercredi 8 avril 2026*

### *a. Une suspension automatique des services numériques américains*

Dans un contexte de quasi-monopole des plateformes américaines, **le juge Guillou a expliqué devant la commission d'enquête s'être trouvé privé de nombreux services numériques** : ses réservations d'hôtel sur les plateformes Booking ou Expedia ont été annulées ; il n'a pas pu réserver une place de concert à l'Olympia car le seul site de revente était américain et a bloqué sa transaction ; et il n'a plus accès aux grandes plateformes de musique ou de cinéma… Lors d'une conférence de presse, le juge Guillou a dit avoir l'impression de « *vivre comme dans les années 1990* » (1). L'autre juge européenne de la CPI sanctionnée, Mme Beti Hohler, a témoigné de la même situation au Parlement européen, déclarant que ses comptes Apple, iCloud, Amazon, et Paypal avaient tous été bloqués ou résiliés, sans avertissement préalable (2).

**Les personnes sanctionnées ne sont pas prévenues en amont, risquant dès lors de « *perdre accès à toutes leurs archives numériques du jour au lendemain* »**, notamment si elles ont souscrit des services de cloud.

La commission d'enquête a interrogé les représentants français de Google, Amazon Web Services et Microsoft sur la suspension de leurs services à M. Guillou. Si le directeur des affaires publiques d'AWS, M. Arnaud David, a éludé en arguant que les clients d'AWS étaient essentiellement des entreprises, **M. Frédéric Géraud de Lescazes, directeur des affaires publiques de Google Cloud, a confirmé formellement que M. Guillou ne pouvait plus ouvrir de compte Gmail ni utiliser la suite de Google, même à titre particulier**.

La présidente de Microsoft France a, pour sa part, assuré que Microsoft n'avait pas coupé ses services à la CPI. Pourtant, la presse avait fait état, en mai 2025, de la fermeture de la boîte mail Outlook du procureur de la CPI Karim Khan. Ce changement de position pourrait s'expliquer par la volonté de Microsoft d'éviter que les sanctions américaines ternissent son image à l'étranger, comme l'a suggéré M. Nicolas Guillou lors de son audition : « *la position de Microsoft a évolué avec le temps – à certains moments, il ne fallait plus rien fournir aux personnes sanctionnées ; à d'autres, ce n'était plus le cas. Microsoft fait un arbitrage assez fort entre ses obligations juridiques et les conséquences pour son* business model. » (3)

**Ces sanctions ont d'autant plus d'impact que les alternatives numériques européennes sont encore peu développées**. Elles peuvent cependant avoir un effet accélérateur, en incitant les donneurs d'ordre à s'orienter vers des solutions non soumises au droit américain. La CPI a annoncé, en octobre 2025, travailler à la migration de son environnement de travail de Microsoft vers le

---

*(1) Karl Meyer,* « J'ai un peu l'impression de vivre dans les années 1990 » : l'alarme de ce juge de la Cour pénale internationale qui ne peut plus utiliser Visa ou Mastercard, *Les Échos, le 18 février 2026.*

*(2) Audition de Mme Beti Hohler devant la commission des affaires juridiques (JURI) et la sous-commission sur les droits humains (DROI) du Parlement européen le 24 février 2026.*

*(3) Audition de M. Nicolas Guillou le 8 avril 2026.*

logiciel open source OpenDesk, développé par le Centre allemand pour la souveraineté numérique de l'administration publique (*Zendis)*. « *Les solutions européennes que nous avons identifiées ne constituent pas encore un équivalent parfait des produits américains, mais elles vont nous permettre de fonctionner en autonomie »* a confirmé le juge Guillou lors de son audition.

***b. Le retrait des moyens de paiement***

**Le juge Guillou a également vu annuler sa carte bancaire et ne dispose plus de moyen de paiement** : « *En tout cas, **aucune banque ne m'a proposé un compte avec une carte CB**. (...) J'ai essayé de me rapprocher indirectement de plusieurs banques, mais aucune ne souhaite avoir des clients sous sanctions* ». (1)

Le juge Guillou n'a pas pu obtenir de carte bancaire qui fonctionnerait uniquement sur le réseau CB ; l'essentiel des cartes sont co-badgées avec Visa ou Mastercard, ce qui entraîne l'application du droit américain.

S'il est techniquement possible d'émettre une carte bancaire relevant exclusivement du réseau CB (2), la direction générale du Trésor a indiqué à la rapporteure que, **bien que certains établissements français aient pu historiquement émettre des cartes « CB only » jusqu'au début des années 2010, cette pratique semble avoir disparu** (3).

Par ailleurs, les établissements bancaires qui lui délivreraient une telle carte pourraient s'exposer à un risque juridique aux États-Unis, à raison de « *la tenue du compte, sur laquelle pèse également un risque de sanction*. », selon M. Erick Lacourrège (4).

Il est à noter que le juge Guillou n'a pas subi de fermeture de compte jusqu'ici, mais que la Banque de France suit de près l'évolution de la situation et examine les solutions dérogatoires qui pourraient être mises en place s'il était bloqué. La magistrate Beti Hohler, et la rapporteure spéciale des Nations Unies sur les territoires occupés, Francesca Albanese, ont vu leur compte bancaire fermé en Slovénie et en Italie (5).

**L'obstacle principal à la délivrance d'une carte bancaire serait ainsi l'application extraterritoriale du droit américain, liée à la suprématie du dollar**. Si *l'executive order* 14203 ne s'applique qu'aux *US Persons* – c'est-à-dire aux citoyens américains, aux résidents permanents étrangers, et aux sociétés

---

*(1)* Ibid.

*(2) Le règlement (UE) 2015/751 du 29 avril 2015 relatif aux commissions d'interchange pour les opérations de paiement liées à une carte n'interdit pas le mono-badgeage ni n'impose le co-badgeage.*

*(3) Réponses écrites de la direction générale du Trésor au questionnaire de la rapporteure.*

*(4) Table ronde sur les services de paiement le 8 avril 2026.*

*(5) Coalition pour la Cour pénale internationale,* La guerre juridique menée par les États-Unis contre le système de justice internationale, *23 avril 2026*

*(https://coalitionfortheicc.org/sites/default/files/cicc_documents/Criminalising%20Accountability%20-%202026_0.pdf )*

américaines, ainsi qu'à leurs filiales et employés à l'étranger –, les États-Unis pourraient poursuivre des entreprises non américaines pour des opérations qui n'ont pas lieu sur le territoire américain, sur le fondement de larges critères de rattachement : l'utilisation du dollar ; le transit par des serveurs du système financier américain ; ou la cotation à la bourse de New York. « *La question de l'extraterritorialité (...) est liée au dollar, par lequel les États-Unis peuvent atteindre toute personne et la menacer de sanctions. Or, il est quasi impossible pour une entité financière en Europe de ne jamais effectuer de transaction en dollar* », a fait valoir Mme Maya Atig, présidente de la Fédération bancaire française.

De fait, plusieurs banques françaises ont dû s'acquitter de lourdes pénalités auprès des régulateurs américains pour avoir contourné les embargos imposés par les États-Unis à l'encontre de Cuba, de l'Iran ou du Soudan – 8,9 milliards de dollars pour BNP Paribas en 2014 et 1,3 milliard de dollars pour la Société générale en 2018. La compétence américaine se fondait sur le fait que les transactions incriminées étaient effectuées en dollars et se traduisaient par une opération-reflet dans les chambres de compensation américaine (1).

**Ces précédents ne sont cependant pas transposables au cas du juge Guillou, dans la mesure où les transactions qui lui seraient destinées seraient réalisées en euros**. La situation est différente pour les ressortissants d'autres régions du monde extrêmement dépendantes du dollar, notamment en Amérique latine, où la magistrate Luz del Carmen Ibáñez Carranza, également sous sanction, témoignait que « *les principales transactions commerciales s'effectuent en dollars* ». Au contraire, « *les transactions au sein de la zone euro sont effectuées via l'espace unique de paiement en euros (SEPA) un réseau de paiement européen qui permet d'effectuer des virements bancaires en euros entre les pays participants sans recourir au dollar américain ni passer par le système américain* » (2). **L'idée selon laquelle les établissements bancaires européens devraient se conformer aux sanctions américaines, même pour des transactions réalisées en euros, relève d'une conception très extensive de l'extraterritorialité, qui n'a jamais été confirmée par une juridiction américaine** (3).

L'impuissance affichée par la Fédération bancaire française pourrait dès lors s'assimiler aux **comportements d'*over-compliance*, ou surconformité, adoptés par certaines entreprises européennes**, par crainte des conséquences néfastes pour leurs activités commerciales aux États-Unis. La Coalition pour la CPI a mis en évidence, dans son rapport du 23 avril 2026, cette mise en conformité automatique qui a conduit « *des banques et des institutions financières non américaines à appliquer ces mesures extraterritoriales, même pour des transactions*

---

*(1) Institut Montaigne,* Extraterritorialité américaine : une arme à double tranchant*, décembre 2024.*

*(2) Coalition pour la Cour pénale internationale,* La guerre juridique menée par les États-Unis contre le système de justice internationale, *23 avril 2026*

*(3) Emmanuel Breen, La compétence américaine fondée sur le dollar : réalité juridique ou construction politique ?, Groupe d'études géopolitiques, Juil 2021, 55-61*

*qui ne comportent aucun lien ni aucune forme de connexion avec les États-Unis ou le dollar* » (1).

**Tout en exprimant la solidarité du secteur bancaire à l'égard du juge Guillou, Mme Maya Atig, directrice générale de la FBF, a concédé une forme d'attentisme : « *nous n'avons pas de solution à apporter* ».** Elle a reconnu que la Fédération Bancaire Française (FBF), qui investit pourtant très régulièrement le champ du lobbying aux niveaux national et international, comme l'a relevé le président Philippe Latombe, n'avait « *pas formulé de propositions de négociation internationale sur ce sujet qui relève de l'ultra-régalien* », quand bien même leurs clients particuliers et professionnels sont directement concernés.

Ces pratiques d'*over-compliance* ne sont d'ailleurs pas propres au secteur bancaire, M. Nicolas Guillou ayant exposé devant la commission d'enquête comment deux acteurs français du secteur de l'assurance, AXA et MSH International, avaient suspendu le remboursement de ses dépenses de santé sans l'en informer : « *En pratique, deux entreprises françaises ont arrêté de rembourser les dépenses de santé d'un citoyen français, alors qu'elles ont été faites sur le sol européen, qu'il n'y a aucun élément de rattachement aux États-Unis, que la transaction n'est pas en dollars et qu'aucune des parties n'est de nationalité américaine. Des sociétés françaises vont s'aligner sur les États-Unis parce qu'elles ne veulent pas prendre de risques par rapport à d'éventuelles sanctions, secondaires ou autres. Leur objectif est en tout cas de pouvoir commercer le plus possible avec les États-Unis Nous avons affaire à une logique qui consiste globalement à maximiser les profits et, pour cela, elles désassurent les citoyens qui sont censés bénéficier de leurs services.* » (2)

**Face à cette situation, le président et la rapporteure ont écrit au président de la République, M. Emmanuel Macron, le 14 avril 2026, pour dénoncer *« l'usage du droit américain comme arme économique »*** et alerter sur le **risque que de telles sanctions puissent, à l'avenir, cibler « *des entreprises ou des États qui seraient considérés comme des ennemis par le dirigeant de la première puissance mondiale.* »** Ils appelaient à ce que le problème des dépendances des services de paiement puisse être abordé dans le cadre du G20, en invitant la France à porter cette initiative dès la réunion des ministres des finances et des gouverneurs des banques centrales du 16 avril 2026, en vue du sommet des chefs d'État prévu à Miami les 14 et 15 décembre prochains.

M. Philippe Laulanie, directeur général du Groupement des cartes bancaires (GIE CB), a déclaré « *Quant à la situation du juge Guillou, **des décisions devront être prises pour que nous puissions distribuer des cartes bancaires à des citoyens menacés de sanctions. Des pistes ont été évoquées, telles que l'émission de cartes par une entité immune de la BCE par exemple***.* » (3)

---

*(1) Coalition pour la Cour pénale internationale,* La guerre juridique menée par les États-Unis contre le système de justice internationale, *23 avril 2026*

*(2) Audition de M. Nicolas Guillou le 8 avril 2026.*

*(3) Table ronde sur les services de paiement le 8 avril 2026.*

### *c. Une regrettable inaction de l'Union européenne*

Si plusieurs États membres et la Commission européenne ont apporté un soutien clair à M. Nicolas Guillou et à Mme Beti Hohler, **aucune action concrète n'a été engagée pour les protéger contre les conséquences des sanctions américaines**.

Malgré les appels en ce sens, **la Commission européenne n'a jusqu'ici pas activé le règlement dit de blocage du 22 novembre 1996** (1). Celui-ci permet de contrecarrer les effets extraterritoriaux des législations américaines de sanction listées dans l'annexe au règlement, lorsqu'ils portent atteinte aux intérêts des entreprises et des citoyens européens. Il prévoit quatre mesures complémentaires :

– priver d'effet sur le territoire de l'Union européenne les législations ou décisions qui prévoient ces sanctions extraterritoriales ;

– interdire aux opérateurs européens de se conformer aux prescriptions ou interdictions adoptées sur leur fondement, sauf sur dérogation accordée par la Commission européenne si le non-respect de ces prescriptions lèse gravement leurs intérêts ;

– obliger toute personne dont les intérêts économiques ou financiers sont affectés directement ou indirectement par de telles législations à en informer la Commission sous trente jours ;

– ouvrir le droit aux opérateurs européens d'être indemnisés de tout dommage découlant de l'application des sanctions extraterritoriales par les personnes qui en sont à l'origine.

Le règlement laisse à chaque État membre le soin de déterminer les sanctions à imposer en cas d'infraction. La France a choisi de l'inscrire dans l'article 459 du code des douanes, qui prévoit des sanctions pénales à l'encontre des opérateurs qui contreviennent à la législation et à la réglementation en matière de relations financières avec l'étranger.

Il appartient à la Commission d'activer le règlement de blocage contre un texte spécifique. Conformément à l'article premier, deuxième alinéa, du règlement, elle doit pour ce faire modifier l'annexe en adoptant un acte délégué. Le Parlement européen et le Conseil ont toutefois la capacité de s'opposer à son entrée en vigueur, respectivement à la majorité absolue et à la majorité qualifiée, dans un délai de deux mois à compter de la notification de l'acte par la Commission. La Commission a mis en œuvre cette compétence en 2018, pour mettre à jour le règlement afin d'étendre son application aux sanctions extraterritoriales rétablies par les États-Unis contre l'Iran (2).

---

*(1) Règlement (CE) n° 2271/96 du Conseil du 22 novembre 1996 portant protection contre les effets de l'application extraterritoriale d'une législation adoptée par un pays tiers, ainsi que des actions fondées sur elle ou en découlant.*

*(2) Règlement délégué (UE) 2018/1100 de la Commission du 6 juin 2018 modifiant l'annexe du règlement (CE) n° 2271/96 du Conseil portant protection contre les effets de l'application extraterritoriale d'une législation adoptée par un pays tiers, ainsi que des actions fondées sur elle ou en découlant.*

**La Commission s'est cependant refusée jusqu'à présent à ajouter les sanctions américaines contre la CPI dans le champ du règlement de blocage, faute de consensus entre les États membres**. La porte-parole de la Commission pour le marché intérieur, Mme Siobhan McGarry a ainsi déclaré que « *la voie diplomatique et la recherche de solutions ciblées étaient privilégiées* » [(1)]. « *C'est probablement à ce niveau que ma déception a été la plus forte,* a déclaré le juge Guillou. *Selon moi, en matière de protection de la souveraineté européenne, autant le Parlement européen souhaite vraiment avancer, autant* ***il n'y a pas de prise de conscience des enjeux et des risques au sein de la Commission européenne, pour l'instant***. » [(2)]

Si la France, la Belgique et la Slovénie sont favorables à l'activation du règlement, d'autres États membres s'inquiètent qu'elle n'entraîne des mesures de rétorsion américaines, notamment de nouvelles hausses de droits de douane. « ***Un certain nombre d'États, de groupes ou de commissaires européens ont peur de déclencher l'application du règlement, car ils craignent de déplaire aux États-Unis*** *»,* selon M. Guillou.

Les opposants à l'application du règlement de blocage mettent également en avant sa faible efficacité, étayée par plusieurs rapports parlementaires [(3)]. Les entreprises européennes se trouveraient confrontées à un **conflit de normes**, entre le droit américain et le droit européen, qui les exposeraient à une double peine. Les diplomates de la Représentation permanente de la France auprès de l'Union européenne, rencontrées par la rapporteure et le président lors de leur déplacement à Bruxelles, considèrent néanmoins que **le règlement de blocage constituerait un « écran protecteur », dont pourraient se prévaloir les opérateurs incriminés devant les juridictions américaines**. Il clarifierait en outre le fait que les fournisseurs de services européens ne doivent pas appliquer les sanctions extraterritoriales visant la CPI.

**Le juge Guillou a indiqué à la commission [(4)] : « *Nous sommes dans un moment de vérité : les États et l'Union européenne croient-ils vraiment ou non au droit international ?* »**

La rapporteure appelle la Commission européenne à activer le règlement de blocage, pour envoyer un message politique fort de défense du mandat de la Cour pénale internationale, de l'indépendance de la justice, et de la souveraineté des pays européens.

---

*(1) Siobhan LcGarry, porte-parole de la Commission européenne pour le marché intérieur, citée par Le Monde, « L'UE peine à réagir aux sanctions de l'administration Trump contre la CPI », 23 avril 2026.*

*(2) Audition de M. Nicolas Guillou le 8 avril 2026.*

*(3) Rapport d'information fait au nom de la commission des affaires européennes du Sénat sur l'extraterritorialité des sanctions américaines par M. Phillipe Bonnecarrère, enregistré le 4 octobre 2018 ; Rapport d'information fait au nom de la commission des affaires étrangères et la commission des finances en conclusion des travaux d'une mission d'information sur l'extraterritorialité de la législation américaine, enregistré le 5 octobre 2016.*

*(4) Audition de Nicolas Guillou, juge à la Cour pénale internationale, le mercredi 8 avril 2026*

*d. Le risque d'une systématisation des sanctions ciblées*

Le juge Nicolas Guillou a mis en garde contre les dangers que représenterait la généralisation de ces pratiques pour faire pression sur certaines personnalités : « *Mais* ***le danger, à mon sens, n'est pas tant la déconnexion massive de millions de personnes que le fait qu'elle cible des décideurs publics, car la simple menace de vivre ce qui m'arrive est susceptible de modifier le comportement d'un certain nombre d'entre eux. C'est un danger pour l'État de droit****. Je pense aux procureurs, aux juges, aux avocats qui refuseraient de défendre, aux parlementaires – députés, sénateurs, députés européens – qui auraient peur de voter la loi, aux services de la Commission européenne en matière de concurrence, ou à tous ceux de l'Union européenne chargés d'exécuter le DMA ou le DSA, les règlements sur les marchés uniques et sur les services numériques. Toute une série d'acteurs publics peuvent renoncer à prendre une décision en raison du risque d'être placé sous sanctions ; c'est alors la peur qui gagne. Or si la peur dicte nos décisions, on en vient à un système qui se rapproche d'un régime autoritaire. Le système judiciaire des pays qui ne sont plus des démocraties fonctionne ainsi : vous n'avez plus besoin de dire au juge la décision à prendre ; la peur est généralisée, les juges décident ce qui satisfait le pouvoir. Voilà le véritable danger. Cette menace représente un risque fondamental pour l'État de droit en France et en Europe*. »

**2. Une coupure générale des services numériques**

*a. Un scénario critique auquel il convient de se préparer*

**La nouvelle ligne de l'administration américaine en matière de politique extérieure**, marquée par des hausses brutales des droits de douane ou la menace d'invasion du Groenland, **a contribué à crédibiliser le risque de *kill switch***, soit la capacité de couper les services numériques fournis par des entreprises américaines à l'Union européenne, par l'application de mesures de contrôle des exportations. Cette menace constitue un puissant levier de pression à l'égard des partenaires commerciaux des États-Unis.

M. Damien Lucas, directeur général de Scaleway, a appelé à prendre ce risque pleinement en considération, au même titre que les atteintes à la confidentialité des données : « *Pourquoi est-ce important ? Pour éviter le risque de* kill switch*. Trop souvent, on réduit le cloud à la question de la protection de la donnée. Mais il est encore plus important de protéger les flux de travail et les opérations de nos clients. Nous le savons, quand il y a une panne chez Azure ou AWS, les avions européens sont cloués au sol. Si l'on coupe le cloud, plus rien ne fonctionne dans notre économie. Oui, il faut protéger la donnée, mais il faut également se protéger contre l'arrêt intempestif du cloud*. » (1)

Le *kill switch* se matérialiserait par la suspension des ventes de logiciels américains à des entités européennes, et par l'arrêt des services de support, de

*(1) Table ronde réunissant des fournisseurs de cloud le 21 avril 2026.*

maintenance et de développement associés. L'accès aux applications et aux données hébergées sur des clouds américains serait coupé, de même que l'ensemble des services numériques fournis par les grandes plateformes. « ***Personne ne dispose aujourd'hui d'une solution face à une coupure généralisée d'accès aux technologies américaines ou chinoises, et si l'Europe se trouvait demain privée de mises à jour, la situation deviendrait rapidement intenable*** », a alerté M. Vincent Strubel, directeur général de l'Anssi [(1)].

**Une telle coupure serait susceptible de paralyser l'ensemble de l'économie européenne, avec des conséquences particulièrement critiques dans les pays européens les plus dépendants aux technologies numériques américaines**. La panne informatique mondiale provoquée, le 19 juillet 2024, par la mise à jour défaillante du logiciel de cybersécurité de la société américaine CrowdStrike, a permis de mesurer la profondeur des vulnérabilités liées à une forte dépendance : dans le monde entier, des avions s'étaient trouvés cloués au sol, des hôpitaux ont été contraints d'annuler des opérations, quand des banques, des marchés financiers, ou des centres d'appel d'urgence ne pouvaient plus fonctionner. M. Vincent Strubel a néanmoins fait observer que la France avait « *été relativement moins touchée, en partie grâce à une moindre dépendance à cette monoculture* » en matière de logiciels de cybersécurité.

L'hypothèse est envisagée sérieusement par le gouvernement, le ministre de l'action et des comptes publics, M. David Amiel, ayant déclaré devant la commission d'enquête qu'« *il fa[llait] parer les risques de* kill switch*, à savoir l'interruption brutale d'un service qui rendrait notre pays vulnérable* » [(2)].

**Cette prise de conscience progresse également parmi d'autres États européens**. M. Max Schrems l'a constaté lorsqu'il a été invité au Danemark s'agissant de la menace pesant sur le Groenland : « *L'armée danoise s'inquiète qu'en cas de conflit avec les États-Unis, ceux-ci ne les privent de l'accès aux services numériques de Microsoft, AWS ou Google, par exemple. De fait, les États-Unis sont en mesure d'appliquer de tels embargos – ils le font actuellement à Cuba, en Syrie ou en Iran. Je suis un mondialiste et j'espère que ce type de situations ne se produira pas. Toutefois, au vu de ce qui s'est passé au cours de la dernière année, la question se pose. Les Danois s'inquiètent des conséquences qu'aurait un tel embargo – les hôpitaux, qui utilisent Microsoft, ne pourraient plus avoir accès aux dossiers, par exemple.* » [(3)]

**Un tel scénario ne serait certes pas dans l'intérêt des grandes entreprises numériques américaines**, dont le marché européen pourrait représenter approximativement un tiers du chiffre d'affaires. La présidente de Microsoft France, Mme Corine de Bilbao, a ainsi entrepris de rassurer en déclarant

---

*(1) Audition de M. Vincent Strubel, directeur général de l'Anssi, le 30 avril 2026.*

*(2) Audition de M. David Amiel, ministre de l'action et des comptes publics, et Mme Anne Le Hénanff, ministre déléguée auprès du ministre de l'économie, des finances et de la souveraineté industrielle, énergétique et numérique, chargée de l'intelligence artificielle et du numérique, le 20 mai 2026.*

*(3) Audition de M. Max Schrems le 26 mars 2026.*

que « *la probabilité d'un* kill switch *est extrêmement faible, voire inexistante. Microsoft est une entreprise globale, qui opère dans 180 pays et s'est engagée à augmenter de 40 % ses centres de données en Europe d'ici à 2027. Au vu du montant de nos investissements, il serait suicidaire d'appliquer un* kill switch. *L'entreprise n'est pas le gouvernement américain.* ». (1) Il est cependant difficile de déterminer de quelle marge de manœuvre disposeraient ces entreprises, établies aux États-Unis, pour ne pas appliquer les injonctions de l'administration fédérale auxquelles même les grands établissements bancaires européens obtempèrent.

***b. Une vulnérabilité liée à l'interruption des mises à jour***

Comme en matière de protection des données, **aucune des mesures techniques et contractuelles mises en place par les *hyperscalers* pour garantir leur capacité à maintenir leurs services dans la durée, ne semble éliminer le risque en totalité**.

Amazon a lancé, en janvier 2026, un cloud souverain européen, « *physiquement et opérationnellement isolé des autres infrastructures d'AWS* », qui reposerait sur des data centers situés en Europe et serait opéré exclusivement par le personnel européen, sans qu'« *aucun contrôle opérationnel ne s'exerce depuis l'extérieur des frontières européennes* ». Selon M. Julien Lépine, représentant en France d'AWS, « *ce nouveau cloud d'AWS bénéficie d'une autonomie de fonctionnement, même si l'Europe devait être coupée du reste du monde* » (2). Ces mesures organisationnelles ne permettront cependant pas de contrecarrer l'obligation d'appliquer les décisions américaines, qui découle de la structure capitalistique de la société. Les injonctions des autorités fédérales s'imposent de fait à toutes les entités implantées aux États-Unis, y compris leurs filiales et leurs employés à l'étranger.

Les *hyperscalers* ont également mentionné les **engagements contractuels pris envers leurs clients pour éviter toute coupure brutale des services**. Pour son cloud souverain, AWS a pris « *l'engagement ferme que, si nous devions mettre fin à tout ou partie des services fournis par celui-ci, nous ne pourrions le faire qu'avec un* ***préavis*** *de douze mois, ce qui laisse de la visibilité aux entreprises* » (3) – une telle clause contractuelle pourrait néanmoins être déclarée non valide si elle faisait obstacle à la bonne application d'un décret présidentiel. D'autres sociétés envisagent de **donner le code source** aux clients pour leur permettre de continuer à opérer l'infrastructure : « *Pour ce qui est des services de Google Cloud Platform en direct, nous avons pris l'engagement, en réponse aux craintes qui se sont exprimées – nous ne sommes pas aveugles aux tumultes du monde –, de fournir à nos clients, en cas d'interruption de nos services, l'accès à notre code pour qu'ils puissent, s'ils disposent des ingénieurs nécessaires, assurer la continuité du service. Ce ne sera*

*(1) Table ronde réunissant des représentants en France des Gafam le 13 mai 2026.*

*(2) Ibid.*

*(3) Table ronde réunissant des représentants en France des Gafam le 13 mai 2026.*

*pas simple, mais c'est notre engagement.* » (1) Cela suppose que les clients disposent des ressources internes, aussi bien techniques qu'humaines, suffisantes.

**Dans le cadre de la certification SecNumCloud, le prestataire doit être** autonome dans l'exploitation de la solution, c'est-à-dire qu'il doit être capable de maintenir la fourniture du service en faisant appel à ses compétences propres, sans intervention extérieure**. Cependant, la certification SecNumCloud ne prémunit pas contre la coupure de l'accès aux mises à jour destinées aux logiciels sur lesquels est basée l'infrastructure**.

**Cela apparaît notamment problématique pour les solutions hybrides qui, bien qu'exploitées par un opérateur européen, reposent sur une technologie américaine**, telles que S3NS, opéré par Thalès sur les technologies de Google. M. Damien Lucas, directeur général de Scaleway, est sceptique sur leur résilience : « *J'ai entendu dire que certaines offres hybrides imaginaient, en cas de coupure des mises à jour, pouvoir faire fonctionner leur cloud pendant un an sans recevoir de correctifs de leurs partenaires américains. Alors là, je ne sais pas comment ils font. Chez Scaleway, nous faisons 72 mises à jour quotidiennes, dont une proportion non négligeable sont des mises à jour de sécurité. Je vois donc deux options : soit ils ont une technologie incroyable que je ne connais pas, soit ils connaissent déjà toutes les failles de sécurité qui seront découvertes dans les douze prochains mois et les ont déjà corrigées.* » (2)

Le directeur général de l'Anssi a confirmé que les mises à jour sont effectivement quotidiennes et que c'est une « *caractéristique inhérente à toute infrastructure numérique complexe* ».

**De fait, les infrastructures de cloud nécessitent un flux continu de mises à jour**. M. Strubel a souligné lors de son audition que « ***nous sommes en train de perdre la bataille contre les vulnérabilités logicielles puisque leur nombre a progressé de 18 % par an en moyenne sur les cinq dernières années pour atteindre 50 000 vulnérabilités rendues publiques chaque année, un tiers d'entre elles étant exploitées dès le jour de leur publication*** » (3). Toute la question est donc de savoir combien de temps le service pourrait être maintenu sans aucun accès aux mises à jour. Selon M. Philippe Limantour, « *les délais avant que les risques deviennent vraiment importants se compteraient en semestres* ». Il existerait des « *mécanismes de défense en profondeur permettant de bloquer l'un des maillons d'une chaîne de dix, quinze ou vingt petits pas, pour bloquer les attaques. Ainsi ce n'est pas parce qu'on trouve une vulnérabilité dans un code qu'elle est exploitable* » (4). Le représentant de Google Cloud témoignait cependant de l'existence de failles critiques, dénommées « zero day » qui impliquent un risque immédiat pour la qualité du service et la sécurité des infrastructures.

---

*(1) Ibid.*

*(2) Table ronde réunissant des fournisseurs de cloud le 21 avril 2026.*

*(3) Audition de M. Vincent Strubel, directeur général de l'Anssi, le 30 avril 2026.*

*(4) Table ronde réunissant des représentants en France des Gafam le 13 mai 2026.*

Au regard de l'ampleur des vulnérabilités et de l'accélération de leur exploitation qui se compte en jours, voire en heures, la rapporteure se questionne sur la capacité des opérateurs cloud reposant sur des technologies américaines à garantir une sécurité optimale durant une période d'un semestre.

Le scénario d'un kill switch, dont la crédibilité a fortement gagné en ampleur au cours des derniers mois sous l'impulsion de la politique suivie par le gouvernement des Etats-Unis, aurait des répercussions techniques, économiques et sociales massives. C'est pourquoi il est urgent de s'y préparer.

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

Le comité évaluera notamment la perte de PIB que cela emporterait pour la France et l'Europe, au global et secteur par secteur.

# TROISIÈME PARTIE :
# LES CAUSES D'UN ENRACINEMENT PROFOND

## CHAPITRE 6 – LE DROIT DE LA CONCURRENCE : TOUJOURS UN TEMPS DE RETARD

Les Big Tech maîtrisent aujourd'hui la plupart des services numériques, que ce soit les plateformes ou les logiciels qui constituent le socle des systèmes d'information des entreprises ou des administrations. Leur activité laisse peu de place à des fournisseurs alternatifs européens, qui ont peine à exister sur de tels marchés.

Le droit de la concurrence a été établi pour protéger le consommateur contre la formation de géants économiques, capables d'imposer leurs conditions et de constituer des rentes à leur profit. Partant du constat de l'ultra-domination des Gafam sur leur marché, comment expliquer que le droit de la concurrence n'ait pu avoir un impact sur leur activité ? Quel est le poids de cet instrument aux mains de la puissance publique ?

La rapporteure a souhaité établir une rétrospective des actions envers les Gafam conduites par les autorités de la concurrence, aux niveau national et européen, afin de mesurer les résultats auxquelles elles sont parvenues et de comprendre les limitations structurelles auxquelles elles se heurtent. L'adoption du DMA est présentée par la Commission européenne comme un véritable changement d'approche.

### A. LES GAFAM : DES POSITIONS DE DOMINATION GRÂCE À LA MAÎTRISE DE L'ENSEMBLE DE LA STACK DU NUMÉRIQUE

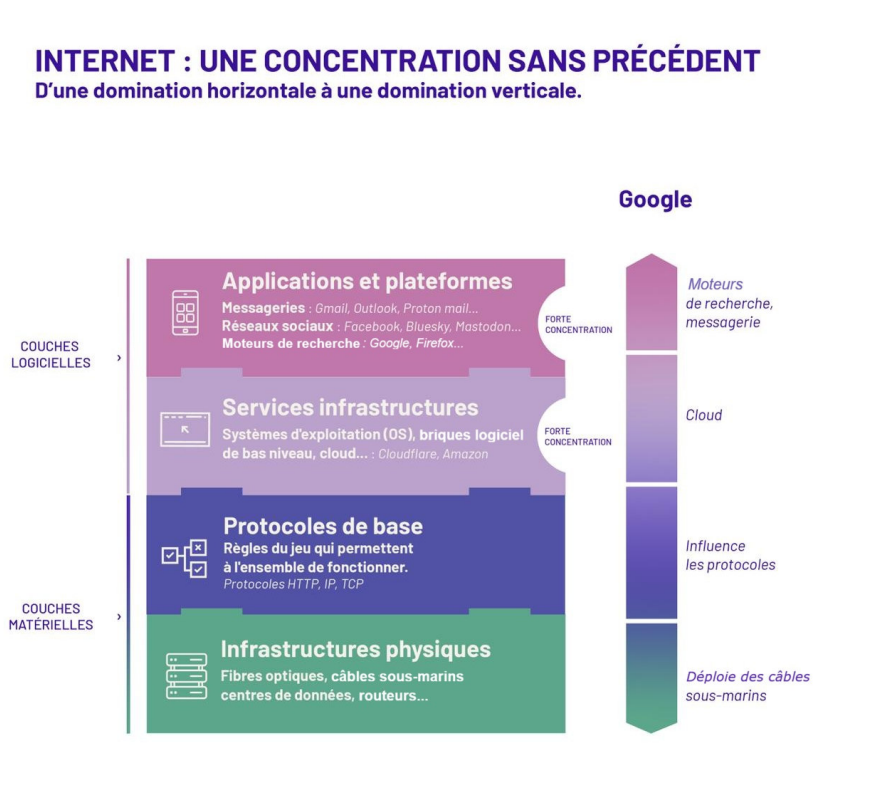
Le secteur du numérique regroupe des activités variées telles que la publicité en ligne, l'IA, le cloud ou encore les réseaux sociaux. Le fonctionnement d'internet repose quant à lui sur une architecture par couche. Une organisation qu'a présentée Mme Francesca Musiani, directrice de recherche au CNRS, lors de son audition par la commission [(1)] : « *Internet repose sur une architecture en couches que l'on peut résumer en quatre niveaux. La première couche est physique : les câbles sous-marins et terrestres, ainsi que les centres de données, où s'effectue le transport concret des données. La deuxième couche est celle des protocoles de base, ces langages qui permettent aux machines de communiquer entre elles. L'Internet Protocol (IP) est le protocole commun par excellence. Le système de noms de domaine (DNS), qui est l'annuaire d'internet, constitue un autre élément critique de cette couche, en assurant une correspondance fiable entre les adresses URL que nous utilisons et les adresses numériques des ressources. La troisième couche est*

*(1) Table ronde, ouverte à la presse, sur les infrastructures numériques, le 2 avril 2026.*

*celle des services d'infrastructure, notamment le cloud, qui fournit stockage et puissance de calcul à la demande. Enfin, la quatrième couche est celle des applications et des plateformes – messageries, réseaux sociaux, moteurs de recherche – où se concentrent traditionnellement les débats sur la régulation du numérique.*

« *Chacune de ces couches est gouvernée par des acteurs différents, avec de fortes interdépendances qui ne sont pas toujours transparentes pour le citoyen, ni même pour les régulateurs. Là où la situation est inédite, c'est que nous observons une concentration significative du pouvoir à chacun de ces niveaux. Pour la couche physique, comme nous l'avons dit, les câbles, historiquement opérés par des consortiums d'opérateurs télécoms, le sont de plus en plus par de grandes entreprises privées comme Google et Meta, qui sont les seules à avoir la force de frappe pour investir dans ces infrastructures devenues trop stratégiques pour elles.* »

Le schéma ci-dessous tente de représenter l'organisation en couches d'internet et la concentration en cours d'une ampleur inégalée.




*Source : rapporteure.*

Cette concentration tout à la fois horizontale (au sein des différentes couches) et verticale (entre couches) est caractéristique des positions ultradominantes des Gafam et produit plusieurs effets :

– les effets de réseau, qui favorisent l'acteur qui dispose du plus grand nombre d'utilisateurs connectés aux services qu'il fournit ;

– les effets de verrouillage des clients, perçus ou réels, à travers de nombreux dispositifs spécifiques qui peuvent être mis en place : difficultés à récupérer ses données, absence d'interopérabilité, etc. ;

– les économies d'échelle, permettant de réaliser des revenus très importants sur un portefeuille client de plusieurs milliards d'individus ;

– l'accès à des données d'utilisateurs à grande échelle, contribuant à l'avance technologique des produits ;

– la vente forcée de produits à travers des offres groupées (« *bundling* ») et la capacité à mettre en place des subventions croisées entre services distincts ;

– la mise en place de barrières à l'entrée pour les concurrents via la standardisation et le contrôle des dispositifs techniques.

En asseyant leurs modèles économiques sur ces spécificités, les grands acteurs du numérique ont pu se développer et, dans le même temps, verrouiller des écosystèmes qui rendent la contestation de leur pouvoir de marché difficile.

Les auditions de la commission d'enquête ont fait apparaître que ces positions ne cessent de se renforcer par une colonisation progressive des différentes couches du monde numérique, comme le décrit Mme Ophélie Coelho [(1)] : « *En tant que passerelle technique, ils prennent possession et privatisent des nœuds importants sur presque toutes les couches technologiques. Partis du logiciel et du web, ils se sont progressivement étendus aux supports de mobilité (ordinateurs, mobiles), aux câbles sous-marins, aux satellites pour certains, et même à des couches réseau avec des réseaux privés qui se superposent aux réseaux existants, et aujourd'hui aux puces électroniques. Nous observons une prise de contrôle de passerelles techniques essentielles. Le leader en la matière reste Google qui, à l'exception des satellites, a déjà des positions fortes dans tous les domaines que j'ai cités.*

« *Un autre de leurs leviers, très important, relève de l'intégration horizontale et verticale. D'une part, un levier transsectoriel : ils agissent de manière transversale sur les secteurs clés de la société, la santé, la sécurité, la mobilité, l'administration, l'éducation. Ils ont ciblé ces secteurs non seulement comme des marchés d'utilisateurs, mais aussi comme des points où s'établir en tant*

*(1) Chercheuse associée à l'Institut des relations internationales et stratégiques (Iris), doctorante au Centre internet société du CNRS (CIS) et au centre d'analyse et de recherche interdisciplinaires sur les médias (Carism-Paris-Assas).*

*qu'intermédiaires et passerelles techniques. Ils ont également ciblé d'autres géants, comme les grandes banques, les grands groupes pharmaceutiques ou les grands opérateurs de télécommunications, qui ne sont d'ailleurs plus si « grands » aujourd'hui. Ils sont devenus des acteurs pesant dans la chaîne de valeur de tous les secteurs clés de la société moderne. D'autre part, l'intégration verticale, ou ce que l'on peut appeler un levier de puissance d'empilement technologique, leur permet de constituer progressivement un écosystème technique complet.*

« *Tout cela mène à deux effets cumulatifs extrêmement puissants. Tout d'abord, la concentration progressive de l'activité au sein de ces acteurs ; ensuite, un levier écosystémique : une fois l'usage concentré au sein de leurs infrastructures et de leur modèle technologique, ils peuvent plus aisément diffuser certaines informations, certains usages et même certaines croyances portées par leurs technologies.* » [(1)]

Le cas des câbles sous-marins transnationaux de fibre optique est à cet égard très éclairant. Ces infrastructures essentielles au fonctionnement de l'internet mondial étaient jusqu'à présent déployées par des consortiums d'acteurs internationaux. Les Gafam sont désormais capables de mener de tels projets seuls, et investissent ce secteur pour des raisons stratégiques. Mme Ophélie Coelho observe que « *la situation des câbles sous-marins a beaucoup évolué. Sans refaire tout l'historique, l'accélération de la présence des géants du numérique dans ce secteur date des années 2010. Plusieurs raisons expliquent ce phénomène : leur consommation croissante de capacité, l'intérêt économique à posséder ces infrastructures, et sans doute une volonté de contrôler l'ensemble de la pile technologique, d'autant qu'ils avaient déjà une expérience des réseaux terrestres aux États-Unis.*

« *Cette tendance s'est accélérée ces dernières années, avec des capacités de câbles qui atteignent désormais des centaines de térabits, une échelle sans commune mesure avec la capacité d'un térabit d'il y a quelques années. La différence majeure réside dans la structure de propriété. Auparavant, nous avions des consortiums d'opérateurs de télécommunications, dont la responsabilité et les choix étaient partagés entre dix à vingt partenaires (…). Aujourd'hui, la configuration a changé : nous avons soit des consortiums beaucoup plus restreints, soit des propriétés uniques. Google, par exemple, possède plus de 30 câbles, et bientôt près de 40 avec ses nouveaux projets dans l'Indopacifique. (…).*

« *Au-delà du nombre de câbles, il faut considérer l'évolution de leurs capacités. En 2021, environ 28 % de la capacité mondiale appartenait aux géants du numérique. (…) je pense que d'ici dix ans, ils pourraient détenir la moitié de la capacité totale en termes de puissance. C'est un changement énorme (…).*

« *Ce mécanisme de dépendance, fondé sur une intégration verticale, influe sur l'ensemble de l'écosystème numérique. Un exemple frappant est la coupure de*

*(1) Table ronde, ouverte à la presse, sur les infrastructures numériques, le 2 avril 2026.*

*câbles survenue en Afrique de l'Ouest en 2024. Quatre câbles historiques ont été sectionnés, privant treize pays africains d'internet. Ce sont les câbles Equiano, de Google, et 2Africa, le consortium incluant Meta et China Telecom, qui ont récupéré la majeure partie du trafic. Cet événement montre que c'est souvent dans les moments de crise qu'ils renforcent leur position et deviennent des partenaires indispensables, à l'instar de ce que l'on a pu observer avec Starlink, bien que ce dernier n'opère pas à la même échelle de puissance.* »

L'exemple des câbles sous-marins n'est pas isolé, des constats similaires peuvent être dressés sur les connexions satellitaires. Du fait de leur positionnement, les Gafam deviennent indispensables au fonctionnement même de nos économies. Cette situation leur confère des avantages considérables. Comment le droit de la concurrence a-t-il appréhendé le rôle de ces acteurs ? Quelle a été son efficacité pour endiguer la constitution de positions dominantes ?

## B. LE DROIT DE LA CONCURRENCE FACE AUX GAFAM : DES SANCTIONS MULTIPLES ET 17 MILLIARDS D'EUROS D'AMENDES AU TOTAL

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

L'activité des acteurs du numérique est soumise au droit de la concurrence, en particulier aux articles 101 et 102 du Traité sur le fonctionnement de l'Union européenne (TFUE), qui sanctionnent respectivement les ententes et les abus de position dominante. Le contrôle de l'application de ces deux articles relève, selon les cas, de la Commission européenne et, pour la France, de l'Autorité de la concurrence.

Comme l'explique M. Umberto Berkani, rapporteur général de l'Autorité de la concurrence [(1)], « *lorsque les marchés examinés présentent une dimension nationale, par exemple en raison de réglementations spécifiques, l'analyse du pouvoir de marché s'exerce nécessairement à cette échelle. Si une opération de concentration y crée une domination trop forte, les règles de concurrence s'appliquent. En revanche, si un marché dispose d'une dimension plus large, notamment européenne grâce à une réglementation homogène, l'analyse est alors menée à ce niveau* ». Lorsque l'autorité nationale se saisit, elle se fonde également sur le droit national, en particulier sur le code de commerce.

Le réseau européen de la concurrence (REC) rassemble la Commission européenne et l'ensemble des autorités nationales de concurrence à des fins de coordination et de répartition des affaires entre niveau européen et niveau national.

*(1) Audition de MM. Umberto Berkani, rapporteur général de l'Autorité de la concurrence et Julien Neto, rapporteur général adjoint, le 5 mai 2026.*

Le droit de la concurrence a récemment été complété par le DMA (voir *infra*), dont l'application est à la main exclusive de la Commission européenne.

Du fait de leur centralité, les cinq grandes plateformes états-uniennes ont fait l'objet d'un contrôle intensif de la part des autorités de concurrence, qui a abouti à de nombreuses sanctions :

– pour Google (groupe Alphabet) : douze sanctions, dont huit avec amendes, représentant un montant cumulé de 12,1 milliards d'euros ;

– pour Apple : six sanctions, dont quatre avec amendes, pour un montant cumulé de 3,6 milliards d'euros ;

– pour Meta : trois sanctions, dont deux avec amendes, pour un montant cumulé de 998 millions d'euros ;

– pour Microsoft : trois sanctions, dont une avec amende, pour un montant de 561 millions d'euros ;

– pour Amazon : deux sanctions.

Outre les amendes, d'un montant total de 17,2 milliards d'euros, les sanctions prononcées ont pu prendre la forme d'engagements obligatoires. Par exemple, par une décision de décembre 2022, Amazon s'est vue interdire l'utilisation des données non publiques des vendeurs tiers recueillies par le biais de sa place de marché dans ses activités de détail propres. De la même façon, Microsoft s'est vue par deux fois imposer des engagements obligatoires – favoriser l'interopérabilité de ses produits de bureautique et limiter les offres groupées – en décembre 2012 et en septembre 2025. Cette dernière décision imposait le découplage de l'application Teams du reste de la suite bureautique Office 365.

Le tableau ci-dessous liste l'ensemble des sanctions prononcées à l'encontre de ces cinq entreprises par la Commission européenne et l'Autorité de la concurrence sur le fondement du droit de la concurrence. Il montre que l'essentiel des pratiques ayant donné lieu à sanction a consisté, pour chaque plateforme, à créer un accès différencié entre ses propres produits et ceux de ses concurrents et à invisibiliser ces derniers. Le pouvoir de marché a pu également être utilisé pour imposer des conditions économiques inacceptables à des parties prenantes comme les éditeurs de contenu et les agences de presse.

**LISTE DES SANCTIONS PRONONCÉES CONTRE LES GAFAM AU TITRE DU DROIT DE LA CONCURRENCE DEPUIS 2010**

| Groupe | Autorité | Affaire | Date | Sanction (M€) | Description |
|---|---|---|---|---|---|
| Amazon | Commission européenne | AT. 40153 Amazon e-book MFNs | Mai 2017 | | Amazon EU SARL : engagements rendus obligatoires. Amazon supprime les clauses de nation la plus favorisée (MFN) dans ses contrats de distribution d'e-books avec les éditeurs européens. Procédure close sans constat d'infraction ni amende. |
| Amazon | Commission européenne | AT.40462 + AT.40703 — Amazon Marketplace & Buy Box Décision | Décembre 2022 | | Amazon : engagements rendus obligatoires dans deux affaires connexes. (1) Marketplace : Amazon s'interdit d'utiliser les données non publiques des vendeurs tiers dans ses activités de détail propres. (2) Buy Box : Amazon garantit un accès équitable et non discriminatoire à la « Buy Box » et au label Prime pour tous les vendeurs. Procédure close sans amende |
| Apple | Commission européenne | AT.39847 / Ebooks | Juillet 2013 | | Apple Inc. et quatre éditeurs (Hachette, HarperCollins,Macmillan, Penguin, Simon & Schuster) : engagements rendus obligatoires. Les parties mettent fin aux clauses de prix d'agence et de nation la plus favorisée (MFN) dans leurs contrats de distribution d'e-books. Procédure close sans amende. |
| Apple | Autorité de la concurrence | Décision 20-D-04 relative à des pratiques mises en œuvre dans le secteur de la distribution de produits de marque Apple | Mars 2020 | 1100 | Apple Inc., Apple Distribution International, Tech Data et Ingram Micro condamnés à un total de 1,24 Md€ (dont 1,1 Md€ pour Apple seule) pour restrictions de clientèle entre grossistes, entente verticale sur les prix de revente des Apple Premium Resellers (APR) et abus de dépendance économique (affaire eBizcuss, pratiques 2005–2013). |
| Apple | Commission européenne | AT.40437 / Apple App Store Practices (Music Streaming) | Mars 2024 | 1840 | Apple Inc. condamnée à 1,84 Md€ pour avoir imposé aux développeurs d'applications de streaming musical (notamment Spotify) des restrictions techniques et contractuelles (interdiction des clauses anti-steering) les empêchant d'orienter les utilisateurs vers des offres hors App Store. La Commission a multiplié l'amende de base par 42 pour effet dissuasif. |
| Apple | Commission européenne | AT.40452. Apple Mobile Payments (NFC) | Juillet 2024 | | La Commission rend contraignants les engagements d'Apple Inc. qui s'engage à ouvrir l'accès au module NFC de ses appareils iOS à des fournisseurs de services de paiement tiers concurrents d'Apple Pay. Procédure close sans constat d'infraction ni amende. |
| Apple | Autorité de la concurrence | Décision 25-D-02 relative à des pratiques mises en œuvre dans le secteur de la publicité sur applications mobiles sur les terminaux iOS | Mars 2025 | 150 | Apple Inc. et Apple Distribution International condamnées à 150 M€ pour avoir abusé de leur position dominante en déployant le dispositif App Tracking Transparency (ATT) de façon symétrique : les règles de consentement au suivi publicitaire des tiers ne s'appliquaient pas de manière équivalente aux propres services d'Apple (avril 2021 – juillet 2023). |
| Apple | Commission européenne | DMA.100055 — Apple App Store (anti-steering) | Avril 2025 | 500 | Apple Inc. condamnée à 500 M€ pour avoir empêché les développeurs d'applications d'orienter librement les utilisateurs vers des offres ou canaux de distribution extérieurs à l'App Store, en violation de l'obligation antisteering du DMA. Première décision de non-conformité DMA de l'histoire. |
| Google | Autorité de la concurrence | Décision 10-MC-01 relative à la demande de mesures conservatoires présentée par la société Navx | Juin 2010 | | Google LLC et Google France enjointes de rétablir sous 5 jours le compte AdWords de la société Navx et de clarifier leur politique de contenus. Premières mesures conservatoires prononcées en France dans le secteur de la publicité en ligne. |

| Groupe | Autorité | Affaire | Date | Sanction (M€) | Description |
|---|---|---|---|---|---|
| Google | Autorité de la concurrence | Décision 10-D-30 relative à des pratiques mises en œuvre dans le secteur de la publicité sur Internet | Octobre 2010 | | Google LLC et Google France : engagements rendus obligatoires. Google s'engage à rendre transparentes et prévisibles les règles AdWords applicables aux dispositifs de contournement de contrôles routiers, faisant suite aux mesures conservatoires 10-MC-01 du 30 juin 2010 (affaire Navx). Pas d'amende. |
| Google | Commission européenne | AT. 39740 / Google Search (Shopping) | Juin 2017 | 2 420 | Google LLC et Alphabet Inc. condamnées à 2,42 Md€ pour avoir accordé, depuis au moins 2008, un placement plus favorable à Google Shopping au détriment des services concurrents dans les résultats de recherche générale. Confirmé par le Tribunal de l'UE le 10 nov. 2021 (T-612/17) et par la CJUE le 10 sept. 2024 (C-48/22P). |
| Google | Commission européenne | AT. 40099 / Google Android | Juillet 2018 | 4 125 | Google LLC et Alphabet Inc. condamnées à 4,34 Md€ pour trois pratiques contractuelles imposées aux fabricants Android : installation obligatoire de Google Search et Chrome, paiements conditionnés à l'exclusivité, restrictions aux versions Android non certifiées. Amende réduite à 4,125 Md€ par le Tribunal de l'UE le 14 sept. 2022 (T-604/18). |
| Google | Commission européenne | AT 40411 / Google Search (AdSense) | Mars 2019 | 1490 | Google LLC et Alphabet Inc. condamnées à 1,49 Md€ pour avoir imposé, de 2006 à 2016, des clauses d'exclusivité anticoncurrentielles dans les contrats AdSense for Search avec des propriétaires de sites web tiers, les empêchant d'afficher des publicités search de concurrents de Google. |
| Google | Autorité de la concurrence | Décision 19-D-26 relative à des pratiques mises en œuvre dans le secteur de la publicité en ligne liée aux recherches | Décembre 2019 | 150 | Google LLC, Google Ireland Limited et Google France condamnées à 150 M€ pour application non objective, non transparente et discriminatoire des règles Google Ads à l'égard des annonceurs (affaire Gibmedia). Injonctions de clarification pour 5 ans. |
| Google | Autorité de la concurrence | Décision 20-MC-01 relative à des demandes de mesures conservatoires présentées par le Syndicat des éditeurs de la presse magazine, l'Alliance de la presse d'information générale e.a. et l'Agence France Presse | Avril 2020 | | Google LLC, Google Ireland Limited et Google France enjointes de négocier de bonne foi la rémunération des éditeurs et agences de presse au titre de la loi n° 2019-775 du 24 juillet 2019 sur les droits voisins, dans un délai de trois mois. |
| Google | Autorité de la concurrence | Décision 21-D-11 relative à des pratiques mises en œuvre dans le secteur de la publicité sur internet | Juin 2021 | 220 | Google LLC, Google Ireland Limited et Google France condamnées à 220 M€ pour avoir favorisé, via le serveur publicitaire DFP, leur propre plateforme d'enchères AdX au détriment des SSP concurrentes (1re décision mondiale sur les enchères programmatiques display). Procédure de transaction. Engagements sur l'interopérabilité rendus obligatoires. |
| Google | Autorité de la concurrence | Décision 21-D-17 relative au respect des injonctions prononcées à l'encontre de Google dans la décision n° 20-MC-01 du 9 avril 2020 | Juillet 2021 | 500 | Google LLC, Google Ireland Limited et Google France condamnées à 500 M€ pour n'avoir pas respecté les injonctions de la décision 20-MC-01 : absence de négociation de bonne foi sur les droits voisins. Google enjointe de se conformer sous astreinte de 900 000 € par jour de retard. |
| Google | Autorité de la concurrence | Décision 22-D-13 relative à des pratiques mises en œuvre par Google dans le secteur de la presse | Juin 2022 | | Google LLC, Google Ireland Limited et Google France : engagements rendus obligatoires pour 5 ans (renouvelables) sur la conduite de négociations de bonne foi, transparentes et non discriminatoires avec les éditeurs et agences de presse pour la rémunération des droits voisins. |

| Groupe | Autorité | Affaire | Date | Sanction (M€) | Description |
|---|---|---|---|---|---|
| Google | Autorité de la concurrence | Décision 24-D-03 relative au respect des engagements figurant dans la décision n° 22-D-13 du 21 juin 2022 relative à des pratiques mises en œuvre par Google dans le secteur de la presse | Mars 2024 | 250 | Alphabet Inc., Google LLC, Google Ireland Limited et Google France condamnées à 250 M€ pour avoir méconnu 4 de leurs 7 engagements de 2022, notamment l'obligation de transparence sur les critères de rémunération et l'obligation de coopération avec le mandataire. Procédure de transaction. |
| Google | Commission européenne | AT.40670 — Google AdTech C(2025) 5965 final | Septembre 2025 | 2950 | Google LLC et Alphabet Inc. condamnées à 2,95 Md€ pour avoir, depuis 2014, favorisé leur propre bourse d'annonces en ligne AdX via leur serveur publicitaire DFP (DoubleClick for Publishers), au détriment des bourses concurrentes et des éditeurs en ligne. 4e sanction antitrust de la Commission contre Google. |
| Meta | Autorité de la concurrence | Décision 22-D-12 relative à des pratiques mises en œuvre dans le secteur de la publicité sur internet | Juin 2022 | | Meta Platforms Inc., Meta Platforms Ireland Ltd. et Facebook France : engagements rendus obligatoires à la suite de la saisine de la société Criteo. Meta s'engage à améliorer l'accès des partenaires publicitaires aux données et outils de son écosystème publicitaire. Procédure close sans amende. |
| Meta | Commission européenne | AT.40684 — Facebook Marketplace | Novembre 2024 | 798 | Meta Platforms Inc. condamnée à 797,72 M€ pour deux infractions : couplage abusif de Facebook Marketplace au réseau social Facebook et imposition de conditions inéquitables à des fournisseurs concurrents de services de petites annonces en ligne. |
| Meta | Commission européenne | DMA.100009 — Meta (Pay or Consent) | Avril 2025 | 200 | Meta Platforms Inc. condamnée à 200 M€ pour avoir contraint les utilisateurs européens de Facebook et Instagram à choisir entre céder leurs données personnelles à des fins de publicité ciblée ou payer un abonnement payant, sans alternative moins intrusive permettant un consentement granulaire. |
| Microsoft | Autorité de la concurrence | Décision 12-D-14 relative à des pratiques mises en œuvre par Microsoft Corporation et Microsoft France | Juin 2012 | | Microsoft Corporation et Microsoft France : engagements rendus obligatoires dans le secteur des logiciels de serveur de messagerie et de collaboration. Microsoft s'engage à améliorer l'interopérabilité de ses produits. Procédure close sans amende. |
| Microsoft | Commission européenne | AT.39530 / Microsoft (Tying) | Mars 2013 | 561 | Microsoft Corporation condamnée à 561 M€ pour n'avoir pas proposé l'écran de choix du navigateur aux utilisateurs de Windows 7 SP1 entre février 2011 et juillet 2012, en violation des engagements pris en 2009. Première décision pour non-respect d'engagements dans le secteur numérique. |
| Microsoft | Commission européenne | AT.40721 + AT.40873 — Microsoft Teams / Teams II | Septembre 2025 | | Microsoft Corporation : engagements rendus obligatoires. Microsoft s'engage à découpler Teams de ses suites Office 365 / Microsoft 365, à proposer Teams séparément à un prix inférieur, à accroître la différence de prix de 50 % et à garantir l'interopérabilité et la portabilité des données (valables 7 à 10 ans). Procédure close sans amende. |

*Source : Autorité de la concurrence.*

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

La croissance forte des activités de cloud a conduit l'Autorité de la concurrence à examiner en profondeur les pratiques sur ce marché, dans le cadre d'une enquête sectorielle. Constatant la prédominance de trois acteurs principaux, AWS, Googlecloud et Microsoft, l'Autorité souhaitait examiner dans quelle mesure leur force de frappe financière et leurs écosystèmes de services numériques étaient en mesure d'entraver le développement de la concurrence.

Cette enquête a débouché en juin 2023 sur la publication d'un avis décrivant l'ensemble des pratiques problématiques constatées [(1)]. Deux sujets ont fait l'objet d'une attention particulière, les crédits cloud et les *egress fees* ou frais de sortie.

Les crédits cloud permettent à des start-up en développement de lancer leurs produits sans engager de fonds pour leurs infrastructures de gestion des données. Mais les fournisseurs de services cloud se servent de cette pratique pour verrouiller les acteurs dans leur propre système. *« L'Autorité considère toutefois que les crédits cloud sous forme d'offres ciblées d'accompagnement doivent faire l'objet d'une attention particulière. Les montants proposés parfois élevés, le vaste écosystème d'entreprises qu'ils concernent et leur durée de validité, les distinguent significativement des essais gratuits qui peuvent être traditionnellement observés dans d'autres industries. Cela soulève des doutes quant à la capacité de tous les fournisseurs de services cloud à les proposer de manière rentable*. En effet, les montants de crédits proposés pouvaient aller jusqu'à 200 000 dollars pour Google Cloud, 150 000 pour Microsoft Azure, et 100 000 pour AWS. La loi Sren prévoit l'encadrement de cette pratique, notamment le plafonnement à un an de leur durée. Toutefois, les dispositions concernées n'ont jusqu'à présent pas été appliquées faute de publication du décret nécessaire. Le président et la rapporteure invitent le gouvernement à prendre ces décrets dans les plus brefs délais.

S'agissant des *egress fees*, l'Autorité considérait qu'ils étaient déconnectés des coûts réels et susceptibles de constituer un frein important à la portabilité des données. Les entreprises facturaient de façon trop importante les flux de sortie des données. Cela pénalisait notamment fortement les entreprises souhaitant mettre en œuvre des architectures dites multi-cloud, pour ne pas dépendre d'un seul et même fournisseur. Depuis, les principaux *hyperscalers* ont revu leurs politiques tarifaires pour anticiper les exigences du Data Act, dont la mise en application complète sur ce point interviendra seulement en janvier 2027.

Que ce soit les *egress fees* ou les crédits cloud, les pratiques constatées profitent du fait que les développements pour transférer vers le cloud un système

---

*(1) Autorité de la concurrence, Avis 23-A-08 du 29 juin 2023 portant sur le fonctionnement concurrentiel de l'informatique en nuage (« cloud »)*

*https://www.autoritedelaconcurrence.fr/fr/avis/portant-sur-le-fonctionnement-concurrentiel-de-linformatique-en-nuage-cloud*

d'information d'une entreprise ou d'une administration sont longs et coûteux à mettre en œuvre. Les migrations en sont d'autant moins facilitées, ce qui accroît le risque de verrouillage par les grands fournisseurs du marché.

D'autres pratiques problématiques ont été relevées par l'Autorité de la concurrence :

– le manque de transparence des tarifs des hyperscalers, en particulier sur les services ultérieurs lors de la réalisation du premier achat ;

– des programmes de certification, pour partie gratuits, à destination des professionnels ;

– des licences qui rendent plus coûteuse l'utilisation des produits dans des environnements cloud concurrents, en particulier s'agissant des produits Microsoft ;

– des mises à jour unilatérales de certains services faisant office de standard technique, auxquelles les autres acteurs ont accès avec un délai, notamment le standard S3 déployé par Amazon.

Qu'en est-il de l'ensemble de ces pratiques, trois ans après la publication de l'avis ? Selon l'entreprise Outscale, concurrente des trois hyperscalers, « *l'avis de l'Autorité de la concurrence de 2023 reste pleinement d'actualité. Les dynamiques décrites se sont même renforcées avec la vague de l'IA générative : les hyperscalers ont intégré verticalement les modèles de fondation, les infrastructures GPU, les outils de développement et les places de marché applicatives. Cette intégration crée des effets de réseau et des frictions de migration allant bien au-delà de ce que l'Autorité identifiait alors.*

« *Les crédits cloud ont proliféré vers les start-up d'IA, créant une dépendance précoce chez des acteurs qui structureront les marchés de demain. Les frais de sortie restent élevés malgré les obligations du Data Act européen, dont l'application effective demeure partielle. L'avantage des hyperscalers ne tient pas à une supériorité technique intrinsèque, mais à leur capacité à subventionner un écosystème complet grâce à des masses financières sans équivalent en Europe.* » (1)

AWS, Microsoft et Google ont eu l'occasion de détailler les évolutions de leurs conditions commerciales lors d'une table ronde, à l'issue de laquelle ils ont ajouté des contributions écrites.

**Google** relève que tous ses prix sont publics et contractuels (2). Concernant les crédits cloud, « *Google justifie le maintien de ses programmes de support aux startups par la nécessité de réduire les barrières à l'adoption du cloud pour les startups. Ces crédits sont conçus comme une allocation financière limitée dans le temps et non exclusive. Ils permettent aux startups d'évaluer la performance des*

*(1) Réponses au questionnaire de la rapporteure.*

*(2) Réponse aux questionnaires de la rapporteure.*

*services Google Cloud, de tester les chemins de migration et de déployer des charges de travail en conditions réelles sans avoir à supporter de coûts initiaux prohibitifs* ».

Depuis janvier 2024, Google applique la gratuité de la sortie des données aux clients qui migrent depuis Google Cloud. « *Nous avons été les premiers fournisseurs à proposer cette mesure, et d'autres ont suivi notre exemple. De même, nous avons été les premiers à rendre gratuits les frais de sortie multi-cloud, allant ainsi au-delà des exigences de la loi européenne sur les données (Data Act), qui n'impose qu'une tarification au coût pour ces frais. Toutes les préoccupations liées à la sortie des données ont été pleinement prises en compte et levées par le Data Act européen ».*

En revanche, Google dénonce le maintien de pratiques de licence juridique déloyales, en particulier concernant les produits Microsoft. « *La possibilité pour les fournisseurs de cloud de gagner de nouveaux clients (notamment les entreprises traditionnelles et les organismes publics) est compromise par les pratiques de licence restrictives des éditeurs de logiciels historiques, en particulier Microsoft. Ces pratiques visent à fidéliser les clients de logiciels sur site à leurs propres plateformes cloud, empêchant ainsi les fournisseurs de cloud concurrents de rivaliser efficacement. Cette situation a permis à Microsoft de tirer un profit substantiel de ses pratiques anticoncurrentielles, ce qui lui a permis d'établir et de consolider sa position dominante sur le marché du cloud ».* Google relève l'existence d'une enquête lancée en mai 2026 par l'autorité britannique de la concurrence et des marchés sur le sujet : *« La CMA [(1)] se dit préoccupée par le fait que les pratiques de licence logicielle de Microsoft nuisent à la concurrence dans le cloud et entraînent une augmentation des coûts d'exploitation et une perte de productivité, tout en aggravant potentiellement les problèmes de résilience. Compte tenu de l'évolution du marché de l'IA et de l'intégration rapide de l'IA avancée dans les outils de base de Microsoft, la CMA reconnaît que les mesures correctives dans ce domaine sont plus urgentes que jamais. (…) La décision d'inclure les logiciels d'entreprise de Microsoft dans cette enquête SMS lui permettra non seulement de répondre à une préoccupation majeure soulevée par son enquête sur le marché du cloud, en examinant les pratiques de licence cloud de Microsoft, mais aussi d'étudier d'autres préoccupations exprimées par les acteurs du marché concernant l'exploitation plus large par Microsoft de sa position dominante sur le marché des logiciels d'entreprise* ».

**Amazon web services** note que les obligations du Data Act imposant aux fournisseurs de cloud de faciliter l'adoption du multi-cloud, d'assurer la portabilité et d'éliminer les frais de transfert sortant de données, sont pleinement applicables depuis septembre 2025 et relèvent du contrôle de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep). L'entreprise déclare qu'elle devance les obligations européennes en ayant supprimé, depuis mars 2024, les frais de transfert de données pour les clients souhaitant quitter

*(1) Competition and Markets Authority.*

AWS à l'échelle mondiale. « *Selon Deloitte, plus de 70 % des clients européens utilisent plusieurs fournisseurs d'informatique en nuage, et 85 % des dépenses informatiques mondiales demeurent sur site. De fait, les clients combinent les services AWS avec ceux d'autres fournisseurs informatiques, notamment Microsoft Azure, Google Cloud et Oracle, des fournisseurs européens tels qu'OVHcloud, IONOS et Scaleway, des opérateurs de télécommunications comme Deutsche Telekom et Orange Business Services, des systèmes sur site, ou des fournisseurs émergents.* » [(1)]

AWS indique également utiliser des normes ouvertes et soutenir les communautés open source, notamment Linux, Kubernetes, PostgreSQL et Apache.

De manière générale, le secteur est décrit comme particulièrement concurrentiel, dans la mesure où « *il attire des milliards de nouveaux investissements à travers l'Europe - de Stackit (11 milliards d'euros en Allemagne), Google, Oracle, et de fournisseurs de nouvelle génération comme CoreWeave, Lambda Labs et Nebius* ».

Enfin, Microsoft relève que l'avis de l'Autorité de la concurrence identifiait « *un certain nombre de* ***préoccupations potentielles****, pouvant surgir sur les marchés cloud si des comportements spécifiques se matérialisaient* » [(2)] et considère, à l'instar d'AWS, que le marché du cloud est dynamique et concurrentiel, en France et à l'échelle mondiale. Microsoft fait état des différends qui ont pu l'opposer à ses concurrents. Sont ainsi mentionnées les questions soulevées par OVH et l'association Cloud Infrastructure Services Providers in Europe (CISPE) concernant les conditions de licence de Microsoft, qui ont été résolues à l'amiable en 2024. Google a par la suite décidé de déposer sa propre plainte en visant les conditions de licence de Microsoft devant la Commission européenne [(3)] *:* « ***Google a retiré sa plainte il y a plusieurs mois****. Nous considérons que cette plainte n'avait aucune base juridique et que Google tentait simplement de faire passer artificiellement un litige purement commercial pour une question de droit de la concurrence. Pour dire les choses simplement : Google se plaignait de devoir rémunérer Microsoft pour ses logiciels lorsqu'il les utilise pour fournir des services cloud à ses clients. Or Microsoft, comme tout éditeur, a le droit d'être rémunéré pour l'utilisation de ses logiciels. Toute affirmation selon laquelle la concurrence serait compromise est manifestement fausse, comme le prouve la rapide hausse des revenus et des bénéfices de nos concurrents.* »

Ces évolutions confirment les constats initiaux de l'Autorité. Elles n'auraient probablement pas eu lieu sans l'action documentée des pouvoirs publics, qu'il s'agisse de l'avis de l'Autorité de la concurrence ou de l'édiction de règles spécifiques (loi Sren, Data Act). Elles montrent que l'encadrement réglementaire

---

*(1) Réponses au questionnaire de la rapporteure.*

*(2) Réponses aux questionnaires de la rapporteure.*

*(3) Communication Google cloud, septembre 2024, https://cloud.google.com/blog/topics/inside-google-cloud/filing-eu-complaint-against-microsoft-licensing?hl=en*

est susceptible de produire des effets correcteurs rapides, finalement acceptées par les acteurs eux-mêmes, et étendus à l'ensemble de leurs usagers dans le monde.

Le secteur reste cependant fortement dominé par les acteurs extra-européens. En effet alors que le marché du cloud est en forte augmentation en Europe, M. Sébastien Lescop, directeur général de Cloud Temple, rappelle que « l*a part des acteurs européens dans le cloud est passée de 27 % en 2017 à 15 % aujourd'hui.* » (1)

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

Plus de deux ans après la publication de la loi du 21 mai 2024 visant à sécuriser et réguler l'espace numérique, les décrets d'application sur l'encadrement du recours aux crédits cloud ne sont pas parus.

### 3. Les quatre limites auxquelles se heurte l'application du droit de la concurrence

Pour importantes qu'elles soient, les sanctions prononcées ne suffisent pas à endiguer l'ensemble des pratiques problématiques constatées. Un exemple concret en est fourni par M. Henri d'Agrain, délégué général du Cigref (2) : « *Sur ce marché, il existe manifestement un défaut d'action publique, puisqu'à de rares exceptions près, les autorités de concurrence et les pouvoirs publics sont restés largement inertes. Le rachat de VMware par Broadcom en constitue une illustration emblématique. Ce rachat a été annoncé en mai 2022. Or, dès septembre 2021, le Cigref avait saisi l'Autorité de la concurrence sur les pratiques abusives de Broadcom à la suite du rachat de CA Technologies et de Symantec Enterprise. Malheureusement, cette saisine n'a jamais été instruite.*

« *En 2022, nous avons alerté la Commission européenne et les autorités françaises : si Broadcom rachetait VMware, les mêmes mécanismes se reproduiraient. À l'époque, tous les adhérents du Cigref, publics comme privés, étaient clients de VMware d'une manière ou d'une autre. Le risque de position ultradominante était donc évident. Les faits nous ont malheureusement donné raison. En 2024 et 2025, nous avons observé des hausses tarifaires massives, des modifications unilatérales des modèles de licences et de tarification, et une véritable prédation sur l'économie européenne, dans un climat d'atonie quasi totale des pouvoirs publics, et notamment des autorités de concurrence.* »

Quatre limites à l'application du droit de la concurrence ont été mises en évidence.

---

*(1) Table ronde, ouverte à la presse, réunissant des fournisseurs de cloud le 21 avril 2026.*

*(2) Audition de M. Henri d'Agrain, délégué général du Club informatique des grandes entreprises françaises (Cigref), le 30 avril 2026.*

Première limite, **toute position très forte d'un acteur ne peut pas être qualifiée de position dominante au sens du droit de la concurrence.** Il revient à l'Autorité de la concurrence de démontrer que le consommateur a subi un préjudice du fait de la position qu'occupe un acteur dominant sur un marché particulier, comme l'explique M. Umberto Berkani : « *Si une position dominante a été acquise par le mérite, elle n'est pas répréhensible en soi. En revanche, l'acteur concerné ne doit pas utiliser cette puissance pour fausser la concurrence sur un autre marché. Par exemple, le producteur exclusif de micros de haute qualité ne doit pas pouvoir contraindre ses clients à acquérir également ses composants de qualité inférieure en liant les deux produits, car il gagnerait ainsi artificiellement des parts de marché. L'idée fondamentale est qu'un monopole, même mérité, finit par augmenter ses tarifs au préjudice du consommateur. Le droit de la concurrence intervient donc pour sanctionner les pratiques qui ne relèvent plus du mérite, mais de l'utilisation abusive d'une position acquise, toujours dans le but ultime de protéger le consommateur.* » [(1)]

Deuxième limite, **le droit de la concurrence n'est pas forcément adapté pour appréhender le cumul de positions qui, prises individuellement, par marché, ne sont pas sanctionnables**. « *Bien que nous ne disposions pas de données chiffrées précises sur le degré de dépendance des entreprises ou des administrations françaises, nous identifions un certain nombre d'acteurs prépondérants. J'emploie ce terme plutôt que celui de « dominant », car ce dernier revêt une acception juridique stricte impliquant généralement un acteur unique sur un marché donné. Or la complexité du numérique réside dans l'absence d'un secteur ou d'un marché unifié. La puissance de ces acteurs ne se cristallise pas sur un marché unique, mais résulte d'une sédimentation d'activités où s'additionnent effets de réseau, économies d'échelle, effets d'apprentissage et mécanismes de verrouillage des clients. Si occuper la première place est initialement un mérite concurrentiel, cette position permet ensuite de capter des informations et d'ériger des barrières à l'entrée. C'est là tout le paradoxe de la concurrence : on ne la pratique que dans l'espoir de devenir, à terme, l'unique opérateur de son marché. Sur certains segments du numérique, on observe ainsi une accumulation de phénomènes qui, pris isolément, se retrouvent sur n'importe quel marché, mais dont le cumul engendre une prépondérance manifeste. Les acteurs puissants dans le secteur du cloud, que vous avez cités, le sont également sur de nombreux services adjacents.*

« *Toute la difficulté pour le droit de la concurrence, fondé sur le principe de la liberté d'entreprendre, est que l'on ne peut limiter l'action d'un opérateur que si ce dernier contrevient aux règles relatives aux ententes ou à l'abus de position dominante. Pour ce faire, il est impératif d'identifier un marché spécifique sur lequel l'acteur exerce sa domination. Dès lors que trois acteurs se partagent 80 % d'un marché, établir la dominance de l'un d'entre eux devient complexe, ce qui interroge l'applicabilité même du droit commun. En revanche, sur les marchés où l'un de ces acteurs est clairement dominant, nous disposons, à l'instar de la Commission européenne, d'une jurisprudence abondante sanctionnant les abus*

*(1) Audition de M. Umberto Berkani, rapporteur général de l'Autorité de la concurrence, le 5 mai 2026.*

*constatés. Mais lorsque nous sommes face à des prépondérances multiples, et en partant du principe que ces acteurs sont en concurrence et ne s'entendent pas, il faut un autre texte pour intervenir. C'est là qu'intervient le DMA, qui permet d'agir même en l'absence d'un cas de dominance classique.* »

**Troisième limite, le droit de la concurrence n'a pas vocation à se substituer à la politique industrielle** ou à en constituer un maillon essentiel. Sa raison d'être est d'empêcher la constitution de positions causant un préjudice pour le consommateur. Il ne doit pas être conçu comme un instrument pour renforcer des positions d'acteurs nationaux « *S'agissant des grandes questions relatives au numérique, je retiendrai d'abord que le droit de la concurrence n'entre pas en compte dans la création de grands champions européens. Le contrôle des concentrations ne s'oppose pas à l'émergence de tels acteurs, mais consiste à analyser les pouvoirs de marché au sein d'espaces définis. Ainsi, lorsque les marchés examinés présentent une dimension nationale, par exemple en raison de réglementations spécifiques, l'analyse du pouvoir de marché s'exerce nécessairement à cette échelle* ».

À ce titre, M. Berkani soulignait le risque de vouloir soumettre le droit de la concurrence à des injonctions politiques, alors que cela n'est pas son objet. D'autres moyens sont plus adaptés pour favoriser le développement de filières européennes. Ainsi, « *la concurrence, loin d'être une fin en soi, constitue un moyen dont l'objectif précis est de garantir le développement de marchés ouverts et équitables. S'il existe d'autres ambitions politiques, notamment en matière économique, il n'appartient que marginalement au droit de la concurrence de se substituer à la représentation nationale ou aux gouvernements pour atteindre des objectifs de politique industrielle ou commerciale. Cela ne signifie pas que le droit de la concurrence soit hermétique à ces enjeux, mais que sa mission principale consiste à garantir le bon fonctionnement des marchés dans le cadre de la réglementation en vigueur.* »

**Il est intéressant de noter que les injonctions peuvent parfois aller dans le sens inverse, sous la forme de pressions pour que les autorités de régulation n'appliquent pas complètement des textes existants** : « *La Commission a été régulièrement sommée d'alléger les contraintes liées à l'application des règles de concurrence ou du DMA qui pèsent sur les entreprises américaines du numérique, notamment en échange d'une baisse de droits de douane sur l'acier et l'aluminium. Cependant, l'adoption des décisions sur le fondement du DMA ou du droit de la concurrence depuis 2025 attestent de la position de la Commission européenne. L'Autorité réitère son appel à ne pas faire de la politique de concurrence une monnaie d'échange dans le contexte de négociations commerciales ou diplomatiques et apporte son entier soutien à une mise en œuvre vigoureuse et impartiale des règles de concurrence ex ante et ex post dans le secteur de l'économie numérique* » [(1)]. M. Thierry Breton confirmait la réalité de ces

*(1) Réponse de l'Autorité de la concurrence au questionnaire de la rapporteure.*

pressions [1] : « *Une amende a effectivement été prononcée [au titre du DSA], et elle a eu un certain retentissement. C'est d'ailleurs quelques jours après l'annonce de cette sanction que j'ai été informé que je n'étais plus* persona grata *aux États-Unis – je ne dis pas qu'il y a une relation de cause à effet entre ces deux événements, mais je remarque la coïncidence du calendrier.* »

Enfin, dernière limite, **le déséquilibre de moyens entre les Big Tech et les autorités de concurrence** est tel que l'application du droit est complexe, imparfaite et prend de nombreuses années. « *Bien que ce phénomène ne soit pas propre au numérique, l'écart de ressources entre les grandes entreprises et les autorités de concurrence est colossal. Dans un État de droit, les entreprises ont le droit de se défendre, et il nous appartient de rendre nos procédures plus efficaces pour compenser ce déséquilibre. […] Concernant nos moyens, le constat est simple : à missions constantes, nous avons perdu cinq ETP en deux ans. Avant d'envisager de nouvelles prérogatives, il faudrait donc déjà pouvoir assurer nos missions historiques avec les effectifs antérieurs* » [2].

S'ajoute au déséquilibre de moyens la **disproportion entre les montants d'amendes prononcés et l'activité économique générée par les entreprises concernées**. Ainsi que l'indiquait M. Thierry Breton, « *120 millions d'euros représentent un montant dérisoire pour des entreprises qui valent des centaines, voire des milliers de milliards. Elles ne se retrouvent pas étranglées. Je rappelle que les textes votés par les colégislateurs, en l'occurrence le DSA – puisque c'est bien celui auquel vous faites allusion, même si des sanctions ont aussi été prononcées au titre du DMA –, prévoient des amendes pouvant aller jusqu'à 6 % du chiffre d'affaires mondial. Si la plateforme ne corrige pas les manquements qui ont été identifiés, la procédure permet de saisir un juge pour obtenir, le cas échéant, une décision de fermeture temporaire du service.* »

« *Je me suis beaucoup battu pour introduire cette possibilité. J'ai eu du mal à y parvenir, car nombre de mes collègues atlantistes de la Commission – je ne les critique pas – étaient contre. Je tenais absolument à ce dispositif, car il s'agissait là enfin d'une sanction majeure pour des entreprises qui font 30 %, 40 % voire 50 % de leur chiffre d'affaires sur le marché européen. Or elles ne regardent qu'une chose : la réaction des marchés financiers. Pour nous, c'est un élément essentiel : si nous représentons un tel poids dans leur chiffre d'affaires et leurs profits, nous devons l'utiliser dans la logique de rapport de force qui prévaut désormais – et qui, hélas, s'est substituée à la logique de confiance.* »

L'application de sanctions pécuniaires et d'injonctions intervient au terme de procédures longues et complexes, nécessitant de démontrer une atteinte à la concurrence sur un marché pertinent. Elle ne permet pas de résoudre de façon structurelle le déséquilibre économique et technique entre les Gafam et les autres

---

*(1) Audition de M. Thierry Breton, ancien commissaire européen au Marché intérieur, ancien président-directeur général d'Atos SE, le 15 avril 2026.*

*(2) Audition de M. Umberto Berkani, rapporteur général de l'Autorité de la concurrence, le 5 mai 2026.*

acteurs. De ce point de vue, le démantèlement pourrait constituer une solution structurelle, mais il est fortement encadré, comme l'indique M. Umberto Berkani : « *À l'instar du démantèlement des trusts américains, nous pouvons défaire des positions dominantes, bien que le standard de preuve requis soit extrêmement élevé. Cela se justifie par le respect de la liberté d'entreprendre : des mesures attentatoires aux libertés individuelles ne peuvent être prises que dans des situations exceptionnelles* » (1).

Plutôt que de mettre en œuvre cette solution ultime, la Commission européenne a souhaité compléter le droit de la concurrence par des mécanismes de contrôle des pouvoirs de marché *ex ante*, complétant les pouvoirs de sanction *ex post*, sanctionnant une atteinte déjà commise.

### C. LE DMA, L'INTRODUCTION DE MESURES DE RÉGULATION *EX ANTE* APPLICABLES AUX PRINCIPALES PLATEFORMES

Le DMA résulte d'une forme d'aveu d'échec, ou en tout cas du constat selon lequel le droit de la concurrence est insuffisant pour prévenir avec efficacité les agissements de grandes plateformes du numérique, compte tenu de la célérité d'action requise vis-à-vis d'elles. Le choix de donner compétence exclusive à la Commission européenne pour prendre des décisions au titre du DMA relève aussi d'un souci d'efficacité face à des acteurs de taille mondiale.

Ce règlement introduit des règles spécifiquement applicables aux plateformes qualifiées de *gatekeepers* par la Commission européenne qui fournissent l'un des dix « services de plateforme essentiels » visés par le texte et remplissent des critères objectifs (nombre d'utilisateurs, capitalisation boursière…). Les entreprises désignées comme contrôleurs d'accès doivent se conformer à un certain nombre d'obligations et d'interdictions : par exemple, permettre l'interopérabilité de leurs services avec les services concurrents ou, à l'inverse, ne pas favoriser leurs propres services et produits proposés par rapport aux services ou produits similaires proposés par des tiers sur la plateforme (articles 5 à 7 du DMA).

Le DMA ne constitue pas une rupture avec le droit de la concurrence. En effet, les obligations figurant dans le DMA s'inspirent de pratiques anticoncurrentielles sanctionnées par les autorités de concurrence. Le DMA est un outil complémentaire des règles de concurrence traditionnelles qui restent pleinement applicables aux pratiques non couvertes par le DMA. Il repose ainsi sur le principe d'une régulation *ex ante,* spécifique aux pratiques d'acteurs importants pour garantir un secteur numérique plus équitable, concurrentiel et innovant, en limitant les pratiques anticoncurrentielles et en protégeant les consommateurs et les entreprises. Comme l'explique M. Berkani, « *l'instauration d'un nouveau niveau de régulation s'explique par la complexité de la collecte de données, issue de sources et de stratégies très diverses. Si le droit de la concurrence dispose de leviers puissants, il ne peut cependant pas tout traiter seul. Le DMA a donc été conçu*

*(1) Audition de M. Umberto Berkani, rapporteur général de l'Autorité de la concurrence, le 5 mai 2026.*

*comme un complément indispensable pour gagner en réactivité face à des pratiques déjà bien identifiées, sans pour autant chercher à innover juridiquement. Il n'appartient pas au DMA de créer de nouvelles catégories d'abus, cette mission demeurant le propre du droit de la concurrence. Une réelle complémentarité s'opère ainsi : dès lors qu'une pratique ne relève pas spécifiquement du DMA, elle continue d'être appréhendée sous l'angle de l'abus de position dominante, même si elle concerne une plateforme régulée.* »

Le DMA étant d'application récente, se pose la question de son effectivité vis-à-vis des pratiques des Gafam. Les premières sanctions sur le fondement du DMA ont été prononcées le 23 avril 2025, à l'encontre d'Apple (500 millions d'euros) et de Meta (200 millions). Dans un document de travail d'avril 2026, la Commission a analysé les effets de la mise en œuvre du DMA sur les marchés du numérique [(1)].

Selon la Commission, la première mise en œuvre du DMA s'est avérée efficace pour modifier le comportement, les choix de conception technique et les dispositions contractuelles des contrôleurs d'accès, créant ainsi des opportunités pour leurs concurrents. La Commission renvoie notamment aux exemples suivants :

– les navigateurs et moteurs de recherche alternatifs, notamment Aloha, Ecosia, Qwant et DuckDuckGo, ont connu un regain d'intérêt depuis la mise en place des écrans de choix, certains fournisseurs faisant état d'une croissance significative de leur base d'utilisateurs sur des marchés clés tels que la France et l'Allemagne ;

– des boutiques d'applications alternatives, telles qu'Aptoide, Epic Games Store et AltStore, ont fait leur apparition sur les systèmes d'exploitation d'Apple auparavant fermés aux boutiques d'applications tierces et ne cessent d'élargir leur offre ;

– les développeurs d'applications peuvent désormais distribuer leurs applications depuis leurs propres sites web sur iOS et iPadOS ;

– une quarantaine de développeurs tiers, dont beaucoup sont des PME, comme DataPods, Gener8, Hoda, Smart Data Donation Service et Fabric, ont réussi à s'intégrer aux API des contrôleurs d'accès pour transférer les données des utilisateurs et développer des services innovants ;

– l'interopérabilité des messageries a permis l'émergence de nouveaux fournisseurs, notamment Fyello Productivity, qui propose BirdyChat, l'un des premiers services à interagir avec WhatsApp.

---

*(1) Commission staff working document Accompanying the document Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the Review of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), in accordance with Article 53 thereof, avril 2026*

*https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52026SC0123*

La Commission relève également que la mise en œuvre du DMA a d'ores et déjà renforcé l'autonomie et la capacité d'action des utilisateurs finaux dans plusieurs domaines clés en leur donnant les moyens de reprendre le contrôle de leurs données et de faire leurs propres choix. Parmi les bénéfices pour les clients, utilisateurs et consommateurs du fait du DMA, elle mentionne notamment les éléments suivants ;

– les utilisateurs finaux disposent d'un choix plus large grâce aux écrans de sélection des navigateurs et des moteurs de recherche, ainsi qu'à la possibilité de désinstaller les applications par défaut ;

– les utilisateurs ont également un meilleur contrôle sur la manière dont leurs données personnelles sont utilisées par les contrôleurs d'accès. Ces derniers doivent obtenir le consentement des utilisateurs finaux avant de combiner ou d'utiliser de manière croisée leurs données personnelles entre leurs différents services, ce qui donne le contrôle aux utilisateurs et empêche tout profilage non sollicité. Changer de service est également plus facile grâce à la portabilité et au partage des données ;

– les utilisateurs finaux peuvent désormais facilement transférer leurs données en dehors des écosystèmes des contrôleurs d'accès, y compris les données issues des publications et des likes sur les réseaux sociaux Facebook, Instagram et TikTok, leur historique de recherche sur Google Search et leur historique d'achats sur Amazon ;

– Alphabet n'oblige plus les utilisateurs d'Android, de YouTube et de Google Play à s'abonner au service Gmail pour pouvoir accéder à ces services ;

– les hôtels et les loueurs de voitures peuvent désormais fixer leurs propres prix et conditions sur leurs propres plateformes et ne sont plus empêchés de proposer de meilleures offres en dehors de plateformes telles que Booking.com, ce qui se traduit par des prix plus bas et de meilleures conditions pour les utilisateurs finaux.

Enfin, la Commission souligne qu'elle restera particulièrement vigilante s'agissant des secteurs du cloud et des services IA, domaines dans lesquels elle a déjà pris des mesures. Elle continuera de suivre l'évolution du marché et d'évaluer si des ajustements supplémentaires sont nécessaires lors des prochains réexamens. Elle a ainsi a annoncé l'ouverture de trois enquêtes, au titre du DMA, dans le secteur du cloud :

– deux enquêtes de marché concernant une éventuelle désignation « qualitative » d'Amazon Web Services et de Microsoft Azure : si l'instruction de la Commission conclut que ces services constituent des points d'accès majeurs pour les entreprises utilisatrices qui cherchent à atteindre leurs utilisateurs finaux (*important gateways)*, ces services seront ajoutés à la liste des services de plateforme essentiels pour lesquels Amazon et Microsoft sont déjà désignés comme contrôleurs d'accès et les obligations du DMA leur seront donc applicables. La

décision est attendue pour la fin de l'année 2026 et, en cas de désignation, les obligations de conformité s'appliqueraient à compter de mai 2027 ;

– une troisième enquête de marché vise à recueillir des informations auprès des acteurs du marché concernés afin d'évaluer si les obligations actuelles au titre du DMA sont efficaces pour lutter contre les pratiques dans le secteur du cloud. L'enquête portera, par exemple, sur les obstacles à l'interopérabilité entre les fournisseurs, l'accès limité ou conditionné des entreprises utilisatrices aux données, les services de vente liée et de groupage et les clauses contractuelles potentiellement déséquilibrées.

Du fait de ses caractéristiques et des positions qu'ont progressivement constituées les Gafam, le numérique est l'un des secteurs les plus scrutés par les autorités européennes et nationales chargées de l'application du droit de la concurrence. Les sanctions prononcées sont significatives, puisqu'elles dépassent 17,2 milliards d'euros depuis 2010. Google concentre à elle seule 70 % du montant des amendes attribuées aux cinq acteurs, témoignant ainsi de la répétition de pratiques illégales.

Toutefois, le droit de la concurrence connaît des limitations fortes. Les articles 101 et 102 du TFUE ne peuvent être appliqués qu'après de longues procédures, nécessitant de démontrer, rétroactivement et avec un haut standard de preuve, l'existence d'abus sur un marché déterminé. Dans un écosystème en perpétuelle évolution, les grands acteurs internationaux conservent toujours un temps d'avance : l'apparition constante de nouvelles technologies et de nouveaux services donne systématiquement lieu à de nouvelles pratiques obéissant chaque fois aux mêmes logiques (préférence donnée à ses propres produits, vente groupée, barrières techniques à l'entrée, capacité de négociation déséquilibrée des conditions contractuelles).

L'entrée en vigueur du DMA pourrait constituer un tournant, et ses effets devront être scrutés au cours des prochaines années afin de mesurer s'il a entraîné un changement profond du fonctionnement du secteur. Toutefois, et ainsi que le montre l'exemple de l'encadrement des crédits cloud et des *egress fees*, la mise en application du DMA ne doit pas détourner les pouvoirs publics de l'édiction de règles ciblées susceptibles de faire changer rapidement des pratiques tuant dans l'œuf les velléités des nouveaux entrants.

## CHAPITRE 7 – LE NARRATIF DE L'ABSENCE D'ALTERNATIVE EUROPÉENNE

Lors de son audition, M. Michel Paulin, président du comité stratégique de filière logiciels et solutions numériques de confiance, a appelé à « *dénoncer les narratifs bien rodés, issus d'un lobbying puissant, qui assènent à longueur de temps qu'il n'existerait pas d'alternative* » (1).

### A. UN DISCOURS CONSTANT DE RÉSIGNATION

La commission d'enquête a constaté la diffusion d'un narratif renvoyant systématiquement dos à dos la souveraineté et la compétitivité, comme si le fait de choisir des solutions numériques européennes impliquait nécessairement des renoncements sur le plan de la performance et des coûts. M. Aiman Ezzat, directeur général de Capgemini, première société de conseil en Europe, s'est fait le relais d'une telle idée, en affirmant que « *la question qui revient le plus souvent »* parmi ses clients est « *puis-je renforcer ma souveraineté sans sacrifier ma compétitivité ? L'équilibre entre souveraineté et compétitivité est devenu le sujet central*. » (2)

#### 1. Des solutions moins performantes et plus coûteuses ?

La première idée reçue serait que les fournisseurs européens ne seraient pas en mesure de fournir les fonctionnalités demandées par les entreprises. La directrice générale de France Digitale a ainsi déclaré devant la commission d'enquête que, *« même si [leurs] membres étaient sensibilisés à l'enjeu de souveraineté »*, il n'était pas possible *« de les forcer à se tourner vers des offres technologiques françaises qui ne correspondent pas à leurs besoins techniques* ».

Cela a été battu en brèche par l'ensemble des industriels auditionnés par la commission d'enquête, qui ont au contraire fait état d'un développement rapide des offres européennes, notamment sur le segment du cloud.

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. Ils se sont tous inscrits en faux contre l'idée, souvent entendue, selon laquelle la bataille du cloud serait perdue face à des *hyperscalers* trop puissants pour être rattrapés. « *C'est le lobbying des Américains qui le prétend. Non seulement il n'est pas perdu, mais il est plus important que jamais, car aujourd'hui, toute l'innovation européenne, ou presque, est dépendante du cloud* », a déclaré M. Damien Lucas, directeur général de Scaleway (3).

---

*(1) Audition de M. Michel Paulin, président du comité stratégique de filière « solutions numériques de confiance » du Conseil national de l'industrie, ancien directeur général d'OVH, le 7 avril 2026.*

*(2) Audition de M. Eiman Ezzat, directeur général de CapGemini, et Mme Karine Brunet, directrice mondiale des opérations et du delivery, et membre du comité de direction générale du groupe, le 26 mars 2026.*

*(3) Table ronde réunissant des fournisseurs de cloud le 21 avril 2026.*

Si les fournisseurs européens ont tardé à proposer la couche des services managés, à savoir les services PaaS, ils ont, depuis, développé leur offre et enrichi les fonctionnalités. Scaleway couvrirait ainsi 90 % des cas d'usage, et l'entreprise serait en mesure de développer les 10 % restants à la demande de ses clients, comme elle le fait avec France Télévisions (1).

L'offre de solutions qualifiées SecNumCloud s'est également étoffée, avec la certification de six nouveaux acteurs au cours de l'année 2025. Au total, en mai 2026, dix fournisseurs de services avaient obtenu la qualification SecNumCloud pour dix-sept de leurs offres (2). Le bilan de la doctrine Cloud au centre présenté par la Dinum en février 2026 souligne également l'enrichissement des fonctionnalités proposées sur des socles SecNumCloud, avec l'émergence de services d'orchestration de conteneurs managé. Cette dynamique a été stimulée par le travail engagé par l'État pour guider les acteurs privés dans l'amélioration de leur offre par des partages sur ses besoins, comme l'a souligné Mme Stéphanie Schaer : « *L'existence d'un cahier des charges faisant état des fonctionnalités attendues, avec un classement par priorités, a aidé les industriels à améliorer leurs réponses* » (3).

*(1)* Ibid.

*(2) Anssi, catalogue des produits, services, profils de protection et sites certifiés, qualifiés, agréés, juin 2026.*

*(3) Audition de Mme Stéphanie Schaer, directrice interministérielle du numérique, et M. Jérémie Vallet, son adjoint, le 14 avril 2026.*

**SERVICES D'INFORMATIQUE EN NUAGE QUALIFIÉS SECNUMCLOUD**

| Fournisseur du service | Service | Type | Début de qualification | Fin de qualification |
|---|---|---|---|---|
| **Cegedim** | CegNumCloud Secured | IaaS | 04/12/2024 | 04/12/2027 |
| **Cloud Temple** | IAAS – Secure Temple | IaaS | 30/05/2025 | 30/05/2028 |
| | PaaS Openshift | PaaS | 30/05/2025 | 30/05/2028 |
| **Index Education** | Pronote | SaaS | 05/05/2025 | 18/06/2027 |
| | Pronote Primaire | SaaS | 05/05/2025 | 18/06/2027 |
| | Hyperplanning | SaaS | 05/05/2025 | 18/06/2027 |
| | EDT | SaaS | 05/05/2025 | 18/06/2027 |
| **OVH** | Hosted Private Cloud powered by VMware | IaaS | 28/12/2023 | 29/12/2026 |
| | Bare Metal Pod | IaaS | 24/03/2025 | 24/03/2028 |
| **Oodrive** | Oodrive_Meet | SaaS | 20/01/2025 | 25/01/2028 |
| | Oodrive_Work | SaaS | 20/01/2025 | 25/01/2028 |
| | Oodrive_Work_Share | SaaS | 20/01/2025 | 25/01/2028 |
| **Orange Business Services** | Cloud Avenue SecNum | IaaS | 11/07/2025 | 11/07/2028 |
| **Outscale** | IaaS Cloud on Demand | IaaS | 30/11/2023 | 30/11/2026 |
| **Thales Cloud Securisé** | Cloud de confiance S3NS | IaaS, PaaS, SaaS | 17/12/2025 | 17/12/2028 |
| **Whaller** | Whaller Donjon SaaS | SaaS | 02/08/2024 | 02/08/2027 |
| **Worldline** | Worldline Cloud Services – Secured IaaS | IaaS | 24/03/2025 | 31/03/2028 |

*Source : Anssi, juin 2026.*

Les centaines de services proposées par les offreurs américains constitueraient davantage un argument contractuel qu'une nécessité, selon M. Eric Haddad, président exécutif de NumSpot : « *L'un des moyens de justifier un bon projet d'achat est cette quantité de services qui, en réalité, seront très peu utilisés. (…) La panoplie de services que nous proposons est très largement suffisante, et quand elle ne l'est pas, nous nous arrangeons avec le client pour développer ce qui est nécessaire* » [(1)]. M. Michel Paulin dresse le même constat : *« Quand j'entends des chefs d'entreprises me dire « vous n'avez pas tous les services », je réponds « lequel ? », ils ne savent pas vous le dire »* [(2)].

M. Philippe Miltin, directeur général d'Outscale, abonde : « *Le sujet est de savoir si nous sommes en capacité de développer des outils logiciels (…) pour opérer un certain nombre de solutions, notamment critiques. La réponse est oui, et nous le prouvons absolument tous les jours, en France, en Europe et dans le monde.*

*(1) Table ronde réunissant des fournisseurs de cloud le 21 avril 2026.*

*(2) Audition de M. Michel Paulin, président du comité stratégique de filière « solutions numériques de confiance » du Conseil national de l'industrie, ancien directeur général d'OVH, le 7 avril 2026.*

*Chez Dassault Systèmes, de plus en plus de pays nous demandent de fournir une solution dite souveraine, en dehors des hyperscalers, parce que nous disposons de ces capacités, avant tout d'un point de vue logiciel. Nous opérons notre propre orchestrateur et hyperviseur, développé par Outscale, et cette capacité à fournir une boîte à outils est un élément extrêmement important. Nous savons le faire. Nous avons toutes les capacités en termes d'ingénierie système. Il faut avoir à l'esprit que les mathématiques françaises sont parmi les plus réputées, et nos ingénieurs sont très recherchés en France comme à l'étranger. Nous avons toute cette capacité de développement*. » (1)

Les personnes auditionnées ont également démenti l'idée selon laquelle les offres européennes seraient plus coûteuses que celles des hyperscalers. « *En moyenne, nous sommes presque 40 % moins chers que les hyperscalers. Quand on connaît leur niveau de marge, ce n'est pas le plus difficile* », a affirmé le directeur général de Scaleway (2). Ces derniers peuvent cependant donner le sentiment d'une baisse de coûts en accroissant le volume de services proposés, sans lien avec les besoins du client, dans le cadre de contrats pluriannuels.

### 2. Des solutions moins intégrées ?

Les auditions ont également conduit à relativiser l'impossibilité d'atteindre le degré d'intégration des produits américains.

Selon M. Yann Lechelle, auditionné au nom d'Eurostack, le problème ne serait pas du côté de l'offre, mais de la demande : « *Du côté de l'offre, des alternatives existent pourtant, dans toutes les couches de la stack. (…) On nous oppose souvent l'argument des hyperscalers. Certes, il reste du travail pour agréger l'offre et créer des produits intégrés et attractifs, domaine dans lequel les entreprises américaines excellent. Elles vendent des bundles, des paquets intégrés. Mais nous avons les compétences, les composantes et le savoir-faire pour produire des offres équivalentes. Cependant, nous manquons d'acheteurs : sans demande, tous les meilleurs plans demeurent théoriques*. » (3) Si le *bundle* était décomposé, les fournisseurs français et européens pourraient répondre aux différents segments. Ainsi, AWS, plateforme de cloud leader, réaliserait 80 % de son chiffre d'affaires sur un seul produit, les machines virtuelles, qui est également disponible en France.

Toute l'ambition de l'initiative Eurostack consiste justement à pousser les entreprises européennes à se coordonner afin d'être en mesure de couvrir l'ensemble de la stack et de concurrencer les *hyperscalers.* Le récent appel d'offres de la Commission européenne en matière d'informatique en nuage a donné à voir une dynamique similaire, les cloudeurs ayant candidaté sous forme de consortiums.

---

*(1) Table ronde réunissant des fournisseurs de cloud le 21 avril 2026.*

*(2)* Ibid.

*(3) Audition du collectif Eurostack, le 26 mars 2026.*

Le défaut d'intégration n'est pas un obstacle lorsque l'on dispose des compétences internes nécessaires, comme l'a fait valoir M. Nicolas Vivant, directeur de la stratégie numérique de la commune d'Echirolles : « *Concernant l'intégration des solutions, j'ai entendu beaucoup d'intervenants déplorer le manque de solution intégrée. Pour les communes de taille moyenne ou importante, c'est notre métier d'intégrer de façon cohérente l'ensemble des solutions dans notre système d'information. C'est notre métier d'interfacer une IA avec notre Nextcloud pour résumer un texte, ou de lancer une visioconférence depuis notre messagerie. Quand on a les compétences en interne, ou même en s'appuyant sur des prestataires, ce travail d'intégration peut être fait. La filière du libre a raison de dire que son incapacité à proposer une solution « tout-en-un » est un handicap face aux big tech. Mais dans les collectivités, nous pouvons aussi réaliser cette intégration par nous-mêmes.* » (1)

Des appels d'offres récents se sont également traduits par la sélection de partenaires européens, démontrant leur capacité à répondre aux besoins des administrations publiques lorsque les cahiers des charges sont définis de façon adéquate.

En avril 2026, la Commission européenne a ainsi retenu quatre opérateurs européens pour fournir des services d'informatique en nuage aux institutions et organismes de l'Union européenne, pour un montant maximal de 180 millions sur six ans (2). Ils ont été sélectionnés sur la base du *Cloud Sovereignty Framework* élaboré par la Commission en octobre 2025, qui évalue la souveraineté à l'aune de huit critères stratégiques, juridiques, techniques, opérationnels et environnementaux (3). Il s'agissait essentiellement de consortiums : l'opérateur luxembourgeois Post Telecom avec CleverCloud et OVHcloud ; l'offre cloud allemande Stackit ; Scaleway ; et l'opérateur de télécom belge Proximus, en partenariat avec S3NS, Clarence et Mistral.

### B. LES 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 et les croyances portés par leurs technologies.** Les travaux de Mme Ophélie Coelho ont ainsi mis en évidence le rôle de ce qu'elle appelle des « passeurs de technologie » : « *Ce sont, par exemple, les sociétés de conseil, souvent américaines, mais aussi les développeurs formés à leurs technologies, qui ont été formés quasi exclusivement à des technologies propriétaires. Il est rare que ces profils connaissent bien les technologies open source ou européennes. Une fois sur le marché du travail, ces*

*(1) Table ronde sur le logiciel libre le 6 mai 2026.*

*(2) Commission européenne, communiqué de presse, 17 avril 2026.*

*(3) Direction générale des services numériques de la Commission européenne,* Cloud Sovereignty Framework, version 1.2.1, *octobre 2025.*

*ingénieurs et techniciens deviennent les meilleurs ambassadeurs de ces géants, car leur accès à l'emploi dépend de ces technologies privées.* » (1)

### 1. Les entreprises de services du numérique

**Par les liens étroits qu'ils entretiennent avec les grandes entreprises numériques extra-européennes, les cabinets de conseil ont pu contribuer à perpétuer leur domination sur le marché**, en recommandant à leurs clients de retenir leurs solutions.

Le poids de ces prestataires au sein de l'État a été mis en lumière par la commission d'enquête sénatoriale sur l'influence croissante des cabinets de conseil privés sur les politiques publiques. Ses travaux ont montré que les dépenses de conseil se concentraient à 72 % sur le segment informatique, ce qui représentait 646 millions d'euros dans le secteur public en 2021 (2). Cette influence se vérifie toujours en 2025, Capgemini ayant réalisé 588 millions de chiffre d'affaires avec le secteur public en France (3).

La commission d'enquête a cherché à déterminer le rôle que jouaient ces cabinets de conseil dans la sélection des solutions technologiques. Si le directeur général de Capgemini a attesté que la décision revenait entièrement au client, les limites entre le conseil et la coproduction peuvent être parfois floues, notamment lorsque les prestataires interviennent très en amont dans la définition du projet. La question se pose de l'influence qu'a eue Capgemini dans le choix de Microsoft Azure pour héberger la Plateforme des données de santé, ainsi que dans celui de Salesforce et AWS par EDF.

Le président et la rapporteure ont relevé les nombreux liens qu'entretient Capgemini avec les géants du numérique. **Capgemini a notamment conclu des partenariats stratégiques avec Microsoft, AWS et Google**, afin d'accompagner ses clients dans l'adoption des technologies de ces entreprises.

Son directeur général, M. Aiman Ezzat a pleinement assumé ces partenariats, qui permettent aux prestataires de Capgemini d'être formés aux solutions des *hyperscalers* : « *C'est surtout la demande des clients qui explique nos choix de partenariats stratégiques. Si nous investissons auprès de Microsoft pour former nos équipes et obtenir des certifications sur des solutions innovantes – c'est bien un investissement ; rien n'est gratuit –, c'est pour répondre à une demande du marché. Nous n'aurions aucun intérêt à former des gens à des solutions qu'aucun client ne souhaiterait adopter ensuite* » (4). **Microsoft constitue de fait le premier partenaire technologique de Capgemini, la vente et l'accompagnement de leurs services représentant un peu plus de 4 milliards d'euros de chiffre d'affaires**,

---

*(1) Table ronde sur les infrastructures numériques le 2 avril 2026.*

*(2) Rapport fait au nom de la commission d'enquête sur l'influence croissante des cabinets de conseil privés sur les politiques publiques, enregistré à la présidence du Sénat le 16 mars 2022.*

*(3) Audition de M. Aiman Ezzat, directeur général de Capgemini, le 26 mars 2026.*

*(4)* Ibid.

selon les déclarations de M. Aiman Ezzat. Même si Capgemini n'a aucun avantage commercial direct à proposer les solutions de Microsoft, cette proximité a pu constituer un biais dans l'accompagnement assuré par ses équipes.

La proximité entre Capgemini et Microsoft s'illustre également dans la composition de son conseil d'administration, avec la nomination le 5 janvier 2026 de Mme Lila Tretikov, directrice-adjointe de Microsoft jusqu'en 2024.

**La posture de Capgemini, qui consiste à dénier toute responsabilité dans l'orientation de la demande, pour se borner à reproduire les situations oligopolistiques du marché, risque d'être un frein à l'engagement d'une véritable bascule**. Son directeur général a ainsi exclu tout rôle prospectif visant à éclairer ses clients sur les risques économiques, juridiques et stratégiques, auxquels ils s'exposent en choisissant une solution américaine : « *Quant au prix des licences, c'est aussi au client qu'il revient de prendre des décisions. En prenant Salesforce, il crée une certaine dépendance ; il en comprend les conséquences, et c'est à lui de gérer cela contractuellement. Nous ne conseillons pas nos clients sur ces aspects, mais en général sur l'évaluation de la solution technique par rapport à leurs besoins. C'est là que nous apportons une valeur ajoutée. Nous ne nous mêlons pas de négociation commerciale, de conditions de licence, de contraintes… En tout cas, je ne suis jamais intervenu dans ce domaine chez un client.* » (1)

Il est ainsi permis de douter de l'engagement de la société en faveur d'une plus grande indépendance numérique, malgré les déclarations de son directeur général sur son « *rôle moteur dans le développement d'offres, d'écosystèmes et de partenariats adaptés aux besoins en souveraineté des grandes orientations européennes* ». De fait, les actions de Capgemini en la matière sont ambiguës : la société a signé un partenariat avec AWS pour implémenter son cloud souverain, dont il a été montré les limites dans le chapitre 5 ; puis, elle a contribué à la **création de Bleu**, dont elle possède 50 % aux côtés d'Orange, qui a vocation à proposer une offre SecNumCloud reposant sur la technologie de Microsoft. **La rapporteure a regretté une décision** « ***qui permettra à Microsoft de continuer à asseoir sa domination alors que la qualification SecNumCloud aurait pu être l'occasion de développer des services fondés à 100 % sur des technologies européennes.*** » (2)

Certains éditeurs auditionnés ont questionné les prix élevés pratiqués par les ESN lorsqu'elles interviennent à leurs côtés sur un projet, en décalage avec leur contribution réelle. M. Thomas Fauré, président de Whaller, a ainsi cité l'exemple d'un contrat que l'entreprise avait remporté auprès de Pôle emploi grâce à Accenture : « *Il me semble qu'à cette occasion il y a eu une captation de valeur importante. Accenture a dirigé le projet au départ, mais nous a ensuite facturé une sorte de mensualité pendant toute la durée du contrat, qui n'était qu'une rétribution pour nous avoir apporté l'affaire, sans service associé.* » (3)

---

*(1)* Ibid.

*(2)* Ibid.

*(3) Audition du collectif #Fab8 le 29 avril 2026.*

**La rapporteure relève 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. L'émission « Complément d'enquête » du 18 septembre 2025 diffusée par France 2 a rapporté plusieurs témoignages suggérant que Capgemini détournait en partie le CIR de son objet pour rémunérer des consultants inoccupés entre deux missions. Si Capgemini a dénié ces affirmations, la rapporteure appelle l'État à renforcer le contrôle de l'utilisation du CIR par les grandes entreprises et à recentrer le dispositif sur les entreprises qui contribuent réellement à l'innovation.

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

### 2. Les centrales d'achat, caisses de résonance du *sovereignty washing*

**Le poids des centrales d'achat 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 [(1)]. La centrale d'achat de l'informatique hospitalière (CAIH) intermédie environ 500 millions d'achats numériques par an pour ses plus de 2 000 membres des secteurs hospitalier, médico-social et social [(2)], quand la centrale d'achat du numérique et des télécoms (Canut), dédiée aux collectivités locales et aux établissements publics, annonçait un volume d'achats numériques attendu entre 120 et 150 millions en 2025 pour plus de 3 000 bénéficiaires [(3)]. Le recours à ces structures est censé permettre aux acheteurs publics de sécuriser et d'accélérer la passation de marché, puisque les procédures de publicité et de mise en concurrence sont effectuées en interne par la centrale, ainsi que d'obtenir des prix plus favorables grâce à une mutualisation de l'offre.

La commission d'enquête sénatoriale sur les coûts et les modalités effectifs de la commande publique avait cependant pu déplorer que la plus grosse de ces centrales, l'Ugap, contribue à entretenir la dépendance des administrations aux grands fournisseurs extra-européens, en se bornant à « *assurer une simple intermédiation entre l'offre et la demande de solutions étrangères* » [(4)]. L'offre de l'Ugap a, en effet, longtemps reflété la domination des acteurs états-uniens sur le marché, comme en a témoigné M. Alain Garnier : « *Lorsqu'on ouvrait la page du*

*(1) Réponses écrites de l'Ugap au questionnaire de la rapporteure.*

*(2) CAIH, « La CAIH adopte son nouveau plan stratégique et lance Alternative », 26 février 2026.*

*(3) Laurent Sounack, « La Canut propose un nouveau marché dédié aux réseaux sécurisés »,* ChannelNews*, 17 octobre 2026.*

*(4) Rapport fait au nom de la commission d'enquête sur les coûts et les modalités effectifs de la commande publique et la mesure de leur effet d'entraînement sur l'économie française, sous la présidence de M. Simon Uzenat, par le rapporteur M. Dany Wattebled, et enregistré à la présidence du Sénat le 8 juillet 2025.*

*site internet des achats de logiciels, on voyait un gros logo Microsoft, un gros logo Oracle et un gros logo SAS Institute, et le reste se trouvait dans un fichier Microsoft Excel.* » (1)

En 2025, l'Ugap a déclaré 293 millions d'euros d'achats de produits Microsoft, 69 millions pour Oracle, et 62 millions pour VMware sur son marché multi-éditeurs (2). Les réponses écrites adressées par les ministères à la rapporteure ont confirmé que la majorité de leurs achats de logiciels américains avaient été passés par le biais de l'Ugap.

En réponse aux recommandations du Sénat, la centrale a amorcé un changement. Ses ministères de tutelle lui ont assigné explicitement la mission de contribuer au renforcement de la souveraineté industrielle et numérique dans la commande publique lors de la signature, le 2 juin 2026, de son nouveau contrat d'objectifs et de performances (COP) 2026-2028. Il y est précisé que « *les solutions souveraines, notamment en matière numérique, ainsi que les offres des PME et des startups innovantes seront valorisées dans le catalogue de l'UGAP* ».

Dans cette dynamique, l'Ugap travaille à renforcer l'information offerte à ses clients pour leur permettre d'identifier les solutions logicielles françaises et européennes, les conditions d'hébergement et de traitement des données, ainsi que les qualifications et référentiels applicables. Sur le marché Nuage public, les offres souveraines sont déjà référencées comme telles. S'agissant des logiciels, l'Ugap a complété les fiches produit pour indiquer la nationalité de l'éditeur. Son président, M. Edward Jossa, projette, dans un deuxième temps, d'offrir des outils d'aide à la décision : « *Nos outils conversationnels intégreront de l'IA et poseront des questions telles que « Êtes-vous soumis à la loi Sren ? », « Souhaitez-vous une solution conforme à la loi Sren ? », « Souhaitez-vous une solution alternative ? ». Nous développons des boutiques de souveraineté sur ugap.fr. Nous allons assez loin dans la présentation des solutions.* ». La centrale s'est enfin engagée à proposer une offre d'accompagnement dédiée à ses clients publics qui voudront migrer vers des solutions souveraines, en se concentrant d'abord sur l'aide à la sortie d'Office 365, d'Oracle et de VMware.

Ces outils ne pourront cependant être efficaces qu'à la condition de reposer sur des critères solides de classification. Or, **la rapporteure a constaté que l'Ugap avait retenu une méthodologie défaillante qui aboutit à relayer les pratiques de *sovereignty washing* de certaines grandes entreprises américaines**.

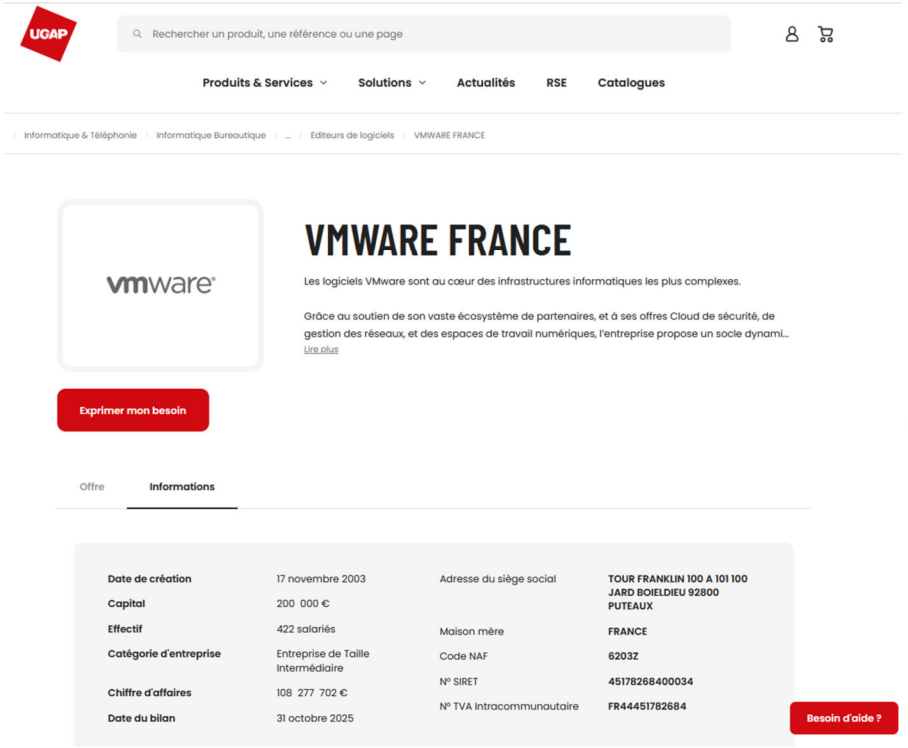
La centrale a déterminé la nationalité des éditeurs de logiciels à partir de données fournies par le cabinet Altares, en retenant le seul critère de la localisation de la maison mère mondiale, sans considérer plus finement les liens de dépendance avec une entité extra-européenne. Cela l'a conduite à **classer des logiciels américains aussi centraux que VMware ou Zoom comme français** sur son

*(1) Audition du collectif #Fab8 le 29 avril 2026.*

*(2) Réponses écrites de l'Ugap au questionnaire de la rapporteure.*

marché multi-éditeurs. Une évaluation plus fine des données a montré que, parmi les 50 premiers fournisseurs de logiciels sur le marché de l'Ugap, les éditeurs américains ont concentré 79 % des dépenses en 2025, bien au-dessus des 44,5 % sur l'ensemble du marché qu'a revendiqués M. Edward Jossa lors de son audition.

**FICHE PRODUIT DU LOGICIEL VMWARE SUR LE MARCHÉ MULTI-ÉDITEURS DE L'UGAP LE 19 JUIN 2026**




M. Edward Jossa a reconnu les limites de cette approche : « *La question de la souveraineté est particulièrement complexe dans le domaine informatique en raison du caractère dématérialisé des produits. (...) Les fournisseurs sont des distributeurs, les fabricants peuvent être des filiales françaises d'entreprises étrangères et les éditeurs peuvent proposer des solutions comportant des degrés de souveraineté différents. Nous nous contentons donc de retenir la nationalité du fournisseur, c'est-à-dire le pays où est implanté son siège social, et de sa maison mère. Cette solution est d'autant plus imparfaite qu'elle repose sur une base déclarative et que le secteur de la tech est en constant mouvement, mais nous n'en avons pas trouvé de meilleure* » (1). L'Union des hôpitaux pour les achats (UniHa) se heurte au même problème.

(1) *Table ronde des acheteurs publics le 9 avril 2026.*

**Recommandation n° 9 : Exiger que les centrales d'achat informent leurs clients sur la nationalité de l'éditeur des solutions logicielles qu'elles proposent, en se fondant sur une méthodologie solide qui tienne compte de la soumission de l'éditeur à des législations étrangères (localisation du siège, structure de l'actionnariat, liens de dépendance effectifs).**

L'inertie est également favorisée par le rôle prépondérant de trois distributeurs, qui intermédient une large partie des ventes de logiciels – les britanniques SCC et Computacenter et le groupe européen Econom. La société SCC notamment, premier fournisseur de l'Ugap, propose un grand nombre de solutions états-uniennes, ce qui limite la capacité des acteurs publics à réduire leurs dépendances. La rapporteure souligne qu'il revient à l'Ugap de formuler des attentes plus élevées en matière de souveraineté, en exploitant le pouvoir de négociation dont elle dispose à l'égard de SCC, dont M. Edward Jossa avait déclaré, devant le Sénat, qu'elle était « *très dépendante de l'Ugap compte tenu du volume considérable que représente le marché multi-éditeurs dont elle est titulaire* ». (1)

Le directeur de l'UniHA a reconnu la nécessité d'endosser une telle responsabilité à l'égard des fournisseurs : « *SCC est aussi un de nos plus importants fournisseurs. Vous avez raison, ils dépendent de la commande publique, et nous sommes donc, en tant que centrale d'achat, en droit d'être exigeants quant aux solutions qu'ils mettent en avant – c'est l'un des enjeux du comité stratégique de filière.* » (2).

La rapporteure s'est également étonnée de l'**inaction de l'Ugap face au détournement des codes de communication du marché Nuage public au profit de la stratégie de *sovereignty washing* d'un acteur américain**. Si le marché de l'Ugap dédié au cloud identifie bien la nationalité des différents hébergeurs par l'apposition d'un drapeau, la société états-unienne Kyndril a utilisé le logo tricolore du marché pour bâtir sa propre campagne de communication, entretenant le doute sur la nationalité de ses infrastructures, et partant leur soumission au droit extraterritorial. La rapporteure appelle ainsi les centrales d'achat à la plus grande vigilance quant à ces récupérations trompeuses qui visent à entretenir la confusion.

Il convient de relever que **d'autres centrales d'achat se démarquent par un rôle beaucoup plus pro-actif dans l'anticipation des risques de la dépendance pour leurs clients et la construction d'alternatives**. L'offre de cloud de la Canut est ainsi 100 % française, avec des solutions de cloud de confiance complétées par des offres d'hébergement régional d'acteurs locaux, et travaille au développement d'un environnement collaboratif souverain (ECS), tandis que la CAIH a lancé un partenariat d'innovation ambitieux pour construire une suite fondée sur des briques open source.

---

*(1) Audition au Sénat de M. Edward Jossa, président de l'Ugap, le 18 mars 2025.*

*(2) Audition de M. Thomas Jan, directeur général adjoint en charge de l'innovation et de la stratégie numérique de l'Union des hôpitaux pour les achats (UniHa), le 9 avril 2026.*

Selon M. Henri Verdier, le positionnement généraliste de l'Ugap serait un frein au développement d'une véritable expertise dans le numérique et à des démarches plus ambitieuses : « *Les achats informatiques requièrent des connaissances précises. L'Ugap accomplit son travail du mieux possible mais son périmètre d'intervention est trop large, qui va de l'informatique aux papiers peints, en passant par la flotte de véhicules, les vacances, etc. J'avais donc suggéré aux autorités qu'il pourrait être pertinent de disposer d'une centrale d'achat dédiée*. » (1)

### C. UNE DÉPENDANCE CULTURELLE FORGÉE DÈS L'ÉCOLE

La dépendance culturelle aux *hyperscalers* est aujourd'hui profondément ancrée chez l'ensemble des utilisateurs de services numériques. Comme le soulignait M. Étienne Gonnu, chargé de plaidoyer de l'April (2), des pratiques telles que les licences à prix cassés ou la vente forcée – par exemple l'installation automatique de Windows lors de l'acquisition d'un équipement informatique sans que le client l'ait demandé – ont abouti à « *restreindre l'imaginaire de l'informatique, pour la majeure partie de la population. Pour beaucoup de gens, c'est Microsoft, Google, Apple. Imaginer qu'une autre forme d'informatique n'est pas si simple, surtout quand on est captif de ces systèmes depuis l'école jusqu'à la vie active* » (3).

Microsoft met en œuvre une stratégie commerciale offensive pour pénétrer les établissements scolaires et favoriser une acculturation précoce à ses solutions. **Les élèves, les étudiants et les enseignants se voient ainsi offrir un accès à très bas coût à la suite Office 365, et même gratuit pour les fonctionnalités essentielle**s.

M. Alain Garnier a exprimé son indignation face à l'absence de réaction publique : « ***Nos enfants sont biberonnés aux outils Microsoft***. *Nous avons laissé cette situation s'installer car, à un moment donné, c'était financièrement intéressant. J'ai moi-même mené et perdu l'un de mes premiers combats en m'opposant à l'entrée de Microsoft dans les écoles. Au moment même où Microsoft a cherché à entrer dans les écoles, un autre géant américain, Coca-Cola, a voulu distribuer gratuitement des canettes dans les écoles. Cela a provoqué un tollé, et son projet a été rejeté. En revanche, faire entrer gratuitement les outils bureautiques de Microsoft pour nos enfants a été perçu comme une excellente chose.* » (4)

Le général Marc Boget confirme que cette « ***stratégie de lobbying extrêmement efficace dès le milieu scolaire*** » n'a rien d'anodin, mais vise à rendre extrêmement difficile toute transition future vers les logiciels libres, « *puisqu'une*

*(1) Audition de M. Henri Verdier, directeur général de l'Inria, le 10 mars 2026.*

*(2) Association française de promotion et de défense du logiciel libre.*

*(3) Table ronde sur le logiciel libre le 6 mai 2026.*

*(4) Audition du collectif #Fab8 le 29 avril 2026.*

*personne formée exclusivement sur ces outils dès son plus jeune âge cherchera naturellement à les retrouver dans sa vie professionnelle.* ***Cette habitude ancrée constitue un frein majeur au changement pour de nombreuses organisations*** » (1). Elle contribuerait à expliquer, selon lui, pourquoi l'ensemble des administrations ne franchissent pas le pas vers Linux.

Par un courrier aux recteurs en date du 28 février 2026, **le ministère de l'éducation nationale a réitéré la proscription de tout déploiement de suites collaboratives en ligne d'éditeurs non-européens dans les établissements scolaires**, en appelant à privilégier les espaces numériques de travail fournis par les collectivités. Le ministère n'est cependant pas en mesure de s'opposer à l'utilisation par les enseignants et les élèves de la suite Microsoft en dehors des établissements sur leur propre matériel.

En dehors des suites collaboratives, les solutions américaines demeurent très utilisées. 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 (2), 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.

**Au-delà des utilisateurs, l'adhérence culturelle serait particulièrement forte parmi les personnels des DSI.**

M. Nicolas Vivant, directeur de la stratégie et de la culture numériques de la commune d'Echirolles, a constaté que la véritable résistance au changement provient du service informatique : « *Le passage au logiciel libre implique en effet de nouveaux outils auxquels le service informatique doit s'adapter, et il n'en a pas toujours la compétence. Imaginez une équipe de dix personnes où une seule maîtrise Linux et toutes les autres travaillent sous Windows. Si vous arrivez et déclarez que Windows n'est plus la priorité et que l'on va désormais travailler sous Linux, un déséquilibre se crée. La personne auparavant marginalisée se trouve soudain valorisée, tandis que les autres membres du service se sentent en difficulté par rapport au projet. La résistance, et je ne l'ai pas observée uniquement dans ma commune car nous échangeons beaucoup entre communes, provient davantage du service informatique que des utilisateurs.* » (3)

Cette dépendance serait entretenue par la **mainmise des *hyperscalers* sur les offres de formation continue des DSI**, dans le public comme dans le privé. Selon

---

*(1) Audition commune de M. Tomasz Blanc et du général Marc Boget le 7 mai 2026.*

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

*(3) Table ronde sur le logiciel libre le 6 mai 2026.*

M. Henri Verdier, « *leur formation continue est assurée par quelques grands acteurs très installés sur le marché, si bien qu'ils ne connaissent même pas l'existence d'alternatives. Le principal enjeu consiste à reconquérir la capacité de produire et de raisonner de manière autonome, de chercher et d'expérimenter de nouvelles solutions. Cela suppose aussi de repenser les dispositifs de formation continue* » (1).

Enfin, dans un écosystème dominé par quelques solutions reconnues, il peut être difficile pour un directeur de systèmes d'information de faire un choix différent dont il faudra assumer seul la responsabilité en cas d'échec, comme l'a souligné M. Damien Lucas, directeur général de Scaleway : « *Il y a vingt ans, on disait «* **Nobody got fired for choosing IBM** ». ***Je pense qu'aujourd'hui, on pourrait appliquer cet adage en remplaçant IBM par AWS*** » (2).

### D. LA PLATEFORME DES DONNÉES DE SANTÉ : UNE DOUBLE ÉMANCIPATION DE MICROSOFT ET DES CABINETS DE CONSEIL

Le cas de l'hébergement de la Plateforme des données de santé (PDS), anciennement dénommée Health Data Hub, par Microsoft Azure est emblématique d'un écosystème qui favorise l'enfermement dans des solutions américaines.

#### *a. Le choix de Microsoft : « un vice de forme et de procédure »*

Créé par la loi du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé, dans la lignée du rapport de Cédric Villani en 2018 « Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne sur l'intelligence artificielle », le Health Data Hub avait vocation à réunir, organiser et mettre à disposition les données issues du système national des données de santé (SNDS) pour faciliter leur exploitation à des fins de recherche et d'innovation. Le principe était de « *permettre à des centaines, et (...) un jour à des milliers, d'acteurs d'accéder, selon des standards de sécurité très élevés à des espaces de travail élastiques, c'est-à-dire capables de s'adapter à leurs besoins pour traiter des volumes massifs de données intrinsèquement sensibles »* comme l'a expliqué la nouvelle directrice générale de la plateforme, Mme Hela Ghariani (3).

Malgré la grande sensibilité des données traitées, le ministère de la santé a fait le choix d'héberger la plateforme sur la solution de Microsoft Azure, arguant du fait qu'elle était la seule à présenter de manière intégrée les fonctionnalités et certifications de sécurité requises. L'étude de marché réalisée par la direction de la recherche, des études, de l'évaluation et des statistiques (Drees) en 2019, sur la base de consultations avec les acteurs industriels de référence, indiquait notamment le sous-dimensionnement des offres souveraines ainsi que l'absence de cartes graphiques, ou *graphics processing units* (GPU), nécessaires pour proposer aux

*(1) Audition de M. Henri Verdier, directeur général de l'Inria, le 10 mars 2026.*

*(2) Table ronde des fournisseurs de cloud, le 21 avril 2026.*

*(3) Audition de Mme Hela Ghariani le 29 avril 2026.*

chercheurs les traitements en intelligence artificielle [1]. Seul un petit nombre d'acteurs disposait alors de la qualification « Hébergeur de données de santé » (HDS), mise en place en 2018.

Le choix de Microsoft s'expliquerait également par la disponibilité immédiate de la solution par le biais de l'Ugap, ce qui devait permettre d'accélérer la création de la plateforme, identifiée comme l'une des priorités de la stratégie nationale pour l'intelligence artificielle. M. Henri Verdier, qui occupait les fonctions de directeur interministériel du numérique et du système d'information et de communication de l'État jusqu'en octobre 2018, considère que « *les personnes qui ont choisi l'unique solution référencée par l'Ugap ont agi ainsi pour gagner du temps et éviter la lourdeur des procédures de marché public : trois ans pour élaborer un appel d'offres, le notifier, le publier, analyser les candidatures et répondre aux éventuels contentieux* » [2].

**L'idée selon laquelle aucune offre souveraine n'aurait répondu aux besoins de la PDS a cependant été infirmée par des travaux de contrôle postérieurs**, qui ont démontré l'existence d'alternatives crédibles, pour certaines déployables dans des délais maîtrisés. La commission d'enquête sénatoriale sur la commande publique a noté que l'offre Santéos, certifiée HDS, remplissait les exigences en termes de sécurité et de performance, même si le déploiement aurait pris entre cinq et huit mois supplémentaires faute de véhicule contractuel adéquat. La Cour des comptes a pour sa part regretté que l'offre du Centre d'accès sécurisé aux données (CASD) n'ait pas été considérée davantage au motif qu'elle n'était pas encore arrivée au terme de la procédure de certification HDS, alors même qu'elle était déjà partiellement interfacée avec le SNDS ; qu'elle était autorisée par la Cnil à travailler sur des données sensibles depuis 2014 ; et qu'elle était mobilisable sans appel d'offres au titre d'un contrat public-public de coopération ou d'une quasi-régie conjointe. La capacité du CASD à répondre aux exigences de la PDS a été confirmée *a posteriori* par l'obtention de la qualification HDS en décembre 2019, quelques mois après la signature du contrat avec Microsoft Azure, puis par la reconnaissance de ses fonctionnalités élevées dans le cadre de l'étude réalisée par la PDS en 2023 pour le projet européen d'entrepôt multicentrique de données de santé (EMC2) [3].

Le manque de considération accordée à ces solutions révèle les limites de l'étude comparative conduite par la Drees pour conclure à l'absence d'alternative à Microsoft Azure. Les travaux de la commission d'enquête sénatoriale ont mis en évidence que les consultations réalisées auprès de l'écosystème « *n'ont en réalité consisté qu'en de simples échanges téléphoniques non préparés, et non à un processus transparent et complet de dialogue et d'information qui aurait permis*

---

*(1) Rapport fait au nom de la commission d'enquête sur les coûts et les modalités effectifs de la commande publique et la mesure de leur effet d'entraînement sur l'économie française, enregistré à la présidence du Sénat le 8 juillet 2025.*

*(2) Audition de M. Henri Verdier le 10 mars 2026.*

*(3) Cour des comptes, rapport sur les enjeux de souveraineté des systèmes d'information civils de l'État, délibéré le 11 septembre 2025.*

*d'obtenir un véritable panorama de l'ensemble des solutions disponibles sur le marché* ».

M. Michel Paulin, qui était alors directeur général d'OVH, abonde en ce sens : « *Il a été indiqué que les notes présentées à la ministre affirmaient qu'il n'y avait pas de solution alternative. Mais il n'y a eu ni appel d'offres, ni mise en concurrence. Quand il n'y a pas de critères factuels sur la souveraineté comme l'indice de résilience numérique, quand il n'y a pas de concours, comment peut-on certifier qu'il n'existe pas de solution alternative ?* » Aussi la PDS constitue-t-elle selon lui **« *l'exemple concret d'un vice de forme et de procédure qui a abouti à la conclusion qu'il n'y avait pas d'alternative, alors qu'en réalité, la solution avait déjà été choisie*** ». (1)

La commission d'enquête s'est interrogée sur le rôle qu'avait joué dans ce choix d'hébergement **le cabinet de conseil Capgemini, qui est intervenu en appui de la Drees dès la phase de préfiguration de la plateforme afin d'en définir les fonctionnalités cibles**.

Le directeur général de Capgemini, M. Aiman Ezzat, a reconnu que son cabinet avait exercé auprès du Health Data Hub « *une mission de conseil pour structurer le projet et les équipes* » (2). M. Laurent Vilboeuf, auditionné en tant que directeur par intérim de la PDS, a attesté avoir constaté une forte pénétration des cabinets de conseil, pour un coût estimé à 10 millions d'euros sur l'ensemble du processus : « *Ces cabinets ont fourni un appui à la conception et à l'organisation, sous les instructions de la PDS. Les consultants, essentiellement ceux de Capgemini, étaient intégrés aux équipes pour aider à la construction et au pilotage, à l'élaboration des tableaux de bord et à la préparation des réunions. Au début, les cabinets ont été fortement sollicités pour la construction de la plateforme elle-même, dépêchant sur place jusqu'à dix personnes par mois.* ». La circulation de documents issus du Health Data Hub présentant des sigles de Capgemini en base de page illustre, selon lui, le rôle de « *coproduction* » assumé par les consultants (3).

Si M. Ezzat atteste que « *les décisions sont toujours prises par les clients* », qui restent « *maîtres de leur choix en fonction de considérations non pas seulement techniques ou technologiques, mais aussi budgétaires, réglementaires ou législatives* », il ressort que la formalisation de certaines spécifications a directement contribué à orienter le choix technologique final, comme le démontrent les études de marché réalisées par la Drees pour la PDS. La rapporteure souligne qu'un tel rôle de coordination et de structuration du projet dépasse les limites du seul conseil, ou même de la coproduction, mais relève déjà de la prise de décision.

Or Capgemini était également prestataire du marché de référencement des offres d'informatique en nuage au sein de l'Ugap, parmi lesquelles était proposé

---

*(1) Audition de M. Michel Paulin, président du CSF « solutions numériques de confiance », le 7 avril 2026.*

*(2) Audition de M. Aiman Ezzat, directeur général de Capgemini, le 26 mars 2026.*

*(3) Audition de M. Laurent Vilboeuf le 17 mars 2026.*

Microsoft Azure, et avait conclu un partenariat stratégique avec Microsoft pour la formation de ses équipes aux outils de l'entreprise.

***b. Un échec sur tous les tableaux, de la protection des données à la performance***

**Le choix de confier l'hébergement à un acteur américain a suscité une vive inquiétude en raison des risques qu'il faisait peser sur la maîtrise des données de santé des citoyens**, risques qui avaient été largement occultés au cours de la procédure.

La Cnil a eu à se prononcer sur les modalités d'hébergement de la PDS dans le cadre de sa délibération du 20 avril 2020 [(1)]. Elle a relevé que les dispositions contractuelles conclues avec Microsoft permettaient que les données soient transférées vers les États-Unis pour y être stockées et traitées, ainsi que dans tout autre pays dans lequel le sous-traitant ou ses sous-traitants ultérieurs sont implantés. Compte tenu de la sensibilité des données traitées, et « *des éventuels risques matériels et juridiques en matière d'accès direct par les autorités de pays tiers* », **la Cnil a recommandé** « ***que la Plateforme des données de santé assure un hébergement et un traitement des données sur le territoire de l'Union européenne*** » **et, à plus long terme,** « ***que son hébergement et les services liés à sa gestion puissent être réservés à des entités relevant exclusivement des juridictions de l'Union européenne*** ».

Le Conseil d'État a également jugé, dans son ordonnance du 13 octobre 2020, que « *les mesures techniques mises en œuvre par Microsoft ou susceptibles de l'être à brève échéance n'écartent pas toute possibilité pour cette entreprise d'accéder aux données traitées sous la responsabilité de la Plateforme des données de santé, en dépit des précautions, limitant ce risque, qui entourent le chiffrement dont elles font l'objet et le stockage des clés de chiffrement utilisées* » et qu'« *il ne peut ainsi être totalement exclu, sur le plan technique, que Microsoft soit amenée à faire droit à une demande des autorités américaines fondée sur l'article 702 du FISA* ».

**Par l'adoption de l'article 31 de la loi Sren du 21 mai 2024, les législateurs ont voulu accélérer la migration de la Plateforme des données de santé vers une solution d'hébergement souveraine, en la soumettant explicitement à l'obligation de recourir à un cloud de confiance**.

Malgré ces multiples alertes, **l'immobilisme a perduré**. Pour la commission d'enquête sénatoriale, cela met en évidence « *les profondes contradictions de l'État qui, d'une part, n'a cessé d'étoffer sa doctrine sur la souveraineté numérique des données et, d'autre part, semble incapable de mettre en œuvre cet impératif crucial dans ses propres achats publics.* »

---

*(1) Délibération n° 2020-044 du 20 avril 2020 portant avis sur un projet d'arrêté complétant l'arrêté du 23 mars 2020 prescrivant les mesures d'organisation et de fonctionnement du système de santé nécessaires pour faire face à l'épidémie de covid-19 dans le cadre de l'état d'urgence sanitaire (demande d'avis n° 20006669)*

**La stratégie qui consistait à faire prévaloir la performance et la rapidité sur la souveraineté s'est elle-même révélée contre-productive, puisqu'elle a empêché le déploiement de la Plateforme des données de santé**, comme le relevait la Cour des comptes dans son rapport de septembre 2025 sur les systèmes d'information civils de l'État. Le choix de Microsoft a entraîné de nombreux recours juridiques et polémiques, qui ont retardé le projet. Puis, la position défavorable de la Cnil a empêché le transfert de la base principale du SNDS de la Cnam vers la PDS, « *laissant à la Cnam une charge administrative conséquente qui a entraîné un goulet d'étranglement au regard des sollicitations reçues* ». La conduite de chaque projet validé nécessite en effet que la Cnam réalise un travail d'extraction des données et de conventionnement avec les porteurs de projet.

### *c. La sortie de Microsoft, enfin concrétisée grâce à un pilotage réaffirmé*

Dans le prolongement du rapport de Jérôme Marchand-Arvier de 2023 « Fédérer les acteurs de l'écosystème pour libérer l'utilisation secondaire des données de santé », le gouvernement a prévu une **solution intercalaire**, à savoir la réplication de la base principale du SNDS sur une infrastructure reposant sur une technologie Oracle au sein de la PDS. Une procédure de mise en concurrence pour mettre en œuvre cette solution a été lancée le 1er juillet 2025.

**La ministre de la santé, Mme Stéphanie Rist, a finalement annoncé le 6 février 2026 mettre fin à l'appel d'offres pour engager directement la migration de la PDS vers la solution souveraine cible**.

**L'intervention de la Dinum a été décisive dans ce changement de stratégie**. Lorsque le projet de solution intercalaire lui a été soumis, de façon volontaire, par la PDS, elle a émis de très fortes réserves au regard de l'évolution des technologies. Comme l'a expliqué M. Laurent Vilboeuf, « *la Dinum a interpellé* [la PDS] *à propos des possibilités de l'informatique en nuage, et une analyse approfondie nous a permis de conclure qu'il était possible de procéder à une migration vers une solution cible dans des délais similaires et pour des coûts plus raisonnables* » (1).

**La 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.** Mme Hela Ghariani analyse l'aboutissement de ce processus comme « *la rencontre entre les besoins particulièrement exigeants* [de la PDS] *et la maturité de l'offre aujourd'hui disponible* » (2). Alors que la PDS a réalisé plusieurs études, en 2019, 2020, 2022, 2023 puis 2026, pour mesurer l'adéquation de ses exigences aux solutions existantes, Mme Ghariani a déclaré avoir observé, notamment entre 2023 et 2026, « *l'apparition de nouvelles offres sur le marché, mais aussi, au sein de ces offres, de nouvelles fonctionnalités* », notamment sur « *la*

*(1) Audition de M. Laurent Vilboeuf le 17 mars 2026.*

*(2) Audition de Mme Hela Ghariani le 29 avril 2026.*

*gestion des identités et des accès, les systèmes de gestion des clés et de chiffrement, ou encore la brique Kubernetes* », des options qui « *sont aujourd'hui disponibles et présentent des niveaux de service et de configuration qui nous permettent de mettre en œuvre notre stratégie de défense en profondeur ».* Les huit fournisseurs de cloud qui ont présenté une offre auraient eux-mêmes reconnu une évolution certaine de l'offre disponible.

**Cette décision atteste également d'un rééquilibrage des critères de choix, marqué par le refus de faire primer les considérations de performance et de délai sur les exigences de souveraineté**. Bien qu'aucune offre présentée n'ait satisfait l'intégralité des 350 exigences formalisées dans l'appel d'offres, la PDS a estimé qu'il serait possible de mettre en place avec le partenaire retenu des mesures de contournement raisonnables en termes de délai et de sécurité. Cette stratégie apparaît pleinement alignée avec les préconisations de la Cour des comptes, qui rappelait dans son rapport de septembre 2025 que « *le parfait exercice des missions de service public peut être garanti sans nécessairement aligner les spécifications des systèmes d'information sur le plus haut niveau technologique dès lors qu'un degré trop élevé de performance à court terme peut constituer un double écueil : par la mise en cause de la souveraineté sur les données et par une dépendance de l'administration vis-à-vis de la politique commerciale d'un éditeur dominant* ».

Dit autrement par M. Philippe Miltin, directeur général d'Outscale Dassault Systèmes : « *Si l'on parle de remplacer directement des hyperscalers qui génèrent plusieurs centaines de milliards en Europe, évidemment que non, nous ne pouvons pas le faire du jour au lendemain. Mais ce n'est absolument pas le sujet. Le sujet, aujourd'hui, est de savoir comment nous allons opérer des solutions critiques et des données sensibles pour l'ensemble des opérateurs et des clients.* » [(1)]

**L'expression des besoins, qui a pu être consultée par la rapporteure, témoigne d'une véritable exigence de résilience et de maîtrise des données**. Outre l'obligation faite aux prestataires privés de garantir la protection des données contre tout accès par des autorités publiques d'États tiers non autorisé par le droit de l'Union européenne ou d'un État membre, conformément à l'article 31 de la loi Sren, la PDS s'est attachée à évaluer leur résilience en cas de rupture de service, ou *kill switch.* Cette problématique de la dépendance technologique est particulièrement prégnante s'agissant des clouds dits hybrides, opérés par des prestataires européens mais reposant sur une technologie américaine, tels que Bleu et S3NS. Une série de questions complémentaires visait ainsi à vérifier la capacité des candidats à assurer le maintien en conditions opérationnelles et en bonnes conditions de sécurité de la plateforme en cas de retrait du support de la part d'un fournisseur ne relevant pas de la juridiction de l'Union européenne, à garantir que le support opérationnel soit uniquement soumis aux cadres juridiques européens, ou encore à limiter leur dépendance à des fournisseurs extra-européens.

*(1) Table ronde des fournisseurs de cloud le 21 avril 2026.*

Mme Hela Ghariani, directrice générale de la PDS, a indiqué que la construction des infrastructures nécessaires à l'hébergement de l'assurance maladie est prévue d'ici la fin de l'année 2026 ou le début de l'année 2027. La PDS devra, au préalable, être auditée par l'Anssi dans le cadre de la qualification Passi (prestataire d'audit de sécurité des systèmes d'information), et obtenir l'autorisation de la Cnil pour opérer la copie de la base principale du SNDS.

Selon les informations transmises par la PDS, **le coût de la migration devrait rester contenu**. L'essentiel des dépenses relèveront du développement de la nouvelle solution d'hébergement. La migration hors de Microsoft n'induira pas de coûts en tant que telle, dans la mesure où les services Azure sont commandés trimestriellement et facturés en fonction de l'usage réel. Il a également été assuré à la rapporteure que Microsoft ne détenait aucun droit de propriété sur les données, et que les codes, données et résultats produits ne seraient pas perdus lors de la migration vers une autre solution d'hébergement. Le contrat avec Microsoft, qui doit s'achever en octobre 2026, devrait néanmoins être prolongé pour permettre le maintien de l'infrastructure actuelle, sur laquelle 250 projets sont hébergés, pendant douze à dix-huit mois, le temps que la nouvelle infrastructure soit en mesure de les accueillir. Mme Gheriani a expliqué ainsi que « *le surcoût est donc plutôt lié à cette période de transition, durant laquelle nous opérerons deux plateformes simultanément* ».

Les échanges techniques avec le partenaire retenu étant toujours en cours, il est difficile de mesurer l'éventuel différentiel de coût pour le fonctionnement de la plateforme lié au changement d'infrastructure. Mme Ghariani a cependant assuré que l'offre de Scaleway faisait partie des moins onéreuses.

**La rapporteure observe que la concrétisation de la migration vers une offre souveraine coïncide avec une volonté revendiquée de réinternalisation des compétences pour recouvrer une pleine maîtrise de la décision et des choix technologiques sous-jacents**. Alors que Capgemini avait apporté un accompagnement sur le choix d'une solution intercalaire, le travail de sélection de la solution cible a été effectué par les seules équipes de la PDS, avec l'appui de l'écosystème public – Inria, Dinum et Délégation du numérique en santé. M. Laurent Vilboeuf a assuré que le recours aux consultants était désormais minime, avec un taux journalier de 0,6 personne [(1)]. Mme Gheriani a précisé que le projet de migration *« sera mené essentiellement par des équipes internes à la PDS* », sans recours à un intégrateur tiers. Deux experts de Scaleway interviendront néanmoins au sein des équipes de la PDS le temps du développement. [(2)]

*(1) Audition de M. Laurent Vilboeuf le 17 mars 2026.*

*(2) Audition de Mme Hela Ghariani le 29 avril 2026.*

## CHAPITRE 8 – LA POLITIQUE DU NUMÉRIQUE : LA GRANDE ABSENTE DES DÉBATS POLITIQUES

### A. UN ÉTAT DÉSARMÉ PAR L'EXTERNALISATION DES COMPÉTENCES NUMÉRIQUES

La dépendance aux solutions propriétaires dominantes est étroitement corrélée à la perte de compétences numériques des administrations. Faute de disposer des effectifs nécessaires, celles-ci sont parfois contraintes de se tourner vers des solutions déjà intégrées et d'externaliser leur maintenance, au risque de perdre la maîtrise de leur stratégie numérique.

La question des compétences est ainsi centrale pour M. Pierre-Yves Gosset, coordinateur des services numériques de Framasoft : « *Au cours des trente dernières années, l'État a externalisé les compétences de développement logiciel. La question se pose donc de savoir comment réinternaliser ces compétences pour que, lorsqu'une ville, une entreprise ou un ministère installe un logiciel libre, il y ait des personnes capables de « soulever le capot » et de comprendre comment il fonctionne. Le philosophe Bernard Stiegler parlait de « prolétarisation » : on nous a retiré le savoir sur le fonctionnement du logiciel. On nous parle de « cloud » comme si c'était dans les nuages, alors qu'il s'agit de quelque chose de très territorialisé et physique. Il va falloir reprendre la main sur la compréhension, les savoirs et les connaissances du fonctionnement du numérique si nous souhaitons que des collectivités, des entreprises et des administrations puissent basculer vers le libre.* » (1)

Alors même que l'externalisation excessive des compétences numériques de l'État et les risques associés sont bien documentés, les progrès demeurent très limités. Cela tient notamment à une gouvernance des ressources humaines numériques éclatée, sans véritable pilotage. Bien que rattachée au Premier ministre et au ministre de l'action et des comptes publics, « *la Dinum n'a pas autorité sur les DSI ministérielles,* comme le remarque Henri Verdier. *Sa mission consiste à animer un réseau interministériel. Elle peut édicter des cadres comme le référentiel général de sécurité ou celui relatif à l'accessibilité, mais elle n'intervient ni dans le recrutement ni dans la détermination des budgets*. » (2)

#### 1. Une répartition très inégale des ressources humaines numériques qui reflète des stratégies ministérielles fragmentées

**La commission d'enquête a constaté que les taux d'externalisation restent élevés, avec de fortes variations selon les ministères, traduisant l'absence de gouvernance unifiée des ressources humaines numériques.**

---

*(1) Table ronde sur le logiciel libre le 6 mai 2026.*

*(2) Audition de M. Henri Verdier, directeur général de la fondation Inria, ancien ambassadeur pour le numérique, le 10 mars 2026.*

La commission d'enquête s'est attachée à mesurer le niveau de dépendance aux prestations informatiques des administrations consultées en demandant à chacune de renseigner les effectifs de leur DSI et le nombre de prestataires auxquels elles avaient recours. Les chiffres ci-dessous doivent cependant être lus avec prudence, les ministères n'ayant pas tous retenu le même périmètre pour leurs ressources humaines et recourant à l'externalisation selon des modalités variées, de l'intégration de prestataires à temps plein au sein des équipes à l'externalisation complète de certaines missions à une entreprise de services numériques, alors évaluée en équivalents jours-homme. Si ces taux globaux offrent une première analyse, ils n'apportent pas la finesse nécessaire pour apprécier le niveau de dépendance sur certaines fonctions critiques ou un projet numérique donné.

Les taux d'externalisation des compétences renseignés par les DSI sollicitées varient dans une fourchette de 10 % à 70 %, et peuvent atteindre 80 % sur certaines fonctions. « *En interministériel, il a été admis qu'un taux dépassant 60 % devenait dangereux et qu'au-delà de 80 %, la situation n'était plus maîtrisable* », a indiqué Audran Le Baron, directeur du numérique pour l'éducation [(1)].

*(1) Table ronde réunissant M. Audran Le Baron, directeur du numérique pour l'éducation du ministère de l'éducation nationale, M. Mathieu Weill, directeur de la transformation numérique du ministère de l'intérieur, et M. Yves Billon, chef du service du numérique au secrétariat général des ministères économiques et financiers, le 9 avril 2026.*

**RESSOURCES HUMAINES NUMÉRIQUES DES ADMINISTRATIONS CONSULTÉES**

| | Agents (en équivalent temps plein ETP)) | Part de contractuels | Taux d'externalisation |
|---|---|---|---|
| **Ministères sociaux** | 173 | 74,9 % | 64 % (306 ETP) |
| **CISIRH** | 140 | 70 % | 46 % (117 ETP) |
| **AIFE** | 249 | 80 % | 71 % (614 prestataires) |
| **DGCCRF** | 73 | 75 % | 0 |
| **DGFiP** | 5 000 | 16 % | 40 %<br>37 % d'externalisation pour la fabrication logicielle (en jours homme) |
| **DGDDI** | 500 | 20 % | 10 % (60 ETP) |
| **Agriculture** | 201 | 60 % | 40 %<br>48 % dans le département plateformes, hébergement, infrastructures<br>52 % dans le département des applicatifs |
| **Culture** | 95 | 84 % | 56 % (120 ETP)<br>79 % de l'équipe « usine logicielle » |
| **Transition éco DNUM (hors fonctions de direction, de support et de stratégie)** | 236 | 17 % | 60 % (359 ETP) |
| **Éducation nationale** | 2 195 | 35 % (53 % en centrale et 23 % en déconcentré) | 17 % (36 % en centrale et 12 % en déconcentré) |
| **Intérieur** | 2 100 hors police et gendarmerie<br>700 à la DTNUM | | Non renseigné<br>332 prestataires présents sur site pour contribuer à la gestion des SI<br>70 % pour le MCO des data centers |
| **ANFSI** | 448 | 110 | 20 % (110 prestataires) |
| **Justice** | 900 à l'échelle du ministère | 88 % à la DNUM. | 63 % (1 500 ETP environ) |
| **MEAE** | 296 | 41 % | 56 % (379 prestataires à temps plein) |
| **APHP** | 595 | 84 % | 43 % (452 prestataires) |
| **Cnaf** | 883 | | 35 % (484 ETP) |
| **Cnav** | 1360 (1101 pour la gestion des SI nationaux et 259 pour la gestion des SI régionaux) | | Non renseigné (les marchés de prestations sont construits en unité d'œuvre, sans décompte du nombre de prestataires) |
| **Cnam (DDSI)** | 1 331 | | Non renseigné (les marchés de prestations sont construits en unité d'œuvre, sans décompte du nombre de prestataires) |
| **France Travail** | 1 724 | | 50 % (1 720 ETP) |

*Source : Assemblée nationale sur la base des réponses écrites des ministères.*

### *a. Une externalisation limitée au sein des ministères qui disposent d'une filière numérique dédiée*

**Le ministère de l'intérieur, la DGFIP et le ministère de l'éducation nationale peuvent s'appuyer sur des corps de fonctionnaires avec une spécialisation dans le numérique**. Pour M. Mathieu Weill, « *cette expertise constitue aujourd'hui un atout considérable pour ces organisations : le fait qu'elles disposent des compétences nécessaires en interne leur permet de maîtriser leurs dépendances.* » (1)

**L'internalisation des compétences est, en effet, au fondement de la stratégie de maîtrise des systèmes d'information de l'Anfsi**, comme l'a expliqué son directeur, le général Marc Boget : « *Mon premier principe est de ne jamais déléguer le pilotage de nos outils et si nous recourons ponctuellement à des prestataires extérieurs, c'est toujours sous la direction d'un noyau dur interne. Je dois être capable, à tout moment, de changer d'industriel sans fragiliser l'institution.* » (2). Dans ce but, la gendarmerie nationale a mis en place, il y a trente ans, une filière de gendarmes spécialisés en « systèmes d'information et de communication », qui lui permet de disposer des compétences rares nécessaires pour assurer en interne la gestion des postes de travail, l'architecture logicielle et le maintien en conditions opérationnelles de ses data centers. Le taux d'externalisation de l'Anfsi demeure ainsi limité à 20 %, avec 448 agents pour 110 prestataires (3).

Les gendarmes recrutés par cette voie spécialisée sont amenés à alterner au cours de leur carrière entre missions de terrain et fonctions techniques, selon un modèle de polyvalence qui « *permet à nos officiers et sous-officiers de concevoir des outils parfaitement adaptés aux réalités opérationnelles* », fait valoir le général Marc Boget. Ces possibilités de mobilité contribuent également à garantir l'attractivité de la filière : « *Un aspect fondamental de notre stratégie d'internalisation réside dans le refus d'une filière exclusivement numérique. Un ingénieur ne rejoindra pas la gendarmerie pour y exercer les mêmes missions que dans le secteur privé, où les rémunérations sont plus attractives. Ce qui motive ces personnels et garantit leur fidélité, c'est la perspective d'une carrière alternant des fonctions techniques et opérationnelles. Ce modèle, qui offre à la fois du sens et une visibilité sur la trajectoire professionnelle, est notre meilleur rempart contre la rotation des effectifs, alors même que ces profils sont très courtisés par le marché* » (4). L'ouverture du concours à une pluralité de profils, notamment

---

*(1) Table ronde réunissant M. Audran Le Baron, directeur du numérique pour l'éducation du ministère de l'Education nationale, M. Mathieu Weill, directeur de la transformation numérique du ministère de l'intérieur, et M. Yves Billon, chef du service du numérique au secrétariat général des ministères économiques et financiers, le 9 avril 2026.*

*(2) Audition commune de M. Tomasz Blanc, chef du service des systèmes d'information de la direction générale des finances publiques (DGFIP) et du général Marc Boget, directeur de l'agence du numérique des forces de sécurité intérieure (ANFSI), le 7 mai 2026.*

*(3) Réponses écrites de l'Anssi au questionnaire de la rapporteure.*

*(4) Audition commune de M. Tomasz Blanc, chef du service des systèmes d'information de la direction générale des finances publiques (DGFIP) et du général Marc Boget, directeur de l'agence du numérique des forces de sécurité intérieure (ANFSI), le 7 mai 2026.*

universitaires, et la réalisation de formations en partenariat avec de grandes écoles d'ingénieur visent à anticiper les besoins futurs.

**La DGFIP dispose d'un modèle similaire**. Sur 95 000 agents, la direction compte 5 000 informaticiens, ce qui lui permet d'opérer en interne ses systèmes d'information : des équipes dédiées prennent en charge l'ensemble des métiers – pilotage, fabrication, exploitation, sécurité, assistance –, les recours à des prestataires externes étant ciblés. Comme l'a exposé le chef du service des systèmes d'information M. Tomasz Blanc, ces moyens internes sont le résultat de la stratégie de priorisation du numérique adoptée par la DGFIP en 2020 qui l'a conduite à renforcer ses compétences numériques alors même que le nombre total d'agents baissait de façon significative. Cela a permis de maintenir le taux d'externalisation moyen à 40 %, bien au-dessous du seuil de risque de 60 %, même si Tomasz Blanc reconnaît que « *certains [des] projets dépassent localement cette limite* » (1).

La DGFIP recrute par la voie de concours spécialisés d'informaticiens des finances publiques, et a commencé depuis 2020 à s'ouvrir aux contractuels, même si leur part demeure limitée à 16 % des effectifs : « *cela a permis de diversifier nos profils tout en capitalisant sur l'attractivité de nos missions, sur notre culture du logiciel libre et sur la maîtrise de nos projets, des arguments forts face à la concurrence du secteur privé.* ».

### *b. D'autres ministères disposant d'une bonne maîtrise globale malgré des dépendances élevées sur certaines compétences critiques*

**La majeure partie des ministères ont adopté un modèle hybride, qui repose principalement sur des compétences internes, avec un recours à des prestations ciblées**. C'est notamment le cas du ministère de l'éducation nationale, qui, quoique bénéficiant lui aussi d'une filière numérique dédiée, fait appel à des prestations externes pour compenser des effectifs parfois trop limités. Le ministère de la transition écologique retient une approche similaire, en conservant la maîtrise interne du SI tout en externalisant certaines compétences spécialisées.

**Le taux d'externalisation demeure cependant élevé sur certaines compétences critiques, notamment le développement.** Si les effectifs informatiques du ministère de l'éducation nationale comptent environ 3 000 ETP, ils ne sont que de 400 ETP sur les fonctions de conception, de développement et d'intégration. Le directeur du numérique pour l'éducation a témoigné que « *sur certains projets nouveaux, la phase de développement a nécessité le renfort de forces vives de travail, ce qui s'est traduit essentiellement par un recours à des prestations extérieures, hors titre 2, au détriment de la maîtrise interne.* » (2)

---

*(1)* Ibid.

*(2) Table ronde réunissant M. Audran Le Baron, directeur du numérique pour l'éducation du ministère de l'Éducation nationale, M. Mathieu Weill, directeur de la transformation numérique du ministère de l'intérieur, et M. Yves Billon, chef du service du numérique au secrétariat général des ministères économiques et financiers, le 9 avril 2026.*

À cet égard, la situation favorable de la DGFIP fait figure d'exception au sein des ministères économiques et financiers. **L'AIFE ne dispose, sur 249 agents dédiés à la gestion des SI, que d'une dizaine de développeurs, ce qui la contraint à recourir à plus de 600 prestataires** pour les évolutions de ses différents produits. De même, les effectifs numériques du ministère de l'intérieur, hors police et gendarmerie, demeurent trop limités au regard du nombre de projets, comme l'a expliqué Mathieu Weil : « *Une DSI comme la mienne, qui est chargée de tout ce qui n'est pas police et gendarmerie, compte environ 700 emplois ; ils couvrent l'hébergement, le soutien de proximité, le développement, etc. Nous avons 150 à 200 projets en cours ; vous imaginez bien que le taux d'externalisation est donc très élevé pour la partie développement* » (1).

D'autres administrations ont engagé des efforts pour retrouver une maîtrise interne, comme le ministère de la culture avec la création en son sein d'une usine logicielle. Jusqu'en 2020, l'ensemble des développements était piloté et réalisé par des prestataires, faute de compétences internes. L'usine logicielle « *reste en grande partie constituée de prestataires externes (11 personnes sur 14, soit 79 % des ressources) »*.

Afin de réduire sa vulnérabilité et sa dépendance aux fournisseurs de solution, **l'AP-HP** a choisi de concentrer les développements internes sur des briques considérées comme critiques ou pour lesquelles des manques de solutions comparables sur le marché ont été identifiées. Elle *« investit fortement dans des briques d'interopérabilité (EAI/bus développé en propre, API management Gravitee, etc.), et une expertise sur le fond (standards européens règlement EHDS, HL7 FHIR, etc.) permettant de réduire sa dépendance vis-à-vis d'éditeurs métier (…). Elle réalise des développements en propre pour une partie réduite du parc applicatif (environ 20 %), car la stratégie de l'AP-HP reste celle de se baser sur des éditeurs, en assurant sa capacité, dans la mesure du possible, d'en changer (réversibilité, etc.). Le développement interne représente un métier assez lointain de celui l'AP-HP (qui assure déjà largement ceux d'accompagnement métier, d'intégrateur et d'hébergeur), mais s'avère parfois utile pour la réduction de la dépendance, ou pour palier des déficiences du marché »* (2). L'AP-HP fournit deux exemples dans lesquels le choix de développer des solutions en interne s'est révélé pertinent : le volet « congés » du SIRH, pour lequel les coûts sont moindres que pour une solution externe, et la création de solutions internes pour la gestion des données (EAI/ETL/Process bus) après un conflit avec le précédent fournisseur, de nationalité américaine.

Concernant la **Cnaf**, *« le cœur des applications métiers est effectivement développé en interne, que ce soit les services à destination des CAFs ou ceux à destination des allocataires et des partenaires. Dans un contexte de transformation*

---

*(1) Table ronde réunissant M. Audran Le Baron, directeur du numérique pour l'éducation du ministère de l'Education nationale, M. Mathieu Weill, directeur de la transformation numérique du ministère de l'intérieur, et M. Yves Billon, chef du service du numérique au secrétariat général des ministères économiques et financiers, le 9 avril 2026.*

*(2) Réponse aux questionnaires, AP-HP*

*numérique, la maîtrise des dépendances technologiques constitue un enjeu majeur pour la résilience, la sécurité et la souveraineté du système d'information (SI). La réduction des dépendances est au cœur de nos préoccupations, nous diversifions notre portefeuille de fournisseurs en gardant à l'esprit la maitrise des situations de dépendance excessive vis-à-vis d'un prestataire unique (*vendor lock-in*) »* (1). La majeure partie des applications de la **Cnam** est développée par des ressources internes accompagnées d'entreprises de services numériques. Le choix est similaire pour la **Cnav,** pour laquelle « l*es développements internes et la maintenance associée représentent 4 fois le coût des licences et logiciels sur étagère, hors poste de travail [102 millions contre 25,5 millions]. Que ce soit pour des développements propriétaires ou d'intégration d'applications métiers, ceux-ci sont réalisés par des ressources internes avec le cas échéant une extension de capacité à faire externe. Les ressources internes sont des profils d'analyse fonctionnelle pour la conception, et des concepteurs-développeurs pour la réalisation. Les ressources techniques sont celles validées et recensées au catalogue technologique de la Cnav* » (2).

### *c. Des ministères contraints d'externaliser toute la gestion de leur système d'information, faute de compétences internes*

**Les ministères sociaux et le ministère de la justice se trouvent dans une situation à risque, au-dessus du seuil de 60 % d'externalisation.**

Le **ministère de la justice** a souligné, dans ses réponses écrites, qu'il disposait d'effectifs numériques plus faibles que les autres ministères, – 0,8 % de ses personnels, contre 3,1 % en moyenne.

Faute de disposer des compétences internes nécessaires, le ministère a un recours important aux prestations intellectuelles informatiques, pour un coût autour de 200 millions d'euros par an, correspondant à 1 500 ETP, à comparer avec l'effectif numérique interne de 666 ETP du ministère, dont moins d'une vingtaine de développeurs. L'infogérance des SI métiers a été confiée à un prestataire français ; les SI liés à l'environnement de travail, hébergés sur site, font également l'objet d'infogérances spécialisées. **Jusqu'à récemment, le seuil d'externalisation pouvait atteindre 90 % sur certains projets, avec parfois même une fonction de chef de projet assurée par un prestataire**. S'il est depuis redescendu, grâce à la campagne interministérielle de réinternalisation des compétences numériques intervenue en 2024, il demeure au-dessus du seuil de 60 % recommandé.

La rapporteure souligne que le manque de compétence interne questionne la faisabilité des annonces faites par le ministre de la justice sur le choc numérique et le « zéro papier ».

La **direction du numérique des ministères sociaux ne compte que 173 ETP dédiés à la gestion des SI,** dont 75 % de contractuels. **Seulement 6 ETP sont consacrés au développement et à la maintenance évolutive des**

*(1) Réponse au questionnaire, Cnaf.*

*(2) Réponse au questionnaire, Cnav, Cnaf.*

**applications**. Il en résulte, là encore, une forte externalisation, tant de la gestion du SI qui est entièrement déléguée à des infogérances, que du développement des applications, **les développements internes ne représentant que 3 % du parc applicatif.** Dans sa réponse écrite, le ministère explique privilégier un fonctionnement « *basé sur le pilotage chefferie de projet, et plaçant les tâches de création-production de logiciel en dehors du champ des compétences internes ».*

### 2. Une perte de maîtrise qui favorise un enfermement dans des solutions extra-européennes

Le constat d'une externalisation excessive des ressources humaines numériques de l'État et des risques associés a été posé clairement en janvier 2023 par un rapport de l'Inspection générale des finances (IGF) et du Conseil général de l'économie (CGE) (1).

La mission relevait que **les dépenses de prestations informatiques avaient crû à un rythme moyen de 16 % par an entre 2017 et 2021** pour atteindre 1,5 milliard d'euros. Tout en notant que cette dynamique pouvait s'expliquer par les évolutions rapides du secteur du numérique (développement du cloud et de la gestion en mode produit), l'IGF et le CGE alertaient sur **l'absence de pilotage de cette externalisation croissante** et pointaient l'impact significatif sur les finances publiques, le **recours à un prestataire occasionnant un surcoût de 20 % par rapport au recrutement d'un agent public disposant des mêmes compétences**. La mission relevait qu'au-delà d'un certain niveau, l'externalisation induit même des « *risques d'insécurité, de perte de maîtrise sur les systèmes d'informations, et de dépendance à l'égard des prestataires* ». Or, en 2023, la moitié des grands projets numériques de l'État et trois ministères dépassaient le seuil de vigilance de 60 % d'externalisation fixé par la Dinum (2).

**Il ressort des travaux de la commission d'enquête que l'externalisation des compétences joue également un rôle déterminant dans la constitution de dépendances à des fournisseurs de logiciels extra-européens.**

De fait, le manque de compétences numériques des administrations contribue à expliquer leur choix de privilégier les solutions « packagées » proposées par les grandes entreprises numériques, plutôt que de déployer des solutions souveraines moins complètes dont elles devraient assurer elles-mêmes l'exploitation, l'intégration et le développement. « *Face au manque de compétences, notamment dans les organisations publiques, ces grandes sociétés ont compris qu'il fallait cesser de vendre le logiciel pour vendre des services, et que les organisations publiques paieraient pour que cela fonctionne* », relève Renaud Chaput, directeur technique de Mastodon (3).

---

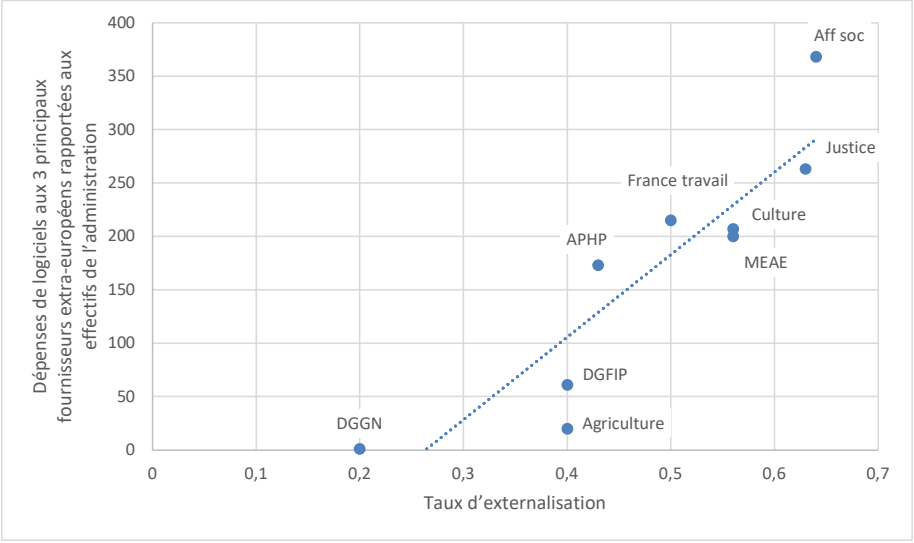
*(1) Rapport de l'Inspection générale des finances et du Conseil général de l'économie de l'industrie, de l'énergie et des technologies sur les ressources humaines de l'État dans le numérique, publié en janvier 2023.*

*(2)* Ibid.

*(3) Table ronde sur le logiciel libre le 6 mai 2026.*

Le croisement du taux d'externalisation de différentes administrations avec le budget qu'elles consacrent au paiement des licences des solutions états-uniennes dominantes du marché tend à montrer l'existence d'une **corrélation claire entre la perte de maîtrise interne d'une organisation et sa dépendance à des acteurs extra-européens**. Pour évaluer le niveau de dépendance de chaque administration aux solutions américaines, la commission d'enquête s'est fondée sur les dépenses moyennes licences versées aux cinq principaux fournisseurs extra-européens par agent, estimées à partir des réponses écrites et de l'effectif des entités [1].

**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.*

Cette relation est confirmée par le service numérique du ministère de la justice : « *Le ministère de la justice, ayant relativement peu de compétences informatiques internes au regard de sa taille, privilégie les solutions dont la gestion et le support nécessitent peu de compétences internes. Ce critère favorise parfois le choix de solutions d'éditeurs ayant un service intégré et performant, ce qui dans certains cas défavorise le recours à des solutions open source, même si elles sont utilisées dès que possible* » [2].

De même, **c'est le déficit de ressources internes qui aurait motivé le choix du ministère de l'éducation nationale de construire son cloud interne sur**

*(1) Plafond des autorisations d'emplois pour l'État en 2025 (article 144 de la loi de finances pour 2025).*

*(2) Réponses écrites du ministère de la justice au questionnaire de la rapporteure.*

**la solution de VMware, plutôt que sur des technologies libres**. Selon le directeur du numérique de l'éducation, VMware a permis au ministère « *d'opérer un cloud interne avec une économie de moyens humains considérable, les effectifs mobilisés étant sans commune mesure avec ceux qu'il faut employer pour faire fonctionner un cloud sur des technologies libres, comme le font la DGFIP ou le ministère de l'intérieur. Cela rejoint la question des compétences internes : c'est précisément parce que nous ne disposions pas des possibilités internes suffisantes, en nombre comme en expertise, que nous avons recouru à ces technologies.* » (1)

**L'État semble, de fait, s'être dessaisi des compétences de développement et de conception**. M. Henri Verdier décrit ainsi la « *culture, très répandue parmi les DSI, tant dans le secteur privé que dans le secteur public, qui consiste essentiellement à acheter des solutions plutôt qu'à savoir coder soi-même* », évoquant « *des DSI ministérielles comptant près de mille personnes, dont seulement deux développeurs* » (2). Selon M. Renaud Chaput, directeur technique de Mastodon, plus personne ne serait capable de « *soulever le capot* » pour savoir comment fonctionne concrètement un logiciel (3).

**L'externalisation des fonctions les plus critiques de maîtrise d'ouvrage, de direction de projet et d'architecture, compromet la capacité même des administrations à définir les orientations stratégiques de leurs systèmes d'information**. L'« *externalisation est devenue excessive, au point de nous placer parfois dans* ***une situation de dépendance où nous perdons jusqu'à la capacité de concevoir le basculement d'un projet vers un autre*** » (4), estime M. Mathieu Weill, directeur de la transformation numérique du ministère de l'intérieur. M. Henri Verdier a observé la même logique d'enfermement lorsqu'il était à la tête de la Dinsic (5) : « *Lorsque l'on évoque l'existence d'alternatives libres, plus sécurisées et moins coûteuses, à des solutions à 2 millions par an et concentrant une large part des attaques cyber, beaucoup ne disposent pas des compétences pour envisager un tel changement* » (6).

L'élaboration et la conduite d'un plan de sortie des dépendances nécessitent en effet de disposer d'agents publics en mesure de porter de tels projets : « *Ils ne peuvent se contenter d'être les intégrateurs de solutions venant des industriels ou les exécutants de projets conçus ailleurs. Il nous faut des architectes et des directeurs de projets, autant de fonctions critiques que l'État doit impérativement réinternaliser »,* a ainsi fait observer M. Mathieu Weill.

---

*(1) Table ronde réunissant M. Audran Le Baron, M. Mathieu Weill, et M. Yves Billon, le 9 avril 2026.*

*(2) Audition de M. Henri Verdier, directeur général de la fondation Inria, ancien ambassadeur pour le numérique, le 10 mars 2026.*

*(3) Table ronde sur le logiciel libre le 6 mai 2026.*

*(4)Table ronde réunissant M. Audran Le Baron, M. Mathieu Weill, et M. Yves Billon, le 9 avril 2026.*

*(5) Direction interministérielle du numérique et du système d'information et de communication de l'État, remplacée par la Dinum.*

*(6) Audition de M. Henri Verdier, directeur général de la fondation Inria, ancien ambassadeur pour le numérique, le 10 mars 2026.*

**Cette maîtrise interne est indispensable même lorsque l'administration décide de recourir aux solutions de marché, car elle engage l'efficacité et la qualité des achats publics**. Un tiers des cas de dérives de grands projets numériques de l'État s'explique par les ressources humaines, et « *en particulier, la difficulté à recruter le directeur de projet, l'absence de chef de produit interne pour arbitrer entre les besoins, le ratio insuffisant entre la maîtrise d'ouvrage interne et externe et l'absence d'architectes central* » [(1)]. M. Henri Verdier atteste que « *lorsqu'une organisation ne sait plus produire elle-même, elle ne sait plus acheter »,* assurant pouvoir citer des « *dizaines d'exemples de factures vingt fois trop chères, simplement parce que les achats avaient été réalisés à l'aveugle* » [(2)]. Cette conviction est partagée par la directrice interministérielle du numérique, qui a rappelé la nécessité de « *disposer des compétences nécessaires et de maîtriser les technologies clés en matière de numérique pour évaluer les choix effectués »* et se prémunir contre les risques de défaillance d'un prestataire [(3)].

De fait, **les administrations qui bénéficient d'importantes compétences internes, telles que la gendarmerie ou la DGFIP, sont celles qui ont mis en œuvre les stratégies les plus ambitieuses en matière de réduction des dépendances et de déploiement du logiciel libre**, comme exposé dans le premier chapitre.

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

La mission conduite par l'IGF et le CGE en 2023 concluait à l'impératif d'un **effort de réinternalisation des compétences numériques les plus critiques pour que l'État retrouve la maîtrise de son activité numérique**. Elle recommandait la **création de 3 500 postes supplémentaires d'ici 2028 sur le périmètre des ministères civils**, notamment en matière de direction des projets, de maîtrise d'ouvrage, de chefferie de produit et d'architecture.

Cette alerte a suscité une prise de conscience au sommet de l'État**. La constitution d'une filière numérique a été érigée au rang des priorités de la stratégie numérique de l'État** dans la feuille de route de 2023 de la Dinum. Elle a conduit celle-ci à endosser le rôle de « DRH du numérique de l'État » avec l'objectif de recruter et fidéliser des talents dans le numérique, dans un contexte de fortes tensions sur ces compétences rares.

**Par une circulaire du 13 février 2023, la Première ministre Elisabeth Borne a fixé des ratios pour encadrer le recours aux prestations intellectuelles informatiques** : « U*n grand projet dont le pilotage ou la réalisation est externalisé à plus de 60 % doit être considéré à risque, être suivi de manière plus approfondie*

*(1) Rapport IGF CGE sur les ressources humaines numériques de l'État, janvier 2023.*

*(2) Audition de M. Henri Verdier, directeur général de la fondation Inria, ancien ambassadeur pour le numérique, le 10 mars 2026.*

*(3) Audition de Mme Stéphanie Schaer, directrice interministérielle du numérique, le 14 avril 2026.*

*et faire l'objet d'un recrutement d'une équipe de direction expérimentée ; au-delà de 80 % d'externalisation, le projet ne peut pas démarrer dans des conditions de maîtrise satisfaisantes* ».

**Un premier programme interministériel de réinternalisation est intervenu en 2024, avec l'ouverture de 345 équivalents temps plein (ETP)** dans les lettres plafond du projet de loi de finances pour 2024. M. Audran Le Baron, directeur du numérique pour l'éducation, a salué « *une vague de réinternalisation de 60 ETP qui s'est avérée cruciale pour ramener les taux d'externalisation d'un certain nombre de nos projets à des niveaux soutenables* » (1).

Le ministère de la justice a bénéficié, dans ce cadre, de 40 ETP supplémentaires sur des fonctions rares ou de pilotage, qui lui ont permis de retrouver une certaine maîtrise. Plus aucun projet ne dépasse désormais le taux d'externalisation critique de 80 % et la maîtrise d'ouvrage est systématiquement internalisée. Le ministère demeure cependant toujours au-dessus du seuil de 60 % recommandé.

La loi d'orientation et de programmation du ministère de l'intérieur (Lopmi) du 24 janvier 2023 a prévu l'ouverture de 300 emplois numériques, incluant un volet cybersécurité et des postes en services déconcentrés, ainsi que 150 emplois supplémentaires fléchés vers l'Anfsi. Le directeur de la transformation numérique, M. Mathieu Weill, a indiqué que 100 postes avaient été créés à ce jour : « *Même si sa trajectoire a dû être révisée pour tenir compte des contingences budgétaires, le ministère de l'intérieur maintient un effort important pour réinternaliser les postes-clés du numérique. Une trentaine de créations de postes sont encore prévues en 2026 dans le cadre de cette réinternalisation, en dépit de différentes contraintes, notamment celles liées au plafonnement des emplois. C'est absolument indispensable si nous voulons maîtriser nos dépendances et réduire nos vulnérabilités*. » (2)

La vague de réinternalisation aurait permis de réaliser une **économie nette de 18,3 millions d'euros en 2025** selon la direction interministérielle du numérique (3).

**Ces efforts n'ont cependant pas été poursuivis les années suivantes, et demeurent bien en deçà de ce que préconisaient l'IGF et le CGE**. Ils n'ont, par ailleurs, pas été ciblés sur les ministères les plus vulnérables. Ainsi, les ministères sociaux n'ont vu leurs effectifs renforcés qu'à hauteur de 15 ETP, insuffisants pour permettre un véritable rattrapage.

**L'ensemble des DSI auditionnés ont ainsi souligné l'urgence de poursuivre la campagne de réinternalisation des compétences numériques engagée en 2024**. C'est notamment le cas de M. Audran Le Baron qui a déclaré

---

*(1) Table ronde réunissant M. Audran Le Baron, M. Mathieu Weill, et M. Yves Billon, le 9 avril 2026.*

*(2)* Ibid.

*(3) Rapport d'activité 2025 de la Direction interministérielle du numérique.*

« *milit[er], tant en interne qu'au niveau interministériel, pour obtenir des dispositifs de réinternalisation de compétences et donc la création d'ETP dans la filière numérique* » (1), faisant valoir que certains des systèmes cœur de métier du ministère présentent encore des faiblesses en matière d'externalisation.

**Cette exigence apparaît particulièrement essentielle pour les ministères les plus dépendants des prestations externes**. Ces derniers ont attesté, dans leurs réponses écrites, que leur capacité à mener à bien un plan de sortie des dépendances serait étroitement corrélée à des investissements dans les compétences, par le recrutement ou la formation. Les ministères sociaux appellent à un nouveau programme interministériel de réinternalisation des compétences, présenté comme la « *condition* sine qua non *de la reprise en main du pilotage de ces fonctions critiques pour l'exploitation du socle industriel* ». Le projet d'évoluer vers un modèle d'infogérance intégré, dont le pilotage serait repris par la Dinum, suppose en effet de réinternaliser quarante-cinq compétences. De même, il a été évalué que la sortie du cloud public Office 365 nécessiterait quinze ETP supplémentaires. Le ministère de la justice indique également conserver « *l'objectif d'élargir l'équipe de développement interne afin de mieux discriminer dans le recours aux équipes de maîtrise d'œuvre externes, ainsi que d'optimiser le fonctionnement de sa fonction numérique via une réorganisation en cours au secrétariat général* ».

En parallèle, plusieurs initiatives ont été déployées par la Dinum pour construire une filière du numérique attractive. Elle a ainsi mis en place le parcours interministériel numérique (Pinum) pour favoriser la mobilité entre administrations et renforcer l'attractivité des carrières. Sur le volet de la formation, elle anime le catalogue de formations interministérielles, via le Campus du numérique public qui a proposé des formations à 127 602 agents publics en 2025, dont 54 261 sur l'IA. Enfin, la Dinum a été chargée de refondre le référentiel de rémunération des métiers du numérique dans un souci d'attractivité, ce qui a constitué « *un progrès majeur pour recruter rapidement dans un secteur privé très concurrentiel* » selon le directeur de l'Anfsi (2).

La Cour des comptes estimait cependant, dans son rapport de 2024 sur le pilotage de la transformation numérique de l'État, que la gouvernance devait encore être renforcée, recommandant la création d'une instance, présidée par la directrice interministérielle du numérique et réunissant les ministères, pour suivre l'ensemble des chantiers liés à la filière RH du numérique et identifier finement les besoins en compétences numériques des ministères (3).

---

*(1) Table ronde réunissant M. Audran Le Baron, M. Mathieu Weill, et M. Yves Billon, le 9 avril 2026.*

*(2) Audition commune de M. Tomasz Blanc, chef du service des systèmes d'information de la direction générale des finances publiques (DGFIP) et du général Marc Boget, directeur de l'agence du numérique des forces de sécurité intérieure (ANFSI), le 7 mai 2026.*

*(3) Rapport de la Cour des comptes sur le pilotage de la transformation numérique de l'État par la direction interministérielle du numérique, délibéré le 8 avril 2024.*

## B. L'ÉBAUCHE D'UNE STRATÉGIE DE SOUVERAINETÉ NUMÉRIQUE, SANS VÉRITABLE PILOTAGE INTERMINISTÉRIEL

En mars 2023, la Dinum a été dotée d'une feuille de route tenant lieu de stratégie numérique de l'État, qui reconnaît explicitement la préservation de la souveraineté au rang des priorités de la transformation numérique. Elle dispose pour ce faire de trois principaux leviers d'action : un rôle de prescription visant à orienter les choix technologiques vers des solutions plus maîtrisées et diversifiées ; un rôle d'animation interministérielle, en favorisant le partage d'expérience et la coordination ; et le développement de briques technologiques mutualisées au niveau interministériel afin de proposer des alternatives souveraines.

**Cette stratégie se heurte néanmoins à une gouvernance numérique éclatée entre les différents ministères et à la faiblesse du positionnement institutionnel de la Dinum**. Placée sous l'autorité conjointe du Premier ministre et du ministre de l'action et des comptes publics, elle n'a pas d'autorité hiérarchique sur les directions du numérique, qui dépendent de chaque ministère et gèrent leur budget de manière autonome. Comme le confirme Mme Julia Mouzon, déléguée du comité stratégique de filière (CSF) logiciels et solutions numériques de confiance, « *la Dinum, ou même le Premier ministre lorsqu'il édicte des circulaires sur la commande publique, recommandent mais dans la plupart des cas, n'imposent pas. Sur toutes les questions de sécurité et d'alignement stratégique sur la souveraineté, il existe en réalité une pluralité d'objectifs et d'outils, où chacun va créer, utiliser et choisir ses propres solutions*. » « ***La Dinum propose et chaque ministère dispose*** », résume Michel Paulin, président du CSF [(1)].

### 1. Des exigences de souveraineté aisément contournées

#### *a. Un dispositif d'audit des grands projets numériques de l'État qui devrait permettre d'appliquer des critères de souveraineté*

**Le principal pouvoir de contrôle dont dispose la Dinum à l'égard des ministères repose sur la procédure d'audit des grands projets numériques de l'État**. Conformément à **l'article 3 du décret du 25 octobre 2019 relatif au système d'information et de communication de l'État et à la direction interministérielle du numérique**, les projets numériques interministériels et ministériels d'un montant prévisionnel supérieur à 9 millions d'euros doivent être soumis pour avis conforme au directeur interministériel du numérique. Avant d'émettre son avis, la Dinum consulte l'Anssi et la direction du budget sur les enjeux de cybersécurité et la soutenabilité financière du projet.

En tant que responsable des systèmes d'information de l'État, le Premier ministre conserve, en outre, « *une capacité d'audit* ab initio*, avec son bras armé qu'est la Dinum* » : il peut saisir la Dinum d'une demande d'évaluation sur tout projet ou système d'information des ministères et des organismes placés sous leur

*(1) Audition de M. Michel Paulin et de Mme Julia Mouzon, le 7 avril 2026.*

tutelle sur la base de l'article 4 du décret du 25 octobre 2019. Les ministères peuvent également solliciter un tel audit. Cette procédure est néanmoins peu mobilisée, avec moins de quatre saisines par an entre 2019 et 2023 selon la Cour des comptes (1).

**À l'origine, cet audit ne prenait pas directement en compte les enjeux de souveraineté**. « *Il s'agissait avant toute chose de s'assurer que, lorsqu'on investit dans un tel projet, il respecte son budget et son calendrier et qu'il finit par produire le service attendu* », après plusieurs dérives de grands projets numériques, a indiqué Stéphanie Schaer (2). Par la suite, **la circulaire du 5 juillet 2021 a intégré à la procédure d'avis conforme le contrôle de la doctrine Cloud au centre,** et notamment le respect des exigences de sécurité et d'immunité au droit extraterritorial pour l'hébergement des données sensibles de l'État.

**La Dinum s'est également emparée du dispositif pour essayer d'orienter l'architecture du projet afin d'éviter la constitution ou le renforcement de dépendances technologiques**, comme l'a expliqué la directrice interministérielle : « *Le droit de regard que nous avons sur les grands projets nous amène à discuter technique avec les équipes pour identifier certaines dépendances au niveau des choix d'architecture. Notre avis peut être favorable, mais avec des recommandations ou des réserves qui amènent les structures à revoir leur choix avant la passation du marché et l'engagement des crédits* » (3). Cela a conduit la direction à alerter les ministères sur les autres solutions techniques disponibles lorsqu'une dépendance était identifiée de longue date, par exemple à Oracle. La Dinum n'est cependant **pas en mesure de se prononcer sur le choix des attributaires des marchés**, puisqu'elle intervient en amont : « *nous agissons sur la façon dont le projet s'organise avec les métiers concernés, c'est-à-dire la structure d'achat, mais pas sur les acteurs en tant que tels, qui de toute façon ne sont pas encore connus* », précise Stéphanie Schaer (4).

***b. En pratique, un impact trop limité***

La procédure d'audit n'a pas pu être pleinement mise au service du renforcement de la souveraineté des systèmes d'information, en raison d'un périmètre trop restreint et de nombreuses possibilités de contournement.

En effet, jusqu'en mars 2026, **les projets des opérateurs de l'État échappaient à la procédure de l'avis conforme**, l'article 3 prévoyant uniquement la consultation du directeur interministériel du numérique pour l'émission de recommandations. Or, comme le notait la Cour des comptes, dans son rapport de 2024, « *une part croissante des grands projets numériques sont portés par les opérateurs* » et « *les ministères confient parfois aux opérateurs certains de leurs grands projets numériques, ce qui tend à brouiller la distinction entre les projets*

---

*(1) Rapport de la Cour des comptes sur le pilotage de la transformation numérique de l'État par la direction interministérielle du numérique, délibéré le 8 avril 2024.*

*(2) Audition de Mme Stéphanie Schaer, directrice interministérielle du numérique, le 14 avril 2026.*

*(3)* Ibid.

*(4)* Ibid.

*des ministères, soumis à l'avis conforme, et ceux des opérateurs, qui y échappent* » (1).

**En outre, l'obligation de saisir la Dinum est fréquemment contournée par les ministères.** La Cour des comptes regrettait déjà, en 2024, des « ***manquements persistants*** », certains ministères s'abstenant de soumettre leurs projets numériques, ou le faisant trop tardivement pour que la Dinum soit en mesure de se prononcer. Elle appelait à « *une réponse ferme et notamment une justification plus systématique des ministères sur les saisines tardives* » (2). La commission d'enquête n'a pas constaté d'amélioration : **sur les vingt-cinq procédures intervenues en 2024 et 2025, un quart n'ont pas pu donner lieu à un avis en raison d'une saisine trop tardive**. La rapporteure appelle le Premier ministre à marquer clairement son refus de tout contournement de la procédure.

**Le projet de refonte du système d'information de gestion des aides à l'emploi (SI Emploi) est emblématique des déficiences qui grèvent l'effectivité de la procédure.**

Ayant été confié par le ministère du travail à l'Agence de services et de paiement (ASP), le projet a d'abord été regardé comme relevant de la procédure d'avis simple applicable aux opérateurs. Constatant un taux d'externalisation de 96 % pour la maîtrise d'ouvrage et de 93 % pour la maîtrise d'œuvre, et le choix d'une offre de cloud commerciale non labellisée SecNumCloud malgré la sensibilité particulière des données hébergées, la Dinum a émis un premier avis défavorable le 9 juin 2022, sans effet contraignant sur la poursuite du projet. Elle recommandait un plan de recrutement ambitieux pour maintenir le taux d'externalisation en dessous de 80 % et pourvoir les fonctions clés en interne avant le démarrage du projet, ainsi qu'une mise en conformité de la stratégie d'hébergement avec la doctrine Cloud au centre.

Le SI Emploi ayant été requalifié en projet relevant du ministère du travail lors d'une réunion interministérielle du 13 février 2023, il a à nouveau été soumis à la Dinum, cette fois-ci au titre de la procédure d'avis conforme. La direction a réitéré son avis défavorable, le 12 juin 2024, en relevant une importante dérive des coûts et des compétences internes toujours insuffisantes pour assurer la maîtrise du projet – les fonctions clés de direction et d'architecture étaient encore assurées en externe, « *dépossédant de fait la puissance publique de sa capacité de pilotage du projet* ». Cela aurait dû, en principe, conduire à la suspension du projet tant que les conditions n'étaient pas réunies.

Le ministère a pourtant choisi de poursuivre les développements. Au moment de la troisième saisine, le projet avait consommé 31,9 millions d'euros, soit 72 % du budget total d'investissement. Dans un dernier avis rendu le 20 juillet 2025, la Dinum a acté que le niveau d'avancement du projet ne lui permettait plus de se

*(1) Rapport de la Cour des comptes sur le pilotage de la transformation numérique de l'État par la direction interministérielle du numérique, délibéré le 8 avril 2024*

*(2)* Ibid.

prononcer. Elle relevait néanmoins des progrès sur la maîtrise interne du projet, avec un taux d'externalisation redescendu à 70 %, la reprise de la majeure partie des fonctions clés, et le choix d'un hébergeur certifié SecNumCloud, tout en regrettant « *une stratégie d'hébergement qui procède par tâtonnements* ».

**La procédure d'avis conforme a également été contournée par le ministère de l'éducation nationale lors de la mise en œuvre du projet de modernisation de son système d'information de ressources humaines, baptisé Virtuo.**

Alors que la rapporteure s'étonnait qu'il ait été possible de choisir le prestataire américain Salesforce pour héberger les données sensibles des agents du ministère, malgré la non-conformité à la doctrine Cloud au centre, le directeur du numérique pour l'éducation a déclaré que cette décision avait été prise de façon concertée « *après une analyse au plus haut niveau* », le sujet ayant « *fait l'objet d'un avis de conformité de la Dinum au titre de l'article 3 du décret de 2019 et [ayant] été visé par la Cnil et l'Anssi* ». (1)

Or non seulement l'Anssi et la Cnil ont émis un avis négatif, mais la Dinum n'a pas non plus rendu d'avis conforme sur le projet Virtuo. Ayant été saisie seulement en mars 2024, alors que le projet était déjà finalisé et devait être déployé dans treize académies à partir du 2 avril 2024, la directrice interministérielle du numérique a estimé, dans son avis du 18 avril 2024, que la situation ne lui permettait plus de « *challenger les options prises* » et qu'en conséquence, « *ce projet Virtuo ne relève plus de la procédure d'avis préalable de la Dinum* ».

Si le ministère considère désormais que ses systèmes d'information de ressources humaines ne traitent pas de données d'une sensibilité particulière au sens de l'article 31 de la loi Sren et ne doivent donc pas être hébergés sur une offre SecNumCloud, **ce précédent démontre l'insuffisance de la procédure d'avis conforme pour assurer le respect par les ministères des exigences de protection des données sensibles**. La rapporteure constate l'absence de corde de rappel lorsque les ministères contournent délibérément l'avis de la Dinum.

Plus généralement, on peut s'étonner de la **latitude dont disposent les ministères pour apprécier la sensibilité de leurs données, dont dépend l'obligation de recourir à un cloud de confiance**. À titre de comparaison, le centre interministériel de services informatiques relatifs aux ressources humaines (CISIRH) des ministères économiques et financiers a retenu une tout autre approche, pour des données pourtant similaires : « *compte tenu des données à caractère personnel traitées dans les outils constituant l'offre de service du CISIRH, les éventuels besoins de technologie cloud s'appuient systématiquement sur le cadre SecNumCloud et sur les offres hébergées dans des data centers de l'État, notamment Nubo* ».

*(1) Table ronde réunissant M. Audran Le Baron, M. Mathieu Weill et M. Yves Billon le 9 avril 2026.*

### *c. Un récent renforcement du dispositif d'audit, qui conserve des angles morts*

**Par un décret et un arrêté du 18 mars 2026 (1), le Premier ministre a profondément remanié la procédure d'avis conforme afin de l'adapter aux nouvelles pratiques**. Le seuil à partir duquel un projet doit être soumis à la Dinum a été relevé à 15 millions d'euros, afin de l'ajuster à l'évolution du coût des projets numériques. Un **seuil spécifique de 2 millions a été introduit pour les commandes de suites collaboratives ou de logiciels à la demande ayant recours à un service commercial d'hébergement en nuage**. Cette mesure répond, selon Stéphanie Schaer, « *à la généralisation des solutions d'hébergement en nuage et témoigne de notre vigilance accrue quant à l'application de la circulaire cloud au centre mais aussi de l'article 31 de la loi visant à sécuriser et à réguler l'espace numérique* ».

**La prise en compte des enjeux de souveraineté par la Dinum lors de l'audit des projets numériques de l'État est pleinement confortée** par l'introduction de l'alinéa suivant à l'article 3 du décret de 2019 : « *L'examen du directeur interministériel du numérique permet de s'assurer que les conditions de réussite du projet sont réunies et que les référentiels introduits par voies législatives, réglementaires ou de circulaires sont appliqués, notamment en matière de sécurisation des données et d'hébergement, en cohérence avec les obligations de l'article 31 de la loi visant à sécuriser et à réguler l'espace numérique, ainsi qu'en matière de préservation de la maîtrise, de la pérennité et de l'indépendance des systèmes d'information et de communication concernés, en cohérence avec les obligations de l'article 16 de la loi du 7 octobre 2016 susvisée*. »

En parallèle, la Dinum a publié en février 2026 un **vade-mecum relatif à la sensibilité des données au sens de l'article 31 de la loi SREN afin de mieux accompagner les directions numériques et les acheteurs publics dans l'analyse de leurs données sensibles**. Il clarifie les critères permettant d'identifier les données d'une sensibilité particulière, à travers des exemples concrets. Parmi les systèmes d'information qui doivent obligatoirement être hébergés sur un cloud de confiance, figurent notamment : les SI contenant des données nécessaires à l'exercice des missions régaliennes de l'État, particulièrement au sein des services du Premier ministre, des ministères de l'intérieur, des armées, de la justice, de l'économie et des finances ou de l'Europe et des affaires étrangères ; les SI liés aux activités relevant de la sécurité nationale ou de la protection de la santé et de la vie des personnes (chaînes d'alertes sanitaires ou sur les dangers environnementaux, Samu…) ; les messageries et outils collaboratifs des administrations ; ou encore les SI relatifs à la paye des agents publics.

---

*(1) Décret n° 2026-193 du 18 mars 2026 modifiant le décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'État et à la direction interministérielle du numérique, et arrêté du 18 mars 2026 modifiant l'arrêté du 5 juin 2020 pris pour l'application de l'article 3 du décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique*

Malgré cette vigilance accrue, la Dinum a précisé par écrit qu'il n'est pas prévu *« de recensement centralisé et systématique à l'échelle interministérielle : celui-ci est réalisé au niveau de chaque ministère, en fonction de ses systèmes d'information et de ses missions ».* Elle ajoute que « *la responsabilité première repose sur les responsables de traitement qui sont en charge de qualifier les données et d'en apprécier la sensibilité via une analyse au cas par cas »* [(1)]. Il n'est donc pas certain que la Dinum soit en mesure de contester la qualification des données réalisée par le responsable du traitement dans le cadre du contrôle qu'elle exerce au titre de l'article 3 du décret du 25 octobre 2019.

### 2. Une mutualisation inachevée de solutions numériques souveraines

La stratégie numérique de l'État, élaborée en 2023, faisait du déploiement de produits numériques interministériels le principal levier de reprise en main des systèmes d'information de l'État, appelant à « *préserver la souveraineté numérique de l'État en investissant dans des outils numériques mutualisés* ». Il y est précisé que « *la Dinum s'engage dans la* ***structuration d'une offre en tant qu'opérateur de produits numériques interministériels mutualisés****, en visant à apporter aux départements ministériels une alternative concurrentielle, évolutive et ergonomique pour les outils de bureautique mais également des outils applicatifs comme les API. C'est un axe essentiel de souveraineté numérique de l'État. Il s'agit en outre pour l'État et dans le cadre d'une animation interministérielle, de* ***disposer de solutions cloud, adaptées aux besoins de l'administration*** ».

Cet effort de mutualisation se heurte néanmoins aux résistances des ministères et, malgré de premiers résultats intéressants, les produits interministériels doivent encore démontrer leur capacité à passer à l'échelle.

#### *a. Les clouds interministériels*

La doctrine Cloud au centre a entrepris de rationaliser les infrastructures d'hébergement cloud de l'État en concentrant les efforts sur les deux offres de services développées par le ministère de l'intérieur, le cloud Pi, et le ministère des finances, le cloud Nubo, qui ont vocation à couvrir les besoins de cloud interne de l'ensemble des ministères.

Elles sont notamment destinées à accueillir les systèmes d'information sensibles au sens de la doctrine, avec un niveau de sécurité équivalent aux offres commerciales certifiées SecNumCloud, comme l'a assuré M. Tomasz Blanc : « *lors des procédures d'homologation de notre cloud Nubo, nous intégrons les règles de sécurité technique de ce référentiel, auxquelles nous ajoutons les exigences de la politique de sécurité des systèmes d'information de l'État (PSSI-E). En matière de*

*(1) Réponses écrites de la Dinum au questionnaire de la rapporteure.*

*sécurité, le cloud Nubo se situe donc au même niveau, sinon au-delà, des offres SecNumCloud* » (1).

Les clouds Pi et Nubo disposent de capacités similaires, comptant chacun plus de 13 000 machines virtuelles, mais se distinguent par leurs choix technologiques : Pi repose sur un partenariat avec Red Hat, pour le déploiement de la solution OpenShift, quand le cloud Nubo est fondé sur le déploiement interne de solutions open source, en particulier OpenStack, opérées directement par la DGFIP. Le cloud Pi assure des astreintes sur les horaires non ouvrés, la disponibilité des SI vingt-quatre heures sur vingt-quatre permettant de répondre aux besoins de continuité de l'action publique. Pi est également seul à proposer un service de diffusion restreinte, en dehors du ministère des armées (2) .

La Cour des comptes relève cependant, dans son rapport sur les enjeux de souveraineté des systèmes d'information civils de l'État de septembre 2025, que les clouds interministériels « *restent peu utilisés, non seulement par les services des ministères qui les ont créés, mais aussi par les autres administrations* » (3).

La Dinum a reconnu que, si l'usage des clouds interministériels progressait en volume, il restait concentré sur les ministères porteurs, l'ouverture interministérielle demeurant limitée. La consommation sur Nubo a atteint 13,4 millions d'euros en 2024, avec 404 projets, soit quatre fois plus qu'en 2020, mais M. Tomasz Blanc concède qu'« *une importante marge de progression subsiste dans leur adoption généralisée* ». Nubo ne couvre encore qu'une part limitée des SI de l'État, même la DGFIP n'y hébergeant que 25 % de ses SI. L'ouverture interministérielle demeure également très limitée : la DGFIP représente 91 % de la consommation, les autres entités du ministère 5 % et la part interministérielle seulement 5 % – il s'agit essentiellement de la Dinum, pour ProConnect, et du système d'archivage opéré par le ministère de la culture (4).

Si selon la Dinum, la situation serait comparable pour le cloud Pi – l'utilisation interministérielle représenterait 5 % de la consommation –, selon le ministère de l'intérieur, 15 % de la capacité est aujourd'hui consommée par des services extérieurs au ministère (5).

Cette situation s'explique par les résistances de grandes administrations, qui « *ne peuvent ou ne veulent pas dépendre d'autres ministères et développent chacune leur propre cloud interne* » (6). En contradiction avec la doctrine Cloud au centre, le

---

*(1) Audition commune de M. Tomasz Blanc, chef du service des systèmes d'information de la direction générale des finances publiques (DGFIP) et du général Marc Boget, directeur de l'agence du numérique des forces de sécurité intérieure (ANFSI), le 7 mai 2026.*

*(2) Réponses écrites de la Dinum au questionnaire de la rapporteure.*

*(3) Rapport de la Cour des comptes sur les enjeux de souveraineté des systèmes d'information civils de l'État, délibéré le 11 septembre 2025.*

*(4) Réponses écrites de la Dinum au questionnaire de la rapporteure.*

*(5) Réponses écrites du ministère de l'intérieur au questionnaire de la rapporteure.*

*(6) Dinum, Bilan de la doctrine Cloud au centre, décembre 2025.*

ministère de l'éducation nationale, le ministère de la transition écologique ou le ministère de l'agriculture continuent ainsi d'investir dans le développement de leurs propres infrastructures cloud sur site, au lieu de s'engager dans la consolidation du cloud interministériel. La Dinum regrette, dans ses réponses écrites, des choix qui *« fragmentent les efforts, limitent les économies d'échelle et complexifient fortement la mise en place et l'exploitation de clouds robustes, dont la construction reste par nature complexe, coûteuse et exigeante en compétences ».* Elle rappelait, dans son bilan de 2025, que « *faire un cloud n'est pas à la portée d'un ministère individuellement, quelle que soit sa taille* ».

**Cette situation traduit l'absence de gouvernance interministérielle du cloud**. De fait, les feuilles de route des infrastructures d'hébergement sont arbitrées au niveau des directions du numérique de chaque ministère, ce qui permet *de facto* à certaines de s'écarter de la doctrine Cloud au centre. En parallèle, le pilotage des deux clouds interministériels Nubo et Pi reste à la main du ministère de l'intérieur et de la DGFIP, ce qui ne garantit pas la prise en compte des besoins des autres administrations utilisatrices. La Dinum anime des réunions trimestrielles associant les référents cloud de chaque ministère, qui se limitent à des échanges de bonnes pratiques, sans capacité décisionnelle.

**Le déploiement des clouds Nubo et Pi se heurterait également à une *« tarification interministérielle dissuasive* »**, selon la Cour des comptes [(1)].

**La tarification des offres Nubo et Pi a été fixée il y a près de dix ans, en 2017, par la Dinsic**, en prenant en compte les coûts de stockage, de mémoire vive et des processeurs. Elle avait retenu un tarif de 220 euros de façon à ce que chaque infrastructure soit rentabilisée à compter de 10 000 machines virtuelles. Il s'agissait d'offrir un tarif suffisamment compétitif par rapport aux offres commerciales, même si cela supposait, à l'époque, de vendre à perte faute d'avoir encore atteint la cible de capacité.

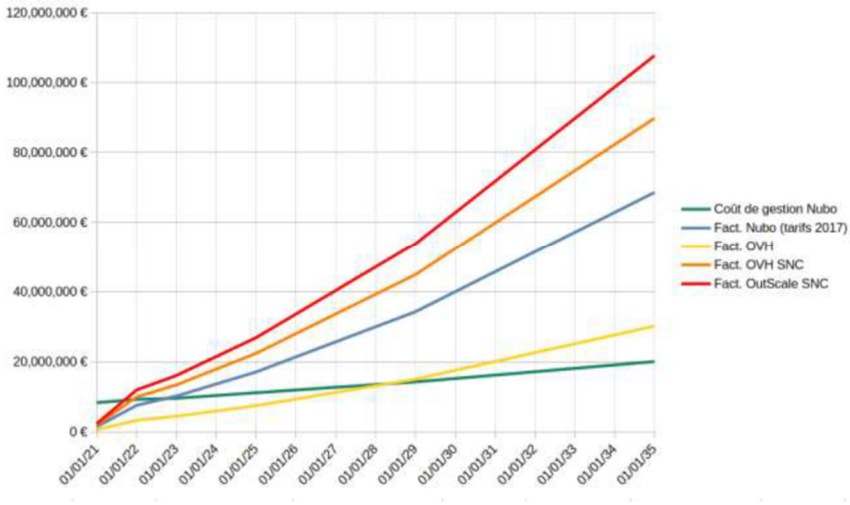
Sollicitée sur ce point, la direction de la transformation numérique du ministère de l'intérieur a fait valoir que « *la comparaison directe du coût du cloud d'État avec des solutions commerciales classiques est peu pertinente, en raison de l'impossibilité du secteur privé de proposer des offres à la hauteur des contraintes propres au ministère de l'Intérieur et aux autres ministères hébergés en termes de sécurité, de confidentialité et de résilience* ». Dès lors, « *l'objectif n'est pas de s'aligner avec les prix pratiqués par le secteur privé, mais de permettre l'entretien et la maintenance des sites, et de couvrir les dépenses d'investissement réalisées* ».

Pour autant, la consommation des clouds interministériels a largement dépassé le point d'équilibre défini en 2017, Nubo et Pi hébergeant chacun près de 20 000 machines virtuelles en 2026. Par conséquent, **la facturation est désormais nettement supérieure au coût de revient**, comme le souligne la Cour : « *pour 12 000 machines virtuelles, la facturation aux tarifs actuels serait*

*(1) Rapport de la Cour des comptes sur les enjeux de souveraineté des systèmes d'information civils de l'État, délibéré le 11 septembre 2025.*

*supérieure de 75 % au coût matériel et humain de leur exploitation. Pour 60 000 machines virtuelles, la facturation interministérielle représenterait un facteur multiplicatif de 5,4 par rapport au coût de revient* » (1). Pour autant, la tarification n'a toujours pas été révisée.

En 2025, la DGFIP a évalué le coût de revient complet de l'offre IaaS de Nubo pour le comparer au coût facturé aux utilisateurs, ainsi qu'aux tarifs des offres commerciales. Il en est ressorti que, même sans avoir revu le tarif pendant neuf ans, le cloud interministériel Nubo était toujours moins coûteux que les offres SecNumCloud proposées par Outscale et OVH, tout en offrant un niveau de sécurité et de performance similaire. Le coût facturé atteindrait cependant le double du coût de revient. La Dinum observe que « *cette analyse gagnerait à être actualisée en intégrant l'évolution des coûts d'acquisition du matériel, qui connaissent actuellement une forte hausse et devraient continuer à se dégrader dans le contexte géopolitique et technologique actuel notamment lié à l'IA et aux tensions internationales* » (2).




*Source : Dinum, d'après DGFIP.*

La rapporteure prend acte de la relance des travaux interministériels pour faire évoluer le modèle de facturation. Elle appelle à ce que les nouveaux tarifs reflètent mieux les coûts de revient, afin de favoriser l'engagement de toutes les administrations dans la mutualisation.

**Certains ministères consultés mettent également en avant des limites en matière de fonctionnalités.** L'une des DSI ministérielles regrette ainsi que « *les couches de services managés actuellement proposés ne couvrent pas l'ensemble des*

*(1)* Ibid.

*(2) Réponses écrites de la Dinum au questionnaire de la rapporteure.*

*besoins attendus pour des usages collaboratifs de grande ampleur, ce qui impliquerait des développements et des charges complémentaires* » tout en pointant des « *contraintes opérationnelles objectives* » qui exigeraient de mobiliser « *des capacités d'exploitation renforcées, notamment en termes de disponibilité humaine pour assurer le maintien en conditions opérationnelles, le support et l'intégration dans un système d'information complexe* ».

Si les clouds interministériels offrent des services comparables aux offres commerciales SecNumCloud, leur couverture fonctionnelle demeure en effet inférieure à celle des offres des *hyperscalers*. La Dinum a confirmé que des progrès sont nécessaires pour offrir des services de type PaaS, de bases de données managées, d'orchestration de conteneurs, ou de gestion fine des identités, accès et annuaires.

Pour y remédier, la feuille de route des deux clouds prévoit néanmoins des investissements dans le développement d'une offre PaaS et l'intégration de cartes graphiques GPU pour accompagner des services d'IA. Ces progrès devraient permettre de concrétiser les projets de migration de certains ministères, notamment l'hébergement des SI du ministère de la justice sur le cloud Pi. « *Ces travaux confirment que ces offres sont tout à fait utilisables par d'autres ministères, y compris dans un contexte d'attention très forte au cloisonnement des données* », selon la DSI du ministère de l'intérieur (1).

En parallèle, des travaux ont été engagés pour rapprocher les deux clouds interministériels, dans un objectif de résilience et d'économies d'échelle. La Cour des comptes recommandait de « *définir la trajectoire de convergence des clouds interministériels pour les rendre plus performants et augmenter significativement leur utilisation mutualisée par l'ensemble des ministères civils* » (2). La Dinum a confirmé à la commission d'enquête que les ministères travaillaient à renforcer l'interopérabilité et la réversibilité entre les différentes offres, afin de mutualiser certaines fonctions (astreintes, supervision) et de réduire les coûts.

### *b. Les produits numériques interministériels au défi d'une généralisation à l'ensemble de l'État*

D'autres produits numériques sont développés et opérés directement par la Dinum. Depuis 2019, elle gère, en partenariat avec des industriels français, le Réseau interministériel de l'État, un réseau unifié de communications électroniques qui interconnecte les services de l'État sur l'ensemble du territoire national et compte désormais un million d'usagers. Elle assure également le téléservice d'identification numérique FranceConnect ou la plateforme data.gouv.fr.

La feuille de route de 2023 a confié explicitement à la direction la mission de structurer une offre d'outils bureautiques qui pourraient constituer une

---

*(1) Réponses écrites du ministère de l'intérieur au questionnaire de la rapporteure.*

*(2) Rapport de la Cour des comptes sur les enjeux de souveraineté des systèmes d'information civils de l'État, délibéré le 11 septembre 2025.*

alternative concurrentielle aux logiciels propriétaires dominants et contribuer à l'indépendance des systèmes d'information de l'État.

C'est dans ce cadre que la Dinum a développé La Suite numérique, une suite d'outils numériques en open source destinée à constituer l'environnement de travail des agents publics. Elle comprend des services de messagerie instantanée (Tchap), de visioconférence (Visio), de transfert de fichiers de façon sécurisée (FranceTransfert), de messagerie électronique (Messagerie) et de stockage et partage de documents (Fichiers). S'y ajoutent des outils complémentaires, encore en cours d'expérimentation : un éditeur de texte collaboratif (Docs) et un tableur collaboratif (Grist). La Dinum propose également un service d'authentification professionnel (ProConnect) pour faciliter l'intégration des différentes solutions.

Si la Cour des comptes estimait, en 2024, que « *ces produits, peu connus, peu utilisés et dont le coût devrait continuer à augmenter, ne semblent pas à ce jour en mesure de concurrencer les offres proposées par le secteur privé, déjà largement adopté par les agents* » [(1)], ce constat ne semble plus avéré.

**Le déploiement des différents services de La Suite s'est accéléré au cours des deux dernières années.** Alors qu'en 2024, les nouveaux produits développés par la Dinum peinaient à trouver leur public, avec moins de 190 000 utilisateurs actifs sur Tchap, ils se sont depuis largement diffusés. Selon la Dinum, Tchap compte, en 2026, plus de 420 000 utilisateurs actifs mensuels (pour 800 000 comptes), Visio plus de 200 000 participants mensuels, quand France Connect rassemble 44 millions d'usagers [(2)].

**Les administrations sont, dans l'ensemble, satisfaites des produits interministériels développés par la Dinum**. Le ministère de la justice estime ainsi que « *le service fourni par les différents produits est de bonne qualité, et répond à un vrai besoin, tout en assurant un très bon niveau de souveraineté* ». Le ministère de la transition écologique témoigne qu'« *adossés à une charte graphique puissante, les produits de la Dinum ont indéniablement une surface et un rayonnement bien plus grands qu'il y a quelques années »,* leur qualité ayant « *conduit à une adoption rapide au sein du pôle interministériel, qu'il s'agisse du RIE, de Tchap, de Visio, de Grist etc. »* [(3)].

Les services de La Suite, en particulier, semblent correspondre aux attentes et pouvoir constituer de **véritables leviers de réduction des dépendances aux logiciels propriétaires américains**, d'après les réponses écrites des administrations. Le ministère de l'éducation nationale a salué des produits qui « *sont novateurs et bénéficient d'un important travail auprès de l'expérience utilisateur qui leur permet de rencontrer un beau succès* », tandis que la Cnam atteste que FranceTransfert, Tchap et Grist sont « *en parfaite adéquation avec les besoins des*

---

*(1) Rapport de la Cour des comptes sur le pilotage de la transformation numérique de l'État par la direction interministérielle du numérique, délibéré le 8 avril 2024.*

*(2) Réponses écrites de la Dinum au questionnaire de la rapporteure.*

*(3) Réponses écrites du ministère de la justice au questionnaire de la rapporteure.*

*agents du ministère* ». La gendarmerie nationale s'est emparée des briques Fichiers, Docs et Grist et considère qu'elles « *apportent une solution performante et sécurisée de collaboration avec des interlocuteurs internes et externes à l'administration ».* Pour la Cnam, « *Visio et Tchap répondent très bien à nos besoins en remplacement de Zoom actuellement déployé sur nos postes ».* Le ministère de l'agriculture dit également attendre beaucoup de l'outil Visio, qui pourrait se substituer à la solution américaine Webex. Les DSI des instituts de recherche auditionnés – Inrae, CEA, CNRS et Inserm – ont également annoncé avoir migré sur Visio, ou envisager de le faire, en remplacement de Teams ou de Zoom. La Suite pourrait également offrir une alternative à Office 365, étudiée notamment par les ministères sociaux.

**Le gouvernement accompagne désormais cette diffusion de façon volontariste**. Une première circulaire du Premier ministre, publiée le 25 juillet 2025, a appelé à **déployer Tchap** au sein de la sphère publique et des cabinets ministériels afin de garantir la sécurité et la confidentialité des communications électroniques des agents publics. Puis, une seconde circulaire du 28 janvier 2026 a acté la **généralisation de Visio** à l'ensemble des services de l'État, en remplacement des solutions de visioconférence extra-européennes. À l'occasion de la publication de la circulaire sur la doctrine de l'État pour les achats publics numériques, en février 2026, le gouvernement a confirmé la stratégie consistant à promouvoir, au sein des administrations, un usage exclusif du « cœur de suite », composé de Tchap, Visio et FranceTransfert. Ce choix répond, pour la directrice interministérielle du numérique, au « *besoin de maîtriser certaines fonctions essentielles à la continuité de l'État grâce à des outils présents dans tous les ministères, avec un service sans couture adapté aux environnements de gestion de crise* » (1).

**La réussite de cette migration suppose que la puissance publique démontre sa capacité à opérer le passage à l'échelle de ces outils numériques souverains, en garantissant leur fiabilité, leur performance et leur résilience sur le long terme.**

Les fonctionnalités de La Suite doivent encore être améliorées, pour couvrir l'ensemble des besoins des ministères et pouvoir ainsi se substituer totalement aux solutions propriétaires. À défaut, le risque est d'entraîner « *une dispersion des usages accompagnée d'une dispersion des données* », met en garde une DSI ministérielle. Par exemple, le déploiement de Visio est encore freiné par son incompatibilité avec les systèmes de visioconférence des salles de réunion, et aucune solution n'est encore proposée pour réaliser des diapositives. Ces limites sont néanmoins inhérentes à la stratégie adoptée par la Dinum : « *en appliquant des méthodes de type " lean start-up ", la Dinum privilégie dans un premier temps la recherche d'impact et d'adhésion des utilisateurs en remettant l'industrialisation et la complétude de la couverture des besoins à des phases ultérieures* », explique la direction du numérique du ministère de la justice.

*(1) Audition de Mme Stéphanie Schaer, directrice interministérielle du numérique, le 14 avril 2026.*

**Le déploiement de La Suite auprès de plus de deux millions d'agents publics implique une montée en charge importante, qui ne pourra réussir qu'avec des moyens humains et financiers adaptés.** Si le ministère de l'intérieur s'est distingué par une adoption rapide de plusieurs outils collaboratifs de la Dinum, concentrant 32 % des utilisateurs de Tchap en octobre 2025, il n'a pas encore pu déployer Visio et Docs en raison du manque de capacité de passage à l'échelle de ces solutions – par exemple, l'impossibilité d'organiser des réunions de plus de 1 000 participants, besoin essentiel pour le réseau des préfectures et services territoriaux. M. Baptiste Grigy, DSI du CEA, estime, à cet égard, qu'« *il faut que la puissance publique accompagne la Dinum pour qu'elle soit plus performante et qu'elle ait les moyens d'assurer un support pour le nombre d'utilisateurs ciblés.* » (1)

**Les ministères consultés ont tous souligné l'importance de définir une feuille de route à moyen ou long terme et de s'y tenir dans la durée**. L'industrialisation des produits et leur déploiement auprès de l'ensemble des agents, avec les efforts de conduite du changement que cela suppose, n'est possible qu'à la condition que la Dinum assure la fiabilité et la résilience de l'offre. Les ministères économiques et financiers insistent ainsi sur « *la nécessité d'une projection plus lointaine de la stratégie, avec des choix d'outils mutualisés pérennes car s'il est sans doute facile de faire preuve d'agilité au niveau interministériel pour suivre les évolutions très rapides du secteur du numérique, en revanche, au niveau ministériel ou directionnel, le déploiement des outils et l'accompagnement des utilisateurs nécessitent des délais incompressibles pour en permettre la bonne appropriation.* » (2)

**La politique d'outillage conduite par la Dinum a en effet pu manquer de continuité par le passé**. Les incidences de l'abandon de la plateforme collaborative Osmose au profit de Resana, acté en mars 2024, n'ont pas pu être correctement anticipées par les ministères qui l'avaient déployée – la plateforme comptait 48 000 utilisateurs en 2023. De même, après avoir soutenu le déploiement interministériel de la messagerie collaborative de l'État, développée par le ministère de la transition écologique à partir de briques open source, la Dinum a changé de stratégie. Le ministère de l'intérieur, qui avait choisi de s'appuyer sur cette solution, s'est trouvé en difficulté du fait de ce désengagement, comme en a témoigné son directeur de la transformation numérique : « *Nous pensions que nous allions nous inscrire dans une dynamique interministérielle. Puis, les priorités ont changé. Le ministère de la transition écologique a continué à nous soutenir mais, tout à coup, la Dinsic, la Dinum ont cessé de participer et d'autres projets ont été lancés – ils parlent, aujourd'hui, d'un autre système de messagerie. Nous étions pourtant engagés sur la voie de cette transition. J'estime que nos équipes ont perdu entre un an et demi et deux ans du fait du changement de stratégie. Il s'agissait de remplacer une messagerie obsolète, ce qui constituait une véritable préoccupation, tant au*

*(1) Table ronde de directeurs des systèmes d'information d'organismes de recherche le 1er avril 2026.*

*(2) Réponses écrites des ministères économiques et financiers au questionnaire de la rapporteure.*

*regard de l'expérience des agents et de l'attractivité qu'en matière de sécurité et de vulnérabilités*. » (1)

**La mise en place du Club de La Suite a permis de renforcer le mode de gouvernance et de consolider le financement, en y associant pleinement les ministères**. Les membres du club s'engagent à contribuer financièrement au développement des différentes briques de La Suite, par le versement d'une participation qui varie par paliers en fonction de leur taille ; en contrepartie, ils ont le droit de participer à la définition de la feuille de route – ce qui leur permet de voir leurs besoins spécifiques pris en compte –, et de recevoir un appui privilégié des équipes de la Dinum dans le déploiement de la solution. Les ministères sociaux se sont ainsi acquittés d'un droit d'entrée de 100 000 euros pour intégrer le club d'utilisateurs et « *renforcer [leur] légitimité à intervenir sur la priorisation des travaux à conduire sur les différents outils de La Suite.* » (2)

**Certains ministères proposent également des solutions avec une ambition interministérielle, qu'il convient de soutenir et de valoriser**. C'est notamment le cas du service d'archivage électronique VaS opéré par le ministère de la culture, ou du service de Parapheur proposé par le ministère de la transition écologique. Stéphanie Schaer a annoncé, lors de son audition, que la Dinum travaillait à l'élaboration d'un catalogue des communs numériques existants susceptibles d'être utilisés à large échelle par différents ministères.

Pour renforcer le pilotage interministériel du socle technologique de l'État, le Premier ministre a annoncé, le 30 avril 2026, la **création de l'Ariane, l'Autorité du numérique et de l'intelligence artificielle de l'État**, pour remplacer la Dinum. La nouvelle autorité sera notamment chargée de définir les standards communs, de piloter les infrastructures numériques stratégiques, de coordonner les grands partenariats technologiques de l'État, et de veiller à la maîtrise des dépenses numériques. Les annonces gouvernementales sur cette nouvelle organisation ont néanmoins été marquées par une certaine confusion : alors que le Premier ministre avait initialement évoqué une fusion de la Dinum et de la direction interministérielle de la transformation publique (DITP), il semblerait finalement que la DITP conservera son autonomie et assurera la prise en charge de la transformation numérique des démarches et des processus administratifs. Interrogé par la rapporteure sur les nouveaux leviers dont bénéficierait l'Ariane pour faire respecter la doctrine numérique de l'État, le ministre David Amiel n'a pas apporté de réponse précise. Il a renvoyé à la mission de préfiguration qui a été confiée à l'ingénieur général de l'armement Walter Arnaud.

*(1) Table ronde réunissant des directeurs de systèmes d'information le 9 avril 2026.*

*(2) Réponses écrites des ministères sociaux au questionnaire de la rapporteure.*

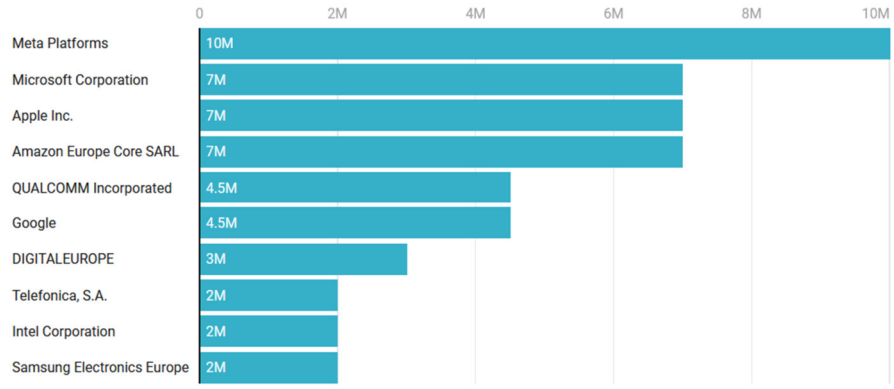
## CHAPITRE 9 – LE LOBBYING : GRÂCE À DES MOYENS MASSIFS, LE COMBAT EN PASSE D'ÊTRE GAGNÉ POUR L'ABOLITION DE LA RÉGULATION

### A. UN LOBBYING FÉROCE

La puissance du lobbying des grandes entreprises numériques extra-européennes a été soulignée de façon récurrente par les personnes auditionnées.

**Les Big Tech déploient des moyens humains et financiers considérables au service de leur stratégie d'influence**. Sur la base du registre européen de transparence, les ONG *Corporate Europe Observatory* et *LobbyControl* ont montré qu'en 2025, les dix entreprises de la tech qui dépensaient étaient à l'origine de 49 millions d'euros de dépenses de lobbying auprès des institutions européennes, dont **35 millions pour les seuls Gafam** (1). À titre de comparaison, les dix entreprises qui ont dépensé le plus en lobbying dans les secteurs de la pharmacie, de la finance et de l'automobile n'atteignent que 42 millions. Ces montants ne cessent de croître, marquant une hausse de 50 % entre 2021 et 2025.

**TOP 10 DES ENTREPRISES DE LA TECH QUI DÉPENSENT LE PLUS EN LOBBYING AUPRÈS DES INSTITUTIONS EUROPÉENNES**




*Source : Corporate Europe Observatory et LobbyControl, octobre 2025*

Ces entreprises peuvent s'appuyer sur un **réseau dense de 210 lobbyistes** pour relayer leurs messages, dont 85 disposent d'un badge qui leur offre un accès illimité au Parlement européen (2).

---

*(1)* Corporate Europe Observatory *et* LobbyControl, « *Les budgets de lobbying des Big Tech dépassent des records* », 29 octobre 2025.

*(2) Registre de transparence de l'Union européenne, à la date du 18 juin 2026*

**NOMBRE DE LOBBYISTES DÉCLARÉS PAR LES GRANDES ENTREPRISES NUMÉRIQUES EXTRA-EUROPÉENNES AUPRÈS DES INSTITUTIONS EUROPÉENNES**

| | Nombre de lobbyistes | dont accrédités pour accéder au Parlement européen |
|---|---|---|
| **Google** | 29 | 17 |
| **Apple** | 28 | 9 |
| **Meta** | 44 | 8 |
| **Amazon** | 55 | 12 |
| **Microsoft** | 15 | 9 |
| **DigitalEurope** | 39 | 30 |
| **Total** | 210 | 85 |

*Source : commission d'enquête, à partir du registre de transparence de l'Union européenne, à la date du 18 juin 2026.*

**Le registre de transparence, qui retrace les rencontres des responsables de l'exécutif européen avec des représentants d'intérêt, reflète leur omniprésence à Bruxelles** : en 2025, **Google a été reçu par la Commission à 53 reprises, Microsoft à 57, Amazon à 70, Meta à 41, et Apple à 44,** et DigitalEurope, le lobby qui représente les grandes entreprises de la tech dont les hyperscalers, a obtenu 40 rendez-vous [(1)]. Cela représente, au total, **plus d'une réunion par jour ouvré**. Le Parlement européen est, lui aussi, régulièrement sollicité, les trois *hyperscalers* ayant déclaré 171 rencontres en 2025.

M. Yann Lechelle a pu éprouver la force d'influence de ces entreprises alors qu'il s'efforçait d'alerter les autorités européennes sur leurs pratiques anticoncurrentielles : « *Mon interlocuteur a trouvé mes éléments très intéressants, mais il m'a conseillé de revenir souvent, car* ***les deux cents rendez-vous avant moi et les deux cents après moi étaient occupés par des représentants de ces mêmes entreprises****. De fait, leur capacité de déploiement pour protéger leurs intérêts, aussi légale soit-elle, leur confère* ***un pouvoir de distorsion absolue du discours***. » [(2)]

M. Renaud Chaput a également regretté que les acteurs du logiciel libre ne soient pas plus souvent consultés par la Commission : « *À Bruxelles, on m'a récemment parlé d'un règlement en cours de discussion, le Digital Fairness Act. Pour préparer ce texte, la Commission a auditionné Meta plus de soixante fois afin de recueillir son avis sur la pertinence de cette législation européenne visant l'interopérabilité et le contrôle des algorithmes. À ma connaissance, aucune association de logiciels libres n'a été conviée à la table à ce moment-là. Je ne pense pas que mes collègues ici présents disposent d'un lobbyiste à temps plein à Bruxelles*. » M. Pierre-Yves Gosset confirme cette asymétrie de moyens entre un logiciel libre, qui n'a que peu de porte-parole, et un lobbying des éditeurs de logiciels propriétaires extrêmement puissant : « *nous jouons à armes totalement inégales »* [(3)].

*(1) Registre de transparence de l'Union européenne, à la date du 18 juin 2026*

*(2) Audition du collectif Eurostack le 26 mars 2026.*

*(3) Table ronde sur le logiciel libre le 6 mai 2026.*

Le lobbying des firmes états-uniennes s'exerce également auprès du gouvernement et des parlementaires français. Selon l'étude que leur a consacrée la Haute autorité pour la transparence de la vie publique (HATVP), Google, Microsoft, Meta, Apple et Amazon ont déposé, entre 2020 et 2024, **533 fiches d'activités** témoignant des actions d'influence qu'elles ont entreprises, directement ou par des intermédiaires, auprès des autorités françaises (1).

Ces initiatives visent, en majorité, à contrecarrer la régulation du secteur du numérique. La HATVP relève que les Gafam ont été particulièrement actifs lors de la transposition du DSA et du DMA par la loi Sren de 2024, afin de dissuader les législateurs français d'introduire des contraintes supplémentaires. Google, Microsoft, Amazon et Facebook ont sollicité directement l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom), l'Autorité de la concurrence ou l'Arcep. *Corporate Europe Observatory* et *Lobby Control* observent une intensification du lobbying en faveur du détricotage des réglementations européennes au tournant de l'année 2025, renforcée par la « *nouvelle tendance à la déréglementation qui souffle à Bruxelles* » depuis la publication du rapport Draghi et par le soutien que leur apporte le président Trump (2).

Les géants du numérique peuvent compter sur le soutien complet de l'administration fédérale dans cette entreprise. C'est ainsi au lobbying et aux menaces des États-Unis que M. Henri d'Agrain, attribue l'échec des négociations européennes visant à intégrer des exigences d'immunité aux lois extraterritoriales dans la certification européenne pour les services cloud EUCS :

« *Jusqu'à la mi-2023, le schéma EUCS comprenait un niveau renforcé, dit High +, intégrant des critères d'immunité face aux législations extraterritoriales. Le 25 mai 2023, les principales associations représentant les entreprises technologiques américaines, notamment la Computer and Communications Industry Association (CCIA) et la Business Software Alliance (BSA), ont adressé un courrier à l'administration Biden pour exprimer leur opposition à ce dispositif européen, qu'elles considéraient comme une menace potentielle pour la sécurité nationale américaine. En septembre 2023, le secrétaire d'État américain Antony Blinken a adressé une note diplomatique à la Commission et aux chancelleries européennes, indiquant que l'adoption de l'EUCS en l'état pourrait engendrer des conséquences sur les relations économiques et sécuritaires transatlantiques.*

« *À l'automne 2023, la Commission européenne décide alors de renvoyer le schéma à l'Agence européenne de cybersécurité (Aesri). Lorsqu'il réapparaît en mars 2024, il est expurgé de l'ensemble des critères d'immunité aux législations extraterritoriales. À l'été 2024, la Commission justifie cette décision par une analyse de son service juridique, soutenant qu'un schéma de certification fondé sur le Cyber Security Act ne pourrait contenir que des critères dits « techniques », c'est-à-dire technologiques.*

---

*(1) HATVP, « La représentation des intérêts des GAFAM depuis 2020, 3 avril 2025.*

*(2)* Corporate Europe Observatory *et* LobbyControl, « Les budgets de lobbying des Big Tech dépassent des records », 29 octobre 2025.

« *C'est ainsi qu'a émergé dans le CSA 2 une distinction artificielle entre risques techniques et risques non techniques, distinction qui, du point de vue des utilisateurs, n'a aucun sens. Qu'un risque soit qualifié de technique ou non, dès lors qu'il affecte la confidentialité, l'intégrité ou la disponibilité des données et des traitements associés, il constitue un risque de sécurité numérique.*

« *En Allemagne, cette évolution s'est traduite par un revirement politique rapide. Les conséquences économiques potentielles, notamment pour l'industrie automobile très exposée au marché américain, ont pesé lourdement. Pourtant, le 30 octobre 2023, un communiqué trilatéral entre la France, l'Italie et l'Allemagne affirmait encore la volonté de travailler à un schéma européen de certification de sécurité intégrant des critères d'immunité extraterritoriale. Un mois plus tard, la position allemande avait changé.*

« *À cela se sont ajoutées les réticences d'autres États, tels que les Pays-Bas, exprimant la crainte de restrictions d'accès au marché américain et aux garanties de sécurité américaines. Ce faisceau de pressions et de lobbying a finalement conduit à l'abandon des critères d'immunité dans le schéma européen de certification. Telle est, en tout cas, l'analyse que j'en fais, au regard des éléments dont nous disposons*. » (1)

Grâce à leur pénétration des cercles juridiques, les Big Tech sont également en mesure d'orienter l'interprétation des règles de droit dans un sens qui leur est favorable. « *Dans l'univers de la protection de la vie privée, le simple fait de connaître la loi et de vouloir la faire appliquer suffit pour être considéré comme un activiste, car 99 % des personnes qui travaillent dans ce domaine sont employées par l'industrie. La plupart des professeurs, par exemple, sont liés par divers contrats à des entreprises du secteur – pas tous, mais la plupart*, explique M. Max Schrems. *En Allemagne et en Autriche, et peut-être dans une moindre mesure en France, la littérature juridique revêt une grande importance : les tribunaux la consultent et la suivent. Or cette littérature est presque toujours rédigée par des avocats d'entreprises. Si une décision a plusieurs interprétations possibles, les ouvrages juridiques mettront en avant, dans la plupart des juridictions, une interprétation très favorable à l'industrie.* » (2)

En parallèle, elles s'appliqueraient à cultiver l'idée qu'elles seraient incontournables et à décourager l'émergence d'alternatives, comme le souligne Mme Cristina Caffara, représentante du collectif Eurostack : « *À un certain niveau, l'administration européenne manque de courage et d'inspiration, et le message de la peur porté par ces acteurs au nom des entreprises américaines s'avère efficace. Le récit qu'ils diffusent est le suivant : il serait extrêmement risqué pour l'Europe de se découpler des États-Unis. (…) Ce récit est largement diffusé et provient directement de l'industrie. Une entreprise mondiale qui vend massivement aux États-Unis ne souhaite évidemment pas être associée à un mouvement perçu comme*

*(1) Audition de M. Henri d'Agrain, délégué général du Cigref, le 30 avril 2026.*

*(2) Audition de M. Max Schrems, le 26 mars 2026.*

*défavorable par les Américains. Lorsqu'une entreprise européenne, qui devrait être un champion pour l'Europe, relaie ce discours, c'est extrêmement dangereux pour l'Europe, on risque de reculer*. » (1)

Ces discours infusent jusqu'à agir sur les cadres conceptuels des responsables économiques, administratifs et politiques. M. Henri Verdier évoque ainsi les *« visiteurs du soir »* qui « *peuvent influencer les manières de raisonner* ». À la demande de la rapporteure, il précise : « *dès qu'une grande entreprise française emploie plusieurs centaines de milliers de salariés et demande à la diplomatie française et au réseau des services économiques de soutenir son effort d'exportation, elle parle aux politiques.* ».

Le lobbying des grandes plateformes extra-européennes et de leurs relais pourrait être contrecarré en veillant, sur la base du registre européen de transparence, à ce que la Commission européenne garantisse la représentativité des acteurs consultés : un seuil minimum de rendez-vous seraient réservés aux petites et moyennes entreprises et aux organisations associatives et, à l'inverse, le nombre d'interactions directes ou indirectes avec les plus grandes entreprises serait limité.

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

### B. L'OMNIBUS NUMÉRIQUE : UN RECUL DE LA RÉGULATION EUROPÉENNE QUI DONNE SATISFACTION AUX BIG TECH

La Commission européenne a présenté, le 19 novembre 2025, un paquet législatif visant à modifier le droit européen sur les données et le règlement sur l'intelligence artificielle. Il s'inscrit dans l'agenda de simplification porté par la Commission à la suite du rapport Draghi, avec l'objectif revendiqué de supprimer les lourdeurs administratives qui entravent la croissance et l'innovation en Europe. Les discussions sur le volet de l'intelligence artificielle étant déjà très avancées (2), les travaux de la commission d'enquête se sont concentrés sur la proposition de règlement dit omnibus numérique (3), qui inclut notamment des modifications importantes du RGPD de 2016.

---

*(1) Audition du collectif Eurostack représenté par Mme Cristina Caffarra, économiste, spécialiste de la concurrence et de la régulation des plateformes numériques et M. Yann Lechelle, entrepreneur, président-directeur général de probabl.ai, le 26 mars 2026.*

*(2) Proposition de règlement du Parlement européen et du Conseil modifiant les règlements (UE) 2024/1689 et (UE) 2018/1139 en ce qui concerne la simplification de la mise en œuvre des règles harmonisées concernant l'intelligence artificielle, présenté par la Commission européenne le 19 novembre 2025 (COM[2025] 836 final)*

*(3) Proposition de règlement du Parlement européen et du Conseil modifiant les règlements (UE) 2016/679 (UE) 2018/1724, (UE) 2018/1725 et (UE) 2023/2854 ainsi que les directives 2002/58/CE, (UE) 2022/2555 et (UE) 2022/2557 en ce qui concerne la simplification du cadre législatif numérique, et abrogeant les règlements (UE) 2018/1807, (UE) 2019/1150 et (UE) 2022/868 ainsi que la directive (UE) 2019/1024, présenté par la Commission européenne le 19 novembre 2025 (COM[2025] 837 final).*

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

Alors qu'il est indiqué dans l'exposé des motifs de l'omnibus numérique que « *le présent règlement propose une série de modifications ciblées du règlement (UE) 2016/679 à des fins de clarification et de simplification, tout en préservant le même niveau de protection des données* », il ressort des travaux de la commission d'enquête que les amendements proposés vont bien au-delà de la simplification, remettant en cause l'équilibre même du RGPD. Selon M. Pierrick Clément, avocat pour la Ligue des droits de l'homme, « *la simplification, en tant que mécanisme juridique, consiste à faciliter l'application des normes par une clarification des définitions, une harmonisation des procédures ou une réduction des redondances. En revanche, redéfinir des concepts juridiques et étendre les dérogations aux garanties fondamentales ne relève pas de la simplification, mais bien d'un choix de dérégulation, qui traduit une décision politique*. »

Dans l'avis conjoint qu'ils ont adopté sur la proposition omnibus le 10 février 2026, **le CEPD et le Contrôleur européen de la protection des données ont souligné que** « ***certaines modifications proposées suscitent d'importantes préoccupations****, car elles peuvent avoir une incidence négative sur le niveau de protection dont bénéficient les personnes, créer une insécurité juridique et rendre plus difficile l'application de la législation en matière de protection des données* » [(1)].

#### *a. Une grave entaille à la définition des données personnelles*

**L'omnibus numérique vise à modifier la définition même des données à caractère personnel, afin d'en exclure les données pseudonymisées**. Alors que l'article 4, paragraphe 1, du RGPD dispose que toute information qui se rapporte à une personne physique identifiée ou identifiable constitue une donnée à caractère personnel, il est proposé d'ajouter le paragraphe suivant : « *Les informations relatives à une personne physique ne sont pas nécessairement des données à caractère personnel pour toute autre personne ou entité du simple fait qu'une autre entité peut identifier cette personne physique. Les informations ne revêtent pas de caractère personnel pour une entité donnée lorsque ladite entité ne peut identifier la personne physique à laquelle elles se rapportent, compte tenu des moyens raisonnablement susceptibles d'être utilisés par cette entité. Ces informations ne se muent pas en informations à caractère personnel pour cette entité du simple fait qu'un destinataire ultérieur éventuel dispose de moyens raisonnablement susceptibles d'être utilisés pour identifier la personne physique à laquelle les informations se rapportent*. » [(2)]

---

*(1) Avis conjoint du Comité européen de la protection des données et du Contrôleur européen de la protection des données sur la proposition de règlement omnibus numérique, adopté le 10 février 2026.*

*(2) Article 3, paragraphe 1, a) de la proposition de règlement « omnibus numérique », présenté par la Commission le 19 novembre 2025 (COM(2025) 837 final).*

**La Commission européenne prétend qu'il s'agit d'une simple codification de l'arrêt SRB de la CJUE** [(1)], comme l'a assuré M. Yvo Volman, directeur des données à la direction générale des réseaux de communication, du contenu et des technologies, au président et à la rapporteure à l'occasion de leur déplacement à Bruxelles.

L'arrêt SRB a, de fait, marqué une inflexion dans l'approche retenue par la CJUE pour apprécier le caractère personnel des données. Alors que la jurisprudence de la Cour avait jusqu'ici tendu à assimiler les données pseudonymisées à des données personnelles, cette décision a établi pour la première fois que des données pseudonymisées pouvaient être considérées comme non personnelles pour le destinataire, s'il ne peut avoir accès aux informations identifiantes, ni transmettre les données à un tiers capable de le faire. Le paragraphe 86 du dispositif précise que « *des données pseudonymisées ne doivent pas être considérées comme constituant, en toute hypothèse et pour toute personne, des données à caractère personnel aux fins de l'application du règlement 2018/1725, dans la mesure où la pseudonymisation peut, selon les circonstances de l'espèce, effectivement empêcher des personnes autres que le responsable du traitement d'identifier la personne concernée de telle manière que, pour elles, celle-ci n'est pas ou n'est plus identifiable* ». En l'espèce, le comité de régulation unique (SRB) avait transmis à l'entreprise Deloitte, sous forme pseudonymisée, des commentaires communiqués par ses clients sur sa dernière résolution afin de les faire analyser. Alors que les clients se plaignaient de ne pas en avoir été informés, la Cour a estimé que le destinataire, Deloitte, n'avait aucun moyen, légal ou pratique, de réidentifier les individus, et que les données ne devaient donc pas être considérées comme personnelles.

La Cour rappelle néanmoins plus haut qu'elle a jugé, dans des arrêts antérieurs, que des données en soi impersonnelles devaient être regardées comme personnelles, dès lors que le responsable du traitement disposait de voies légales pour obtenir auprès d'autrui des informations supplémentaires permettant de l'identifier [(2)], ou si elles pouvaient faire l'objet d'un transfert ultérieur à des tiers et qu'il n'est pas exclu que ces tiers seront raisonnablement en mesure d'identifier la personne concernée [(3)].

**La modification proposée par la Commission européenne va donc bien au-delà de la jurisprudence de la Cour**. Comme l'a exposé M. Max Schrems, « *dans l'arrêt SRB, la CJUE a pris le soin de reprendre explicitement tous les arrêts précédents et d'affirmer très clairement qu'elle ne modifiait pas son raisonnement juridique ; elle ne l'aurait pas fait si elle n'avait pas voulu signifier qu'elle s'en tenait à sa ligne habituelle. En l'occurrence, l'affaire portait sur le cas très spécifique de l'entreprise Deloitte, qui, pendant deux mois, avait recueilli des données partiellement anonymisées, ou pseudonymisées. **La Commission***

---

*(1) Arrêt de la Cour de justice de l'Union européenne du 4 septembre 2025,* EDPS c. SRB *(affaire C-413/23).*

*(2) Arrêt IAB Europe du 7 mars 2024.*

*(3) Arrêt du 9 novembre 2023, Gesamtverband Autoteile-Handel*,

***européenne et la majeure partie du secteur juridique ont extrait un ou deux demi-paragraphes du jugement pour en déduire que la définition des données personnelles avait soudain changé.*** *Le respect dû à la CJUE imposerait pourtant de lire l'intégralité de la décision et de restituer fidèlement ce qu'elle voulait dire. On peut concevoir que, dans le cas où un destinataire unique reçoit, pendant une période limitée, des données dont on peut raisonnablement considérer qu'elles ne peuvent pas être rattachées à une personne identifiée, ces données ne sont pas des données personnelles au sens où la Cour l'entend. Mais c'est très différent de ce que la Commission européenne entend introduire dans le paquet omnibus numérique pour modifier le premier alinéa de l'article 4 du RGPD – puisque, je le répète, on pourrait conclure de cette modification que les données des utilisateurs exploitées pour la publicité en ligne ne seront plus protégées en tant que données personnelles*. » (1)

**La présidente de la Cnil, Mme Marie-Laure Denis, considère également que la Commission européenne a « *surtransposé* » l'arrêt SRB. Le risque d'affaiblissement de la protection des données personnelles qui en résulterait constitue le principal point de vigilance de l'autorité sur l'omnibus numérique** : « *La proposition de la Commission tend à brouiller cette distinction, en introduisant une dose de relativisme, et sans en encadrer l'usage. Désormais, une donnée susceptible d'être rattachée à une personne pourrait être considérée comme anonyme, et donc être exclue du champ du RGPD, s'il apparaît que celui qui la détient « ne dispose pas de moyens pouvant raisonnablement être utilisés » pour établir le lien entre les données et la personne. Par opportunisme, ou, tout simplement, faute d'avoir compris des règles qui ne sont pas si simples****, les responsables de traitement de données risquent de traiter des données à caractère personnel comme des données anonymes, donc de ne pas soumettre leur traitement au RGPD.*** *Ils s'exposeront à des sanctions si nous ne partageons pas leur appréciation. Surtout, ils priveront les utilisateurs des garanties nécessaires, alors mêmes que leurs données sont susceptibles d'être transmises à des tiers, y compris des tiers étrangers*. » (2)

Dans leur avis conjoint, les autorités européennes de protection des données font également valoir des préoccupations majeures. Elles « *invitent instamment les colégislateurs à ne pas adopter les modifications proposées à la définition des données à caractère personnel, étant donné qu'elles vont bien au-delà d'une modification ciblée ou technique du RGPD. En outre, elles ne reflètent pas exactement et vont clairement au-delà de la jurisprudence de la CJUE, et elles aboutiraient à une réduction significative de la notion de données à caractère personnel* » (3).

---

*(1) Audition de Mme Marie-Laure Denis, présidente de la Cnil, le 15 avril 2026.*

*(2) Audition de M. Max Schrems, fondateur de l'association Noyb, le 26 mars 2026.*

*(3) Avis conjoint du Comité européen de la protection des données et du Contrôleur européen de la protection des données sur la proposition de règlement omnibus numérique, adopté le 10 février 2026.*

M. Julien Rossi confirme le **risque que l'exclusion des données pseudonymisées du champ des données personnelles empêche de prendre en compte des situations pourtant sensibles** : « *cette redéfinition pourrait conduire à ignorer des jeux de données qui, bien que ne comportant ni le nom de la personne, ni son adresse, ni son numéro de téléphone, ni son adresse IP, restent hautement révélateurs. Prenons l'exemple de données composées uniquement de points de géolocalisation horodatés. Si l'on sait qu'une personne passe 90 % de ses nuits dans un lieu donné, 90 % de ses horaires ouvrés dans un autre lieu donné, et une part significative de ses dimanches matin, ou de ses vendredis, dans un lieu de culte précis, il devient relativement aisé de reconstituer un fichier d'individus classés par religion. Dans ce cas, il ne s'agit formellement que de données pseudonymes, puisque le nom de la personne n'apparaît pas. Néanmoins, un tel jeu de données peut faire courir un risque réel, y compris physique, aux personnes concernées, notamment dans des contextes de tensions religieuses. C'est pour cette raison que certains collègues, en particulier Szilvia Lestyán, évoquent le phénomène d'« anonymity washing », ou blanchiment par l'anonymisation, afin de souligner que des données présentées comme anonymes ou pseudonymes peuvent malgré tout faire courir un risque aux personnes concernées*. » (1)

### *b. Une fragilisation des droits d'accès, d'information, d'opposition et d'effacement*

La Commission propose d'inscrire dans le règlement une **définition très extensive de la recherche scientifique** comme « *toute recherche pouvant également soutenir l'innovation, dont le développement technologique et la démonstration. Ces travaux contribuent aux connaissances scientifiques existantes ou appliquent les connaissances existantes de manière inédite, ont pour objet de contribuer à l'accroissement des connaissances et du bien-être généraux de la société et respectent les normes éthiques dans le domaine de recherche concerné. Cela n'exclut pas que la recherche puisse également viser à promouvoir un intérêt commercial.* » (2).

**Cela aurait pour conséquence d'étendre les possibilités de déroger aux droits des personnes sur leurs données**. La recherche scientifique bénéficie en effet d'un certain nombre d'exceptions : elle peut justifier le traitement de données personnelles sensibles ; elle dispense de l'obligation de fournir des informations quand les données personnelles n'ont pas été collectées auprès de la personne concernée et que cela exige des efforts disproportionnés ; elle permet de limiter le droit des personnes à s'opposer au traitement de leurs données personnelles, à y accéder, ou à en demander la rectification ou l'effacement.

---

*(1) Table ronde sur la protection des données personnelles associant Mme Nataliia Bielova, directrice de recherche au centre Inria de l'Université Côte d'Azur, et M. Julien Rossi, maître de conférences en sciences de l'information et de la communication à l'UFR Culture et communication et au Centre d'études sur les médias, les technologies et l'internationalisation (Cémti) de l'université Paris 8, le 1er avril 2026.*

*(2) Article 3, paragraphe 1, b) du règlement omnibus numérique.*

L'omnibus tend également à **limiter le droit d'accès aux données personnelles, consacré à l'article 15 du RGPD**. Il est proposé de modifier l'article 12, paragraphe 5 pour autoriser le responsable de traitement à refuser de donner suite aux demandes d'accès aux données personnelles, ou à exiger le paiement de frais raisonnables en contrepartie, lorsque la personne concernée « *abuse des droits conférés par le présent règlement à des fins autres que la protection de ses données* ». La charge de la preuve serait par ailleurs réduite, le responsable de traitement n'ayant plus à démontrer « *le caractère manifestement infondé ou excessif de la demande* », mais seulement « *qu'il existe des motifs raisonnables de croire qu'elle est excessive* », selon une formule imprécise qui accroît l'insécurité juridique.

**Cette réduction du droit d'accès à la seule fin de protection des données permettrait aux responsables de traitement de rejeter les demandes qui auraient des finalités économiques, politiques ou juridiques**. Ces dernières sont pourtant tout aussi essentielles, comme l'a expliqué M. Max Schrems : « *Dans le monde du travail, par exemple, il arrive que des personnes demandent à obtenir le registre des heures qu'elles ont travaillées en vue de se faire payer leurs heures supplémentaires ; elles invoquent alors cet article 15. Or, en Allemagne, on entend monter la volonté que de telles requêtes ne puissent être faites qu'à des fins de protection des données personnelles. Les entreprises, si elles pouvaient ainsi statuer sur la recevabilité de chaque demande en fonction de ses motifs, en profiteraient pour les rejeter – ce qui serait le point de départ de procédures judiciaires longues de plusieurs années* » (1).

Si la Commission européenne prétend vouloir prévenir les usages abusifs du droit d'accès, cet objectif paraît en décalage avec la situation observée, surtout marquée par un **large contournement du droit d'accès par les entreprises**. L'association Noyb relevait ainsi, en avril 2026, que seules 16,5 % des demandes d'accès qu'elle avait transmises aux entreprises au cours des huit dernières années avaient reçu une réponse satisfaisante, quand 30 % étaient restées sans réponse, et 53,7 % n'avaient obtenu qu'une réponse incomplète (2).

La restriction du droit d'accès est d'autant plus préoccupante qu'il est la condition préalable à l'exercice des autres droits des personnes sur leurs données, en permettant de savoir si de telles données ont été collectées et font l'objet d'un traitement.

L'omnibus prévoit, enfin, de dispenser de l'obligation de fournir des informations sur le traitement de données personnelles, s'« *il existe des motifs raisonnables de supposer que la personne concernée dispose déjà des informations visées* » (3), là où il était auparavant nécessaire de s'en assurer.

---

*(1) Audition de M. Max Schrems, fondateur de l'association Noyb, le 26 mars 2026.*

*(2) Noyb, « Digital omnibus : 83,5 % des demandes d'accès ne reçoivent pas de réponse adéquate », 16 avril 2026. https://noyb.eu/fr/digital-omnibus-reality-check-835-access-requests-not-properly-answered*

*(3) Article 3, paragraphe 5 du règlement omnibus numérique.*

### *c. Un blanc-seing pour utiliser des données personnelles dans l'entraînement et l'exploitation des systèmes d'IA*

L'omnibus comprend plusieurs dispositions destinées à faciliter le traitement des données personnelles pour entraîner et exploiter des modèles d'IA. La Commission vise ainsi à répondre aux questions soulevées par l'application du RGPD aux systèmes d'IA, en particulier concernant le recueil du consentement et l'exercice des droits des personnes.

Il est notamment prévu d'introduire un **article 88 *quater* pour permettre que le traitement de données à caractère personnel nécessaire à l'entraînement et au développement de systèmes d'IA puisse se fonder sur l'intérêt légitime, cette base légale dispensant les développeurs de modèles d'IA de recueillir le consentement des utilisateurs** [(1)].

De fait, le recueil du consentement peut être difficile lorsque l'entraînement s'appuie sur un volume important de données publiquement accessibles en ligne ou au sein d'une base de données ouverte, sans contact avec les personnes concernées.

**L'ajout d'une nouvelle base légale n'apparaissait cependant pas nécessaire dans la mesure où l'intérêt légitime est déjà prévu par l'article 6, paragraphe 1, point f) du RGPD**. Le CEPD a confirmé, dans son avis du 17 décembre 2024 sur les modèles d'IA [(2)], qu'il pouvait bien être invoqué pour le traitement de données personnelles par des systèmes d'IA. L'avis rappelle cependant que l'utilisation de l'intérêt légitime est conditionnée à un **triple test de proportionnalité** :

– l'intérêt poursuivi doit bien être légitime, c'est-à-dire légal au regard du droit et déterminé de façon suffisamment claire et légitime ;

– le traitement doit être nécessaire à l'entraînement du modèle, sans qu'il soit possible d'atteindre l'intérêt par des moyens moins intrusifs pour la vie privée ;

– l'utilisation des données personnelles ne doit pas porter une atteinte disproportionnée à la vie privée des personnes, ce qui s'apprécie au cas par cas. Le responsable de traitement devra mettre en place des garanties limitant ces risques, par exemple l'anonymisation ou la pseudonymisation des données personnelles collectées, ou des dispositifs permettant aux personnes d'exercer leurs droits d'opposition ou d'effacement.

Or, l'omnibus ne fait aucune référence à cette triple exigence de proportionnalité. La seule finalité d'entraîner et d'exploiter des modèles d'IA paraît

*(1) Article 3, paragraphe 6 du règlement omnibus numérique.*

*(2) Avis du Comité européen de la protection des données relatif à certains aspects de la protection des données liées au traitement de données à caractère personnel dans le contexte des modèles d'IA, adopté le 17 décembre 2024*

à cet égard bien trop large pour pouvoir constituer un intérêt légitime au sens de la jurisprudence de la CJUE.

L'article 88 *quater* prévoit que le traitement des données personnelles par les systèmes d'IA doit faire l'objet « *de mesures organisationnelles et techniques et de garanties appropriées pour les droits et libertés de la personne concernée* ». Il mentionne notamment la minimisation des données, la non-divulgation des données conservées de façon résiduelle, et le droit inconditionnel des personnes à s'opposer au traitement de leurs données personnelles.

**Ces garanties ne sont cependant citées qu'à titre d'exemple et ne sont pas définies de façon suffisamment claire. Leur mise en œuvre risque par ailleurs de se heurter aux difficultés techniques souvent invoquées par les développeurs de systèmes d'IA pour ne pas donner suite aux demandes**. Afin d'être en mesure d'exercer leurs droits, les personnes devraient être informées en amont de l'utilisation de leurs données personnelles et disposer d'un délai suffisant pour s'opposer au traitement avant que celui-ci ne débute, comme le relève le CEPD (1). Or, en pratique, les informations de contact sont souvent manquantes et l'identification des données personnelles relatives à une personne est complexe (2). Les droits de rectification, d'effacement et d'opposition nécessitent, en outre, de réentraîner les systèmes d'IA sur une nouvelle base de données.

Les mesures prises pour limiter la divulgation ou la « régurgitation » des données personnelles ne sont pas plus satisfaisantes, comme l'a illustré M. Max Schrems : « *Une de nos affaires en cours concerne par exemple un ressortissant norvégien dont l'intelligence artificielle d'OpenAI prétend qu'il a assassiné ses enfants, maltraité sa femme et commis toute une série d'actes aussi horribles que fictifs. Or, quand nous demandons à OpenAI de corriger ces informations produites par son algorithme, l'entreprise explique être techniquement incapable de le faire. De nombreuses personnes témoignent de cas similaires. (…). Que des compagnies de la Big Tech, qui engrangent des milliards, affirment n'avoir aucun moyen de corriger ces erreurs ou de traiter le problème est affligeant. C'est précisément pour ces raisons que nous nous sommes dotés des principes qui figurent dans le RGPD.* » (3)

**La reconnaissance explicite d'une présomption d'intérêt légitime pour les modèles d'IA rompt avec la neutralité technologique qui caractérisait le RGPD**. Selon l'association Noyb, cela revient à consacrer une sorte de **« *privilège de l'intelligence artificielle* »** en autorisant les sociétés à déroger largement à l'obligation de recueillir un consentement libre et éclairé : « *Au cœur du débat sur l'entraînement des IA se trouve la nécessité soit d'obtenir le consentement d'un nombre suffisant d'utilisateurs pour pouvoir entraîner les modèles (opt-in), soit de permettre aux entreprises d'utiliser simplement les données de tout le monde tout*

*(1) Avis conjoint du Comité européen de la protection des données et du Contrôleur européen de la protection des données sur la proposition de règlement omnibus numérique, adopté le 10 février 2026.*

*(2) Noyb, rapport sur l'omnibus numérique, publiée le 24 février 2026.*

*(3) Audition de M. Max Schrems, fondateur de l'association Noyb, le 26 mars 2026.*

*en offrant uniquement la possibilité de s'y opposer (opt-out).* ***La proposition de la Commission tend à faire peser la charge de la gestion minutieuse des choix des utilisateurs sur 450 millions d'Européens, plutôt que sur une poignée d'entreprises spécialisées dans l'entraînement des IA.*** »

En parallèle, **l'omnibus étend la possibilité que les modèles d'IA traitent des données personnelles sensibles,** par un amendement à l'article 9 du RGPD (1). Cela recouvre notamment les données qui révèlent l'origine ethnique, les opinions politiques, les convictions religieuses, l'orientation sexuelle, des données biométriques, ou encore les données de santé. Actuellement, les modèles d'IA ne peuvent traiter de telles données qu'à titre exceptionnel, pour détecter et corriger les biais des systèmes d'IA à haut risque, conformément à l'article 10 du règlement sur l'intelligence artificielle. Le CEPD a estimé que les garde-fous prévus par le texte étaient, là encore, vagues et insuffisants.

### *d. L'intégration de la régulation des cookies dans le RGPD : en pratique, un transfert de compétence à l'Irlande*

L'omnibus porte, enfin, 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 via le placement de traceurs soit uniquement régi par le RGPD, et non plus par l'article 5, paragraphe 3 de la directive e-privacy** comme c'est le cas aujourd'hui (2). La Commission européenne espère ainsi mettre fin au double régime qui prévaut pour le traitement des données personnelles et unifier la répartition des compétences entre différentes autorités dans le cas de traitements transfrontaliers. De fait, seul le RGPD a mis en place un mécanisme de guichet unique, la directive e-privacy renvoyant à la compétence de chaque État membre.

**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.**

La présidente de la Cnil, Marie-Laure Denis, a mis en garde contre le **risque d'affaiblissement de la protection des données qui résulterait de la perte de l'expertise construite par la Cnil sur ce sujet** : « *Le texte conduirait en pratique à soumettre la régulation des traceurs au mécanisme européen dit du guichet unique, donc, très concrètement, à la confier à deux ou trois autorités au sein de l'Union européenne – les autorités irlandaise et luxembourgeoise, par exemple. Je ne sais pas comment cela peut se traduire en pratique :* ***la Cnil a reçu 2 000 plaintes***

*(1) Article 3, paragraphe 3, point a) de la proposition de règlement omnibus numérique.*

*(2) Article 3, paragraphe 15, de la proposition de règlement omnibus numérique.*

***concernant les traceurs ces trois dernières années ; comment une ou deux autorités vont-elles pouvoir absorber toutes les plaintes actuellement déposées dans vingt-sept pays ? Si cette réforme aboutit, n'y a-t-il pas un risque que cela se traduise par une diminution des droits des personnes et de l'effectivité de la régulation ?*** *Or, en France, nous avons particulièrement investi ce champ de la régulation depuis six ans. Nous avons été à l'avant-garde pour construire une régulation équilibrée, validée par le Conseil d'État, qui a donné lieu à quarante-huit sanctions et à 953 millions d'euros d'amende. En tout cas, c'est une préoccupation pour nous*. » (1)

La rapporteure relève qu'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, et qui relèveraient donc des autorités luxembourgeoise, irlandaise ou néerlandaise si la fusion était adoptée**.

**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.** Il sera ainsi possible d'y déroger pour « *créer des informations agrégées sur l'utilisation d'un service en ligne afin de* ***mesurer l'audience*** *de ce service* », ou « ***maintenir ou rétablir la sécurité*** *d'un service fourni par le responsable du traitement et demandé par la personne concernée ou l'équipement terminal utilisé pour la fourniture de ce service* ».

Pourtant, les traitements visant à mesurer l'audience sont loin d'être neutres, comme l'a expliqué Mme Nataliia Bielova : « *La proposition omnibus semble considérer que ces pratiques auraient peu d'impact sur la vie privée et sur la collecte de données. Or, nos travaux montrent que certains de ces services collectent un volume considérable de données granulaires. Nous avons étudié l'un de ces services qui suit, de fait, chaque clic de souris, chaque mouvement, chaque interaction sur internet. Il apparaît que, bien souvent, le volume de données collectées est totalement disproportionné par rapport à la finalité affichée. Nous estimons, en conséquence, que ces pratiques posent un problème d'autant plus grave qu'elles sont fréquemment combinées et fusionnées avec d'autres profils. Dans nos travaux antérieurs, nous avons observé des techniques de fusion permettant de relier deux identifiants distincts. Sur un échantillon de 9 000 sites étudiés, 40 % recouraient à ce type de méthode. Le projet actuel affaiblit donc, selon nous, la protection des données personnelles*. » (2) Le CEPD partage ces inquiétudes et a recommandé de limiter le champ de l'exception à la collecte d'informations anonymes permettant d'évaluer la performance d'un site sans être directement reliées à des individus.

---

*(1) Audition de Mme Marie-Laure Denis, présidente de la Cnil, le 15 avril 2026.*

*(2) Table ronde sur la protection des données personnelles le 1er avril 2026.*

S'agissant de la dérogation dont bénéficierait l'accès aux données personnelles dans le terminal à des fins de sécurité, elle risque selon Noyb de *« permettre des recherches étendues et massives dans les données stockées localement sur les smartphones, les ordinateurs et autres appareils similaires »*. Si aucune exigence de proportionnalité ne s'appliquait, il serait, par exemple, possible qu'un fournisseur de jeux vidéo analyse l'intégralité de l'ordinateur des joueurs pour s'assurer que ceux-ci n'ont pas installé de logiciels de triche.

Enfin, l'omnibus entend lutter contre la fatigue des cookies en exigeant que l'utilisateur puisse **rejeter les demandes de consentement au moyen d'un « *bouton à simple clic ou par un moyen équivalent* »**. Il est également prévu que les fournisseurs de navigateurs fournissent des **moyens techniques permettant aux personnes de donner ou de refuser leur consentement de façon automatisée et lisible par machines**.

Si ces dispositions sont intéressantes et répondent à un réel besoin, elles soulèvent là encore des questions. Mme Nataliia Bielova note que le mécanisme permettant de refuser les cookies en un seul clic ne suffira pas à protéger les utilisateurs contre les interfaces trompeuses, non traitées par l'omnibus. **Quant au traitement automatique du consentement, il sera essentiel que les choix des utilisateurs puissent être renseignés avec la granularité nécessaire**, en distinguant les finalités de traitement, et en prenant en compte les *cookie walls*. Les utilisateurs pourraient sinon être amenés à accepter par défaut l'ensemble des cookies pour ne pas se voir refuser systématiquement l'accès à des sites web qui appliquent ce mécanisme. M. Thomas Dautieu, directeur de l'accompagnement juridique de la Cnil, a confirmé ce risque : « *Si vous dites non à tout, ça marche. Mais si vous souhaitez par exemple accepter les cookies seulement pour les sites culturels et non pour les sites marchands, ça marche moins bien : c'est tout ou rien*. » (1) La Cnil a engagé des discussions avec des entreprises qui proposent des solutions techniques pour une approche plus fine via le navigateur.

### 2. À rebours des objectifs affichés de simplification et de soutien aux PME, des propositions qui accroissent l'insécurité juridique au profit des grandes plateformes

Alors que l'omnibus numérique visait à simplifier le droit de la protection des données afin d'alléger les charges administratives pesant sur les petites entreprises et de favoriser l'innovation en Europe, il ressort des travaux de la commission d'enquête que les modifications proposées risquent, au contraire, d'accroître la complexité juridique et de consolider la position dominante des grands acteurs extra-européens. La perplexité exprimée par M. Robin Berjon, informaticien et directeur de l'agence Supramundane, fait écho à celle de l'ensemble des personnes auditionnées : « *Pour ce qui est de l'omnibus, le texte est tellement mauvais – concernant presque l'intégralité de ses dispositions – que je ne sais pas*

*(1) Audition de Mme Marie-Laure Denis, présidente de la Cnil, le 15 avril 2026.*

*quoi vous dire.* ***Si l'on cherchait à couler ce qu'il reste de l'industrie technologique en Europe, on ne pourrait pas mieux faire****.* » (1)

***a. Une simplification manquée***

L'objectif de simplification poursuivi par la Commission européenne est, certes, pleinement légitime. Certaines dispositions du RGPD sont excessivement difficiles à mettre en œuvre et suscitent une charge administrative importante, notamment pour les petites et moyennes entreprises. M. Robin Berjon, qui dit avoir travaillé à l'application du RGPD pendant cinq ans, reconnaît que « *des évolutions qui ne nuiraient à personne seraient possibles, notamment à l'article 30 ou aux articles 12 à 19. ».* L'association Noyb soutient également la démarche de simplification de la Commission et salue quelques modifications qui permettent une réelle réduction des formalités administratives.

Force est cependant de constater que **la majeure partie des modifications portées par la Commission ne font qu'accroître la complexité juridique du RGPD, par des dispositions souvent confuses, imprécises ou inapplicables**. L'utilisation d'expressions aussi vagues qu'« 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.

**Le cas emblématique en est la modification de l'article 13 du RGPD** sur l'obligation de fourniture d'informations lorsque des données à caractère personnel sont collectées auprès de la personne concernée. Le paragraphe 4 prévoit actuellement que les obligations prévues aux trois premiers paragraphes « *ne s'appliquent pas lorsque, et dans la mesure où, la personne concernée dispose déjà de ces informations* ». La Commission européenne propose de remplacer cette disposition claire et simple par le paragraphe suivant : « *Les paragraphes 1, 2 et 3 ne s'appliquent pas lorsque les données à caractère personnel ont été collectées dans le cadre d'une relation claire et circonscrite entre des personnes concernées et un responsable du traitement exerçant une activité sans usage intensif de données et qu'il existe des motifs raisonnables de supposer que la personne concernée dispose déjà des informations visées au paragraphe 1, points a) et c), sauf si le responsable du traitement transmet les données à d'autres destinataires ou catégories de destinataires, les transfère vers un pays tiers, pratique la décision automatisée, y compris le profilage, au sens de l'article 22, paragraphe 1, ou que le traitement est susceptible de comporter un risque élevé pour les droits et libertés des personnes concernées au sens de l'article 35*. »

**Alors que l'objectif était d'assouplir l'obligation de fournir des informations, la dérogation demeure soumise à pas moins de sept critères, dont certains très vagues, qui pourraient faire l'objet d'interprétations divergentes**. La Commission fait valoir, dans le document de travail accompagnant la proposition, que cette « *simplification des exigences en matière d'information*

*(1) Audition de M. Robin Berjon, informaticien, directeur de l'agence Supramundane, le 10 mars 2026.*

*aiderait grandement les PME qui ne mènent pas d'activités de traitement à forte intensité de données ou à haut risque, telles que les artisans, les coiffeurs ou les boulangers, car elles seraient dispensées de l'obligation de rédiger des avis de confidentialité* ». Selon Noyb, il est très peu probable que les PME puissent bénéficier de cet allègement, puisqu'elles n'en vérifieront pas les conditions : elles ont généralement recours à des sous-traitants (hébergeur web, fournisseur de messagerie électronique, logiciels de comptabilité) et transmettent donc les données à des destinataires, dont certains sont situés dans des pays tiers (1).

De même, **l'omnibus risque de complexifier le cadre applicable aux traceurs**. Il est prévu de soumettre au RGPD les seuls traceurs permettant le traitement de données personnelles ; l'accès aux données non personnelles stockées dans l'équipement terminal resterait régi par la directive e-privacy. Les représentants du Comité européen de la protection des données ont fait part à la rapporteure et au président de leur inquiétude qu'une telle scission compromette la bonne application des règles et la détermination des compétences : l'autorité compétente ne sera pas la même selon que les données sont personnelles ou non, ce qui pourrait être difficile à déterminer a priori. Le nouveau cadre aurait, de surcroît, l'effet incohérent de soumettre l'accès aux données personnelles à des conditions moins protectrices que pour les données non personnelles.

**Le même constat s'impose pour le changement de définition des données personnelles**, comme l'a développé la présidente de la Cnil : « *De mon point de vue,* ***ce serait tout sauf de la simplification : ce qui serait une donnée à caractère personnel pour l'un serait une donnée anonyme pour l'autre. Des données identiques prendraient ainsi un double visage****. Les responsables de traitement de données devraient porter une appréciation sur leur capacité à identifier ou non les personnes derrière les données qu'ils détiennent. Or une telle appréciation serait subjective : à partir de quel degré d'effort estime-t-on que l'identification n'est pas « raisonnablement » possible ? De plus, cette appréciation devrait évoluer avec les technologies.* » (2)

**La démarche de la Commission européenne tendant à codifier les arrêts de la CJUE ou des lignes directrices des autorités de protection des données suscite également des interrogations**. Comme l'ont fait observer les représentants du CEPD, la jurisprudence de la Cour est juridiquement applicable sans qu'il soit nécessaire de l'inscrire explicitement dans le règlement. De nombreuses questions ont déjà fait l'objet de lignes directrices ou d'opinions du CEPD, que les autorités sont tenues d'appliquer et qui sont souvent bien plus détaillées et précises que les amendements proposés par l'omnibus. C'est notamment le cas de la définition de la recherche scientifique (3), de l'application du RGPD aux modèles d'IA (4), de

*(1) Noyb, rapport sur l'omnibus numérique, publiée le 24 février 2026.*

*(2) Audition de Mme Marie-Laure Denis, présidente de la Cnil, le 15 avril 2026.*

*(3) Lignes directrices 1/2026 sur le traitement de données personnelles pour les finalités de recherche scientifique, adoptées le 15 avril 2026.*

*(4) Avis 28/2024 relatif à certains aspects de la protection des données liés au traitement de données à caractère personnel dans le contexte des modèles d'IA, adopté le 17 décembre 2024.*

l'intérêt légitime [1], ou encore de la pseudonymisation [2]. La possibilité de se fonder sur l'intérêt légitime pour traiter des données personnelles aux fins d'entraîner un modèle d'IA était ainsi déjà admise par l'avis du CEPD, et la codification n'apporte à cet égard aucune clarification puisque c'est aux autorités ou aux juridictions qu'il reviendra de vérifier que la triple exigence de proportionnalité est bien remplie.

Au-delà de l'omnibus numérique, **c'est toute l'approche par les risques sur laquelle repose le RGPD qui serait en cause** selon M. Max Schrems : « *En effet, ce que le législateur européen appelle « approche fondée sur l'analyse des risques » implique de confier aux entreprises elles-mêmes l'évaluation des risques. Elles sont ainsi comme des enfants dans un magasin de bonbon, qu'on autoriserait à définir combien de sucre il est souhaitable et raisonnable de consommer. De telles normes juridiques ne sont pas applicables ; elles n'aident personne. Les avocats les critiquent beaucoup car elles leur rendent difficile d'indiquer à leur client ce qui est autorisé et ce qui est interdit. J'aime dire que ces lois numériques européennes sont comme les autoroutes allemandes, où chaque conducteur définit librement sa vitesse, c'est-à-dire le niveau de risque qu'il estime correct pour lui. Mais on pourrait choisir une autre approche de l'analyse du risque, ce que font, d'ailleurs, la majorité des pays européens, en limitant la vitesse – à 30 kilomètres à l'heure devant les écoles, 50 kilomètres à l'heure en ville, et ainsi de suite. Ces limitations rendent le risque gérable, avec des lignes rouge claires*. » [3]

***b. Un « énorme cadeau » aux Big Tech***

La Commission européenne prétend que « *les PME et autres petits opérateurs bénéficieraient de la plupart, voire de la totalité, des modifications proposées*. » [4]

**Cet argument est battu en brèche par M. Max Schrems** : « *On entend souvent que les lois les plus flexibles sont plus adaptées aux petites et moyennes entreprises ; en réalité, elles les accablent, parce qu'elles les contraignent à recruter des avocats simplement pour comprendre à quelles obligations elles sont soumises, alors qu'elles n'en ont pas les moyens. Nous le constatons au quotidien dans les litiges :* ***les entreprises qui gagnent à la flexibilité du droit sont celles de la Big Tech, dont les avocats débattent pendant des centaines d'heures sur les obligations légales attachées au moindre cookie****. Plutôt que de se demander quel gros titre on pourra tirer d'une législation, il faut se demander à qui elle profitera*

---

*(1) Lignes directrices 1/2024 sur le traitement des données personnelles fondé sur l'article 6(1)(f) du RGPD, adoptées le 8 octobre 2024.*

*(2) Lignes directrices 01/2025 sur la pseudonymisation, adoptées le 16 janvier 2025.*

*(3) Audition de M. Max Schrems, fondateur de l'association Noyb, le 26 mars 2026.*

*(4) Document de travail de la Commission européenne accompagnant les propositions de règlements dits omnibus numérique et omnibus sur l'intelligence artificielle (SWD[2025] 836 final) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025SC0836*

*réellement.* » [1]. C'est d'autant plus le cas que cette flexibilité repose sur une complexification des règles.

Au contraire, les petites entreprises ont besoin de s'appuyer sur des règles claires et accessibles. « *Ma mère a une petite entreprise de dix employés et elle ne veut pas avoir à définir elle-même les obligations auxquelles elle doit se soumettre dès lors que le nombre d'abonnés à sa newsletter dépasse les 10 000,* souligne M. Max Schrems. *Dans une société démocratique, le législateur a le devoir de fixer des règles claires de régulation du numérique – ce qui est bien autre chose que de se décharger de l'évaluation du risque et de la fixation des règles sur les acteurs économiques*. »

Selon M. Henri Verdier, la technique des lobbyistes « *ne consiste pas tant à murmurer des contre-vérités à l'oreille des dirigeants qu'à tout complexifier ».*

**Les grandes plateformes extra-européennes sont également les 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. Elles pourront pleinement exploiter les dérogations aux droits des personnes créées par l'omnibus, notamment au droit d'accès, au risque de compromettre de larges pans du RGPD. Elles seront également les plus à mêmes de tirer profit des possibilités offertes par l'omnibus en matière d'IA, ayant déjà commencé à entraîner leurs modèles sur les stocks considérables de données personnelles dont elles disposent.

**L'omnibus numérique pourrait ainsi renforcer la position dominante des grandes plateformes, en accélérant la concentration des données à leur profit**, comme met en garde M. Robin Berjon : « *L'omnibus numérique risque de couler les entreprises européennes parce qu'il part d'une théorie complètement fausse selon laquelle plus les données circulent, plus on crée de la valeur. Les personnes qui défendent cette idée estiment que le RGPD a empêché les données de circuler – ce qui est faux – et qu'en fluidifiant leur circulation, tout le monde bénéficiera de cette économie numérique fondée sur les données. Or nous savons, notamment grâce aux travaux de juristes américains comme Lina Khan, qu'**accroître la circulation des données favorise les grands acteurs et crée un phénomène de concentration**. Si le texte proposé aujourd'hui était adopté en l'état, ce serait un **énorme cadeau fait à Google et à Meta**, qui pourraient collecter un nombre supérieur de données encore plus facilement. À l'inverse, les entreprises européennes ne pourraient plus tirer avantage de leur accès à certains publics et aux données qu'elles collectent elles-mêmes pour leurs propres besoins*. » [2]. **La proposition de la Commission européenne porte l'empreinte du lobbying des grandes plateformes extra-européennes**. Une étude conduite par les ONG

*(1) Audition de M. Max Schrems, fondateur de l'association Noyb, le 26 mars 2026*

*(2) Audition de M. Robin Berjon, informaticien, directeur de l'agence Supramundane, le 10 mars 2026.*

*Corporate Europe Observatory (CEO)* et *Lobby Control* [1] révèle que **de nombreux amendements proposés par la Commission répondent directement à des demandes formulées par les Gafam**. Le tableau ci-dessous met en regard les propositions d'amendements transmises à la Commission européenne ou à des États membres par ces entreprises ou leurs groupes d'intérêt et les modifications effectivement retenues dans l'omnibus numérique.

*(1)* Corporate Europe Observatory *et* LobbyControl*, « Article par article, comment les Big Tech ont influencé le recul de l'Union européenne en matière de droits numériques », 14 janvier 2026 (https://corporateeurope.org/en/2026/01/article-article-how-big-tech-shaped-eus-roll-back-digital-rights).*

**COMPARAISON DES MODIFICATIONS AU RGPD PROPOSÉES PAR L'OMNIBUS NUMÉRIQUE AVEC LES CONTRIBUTIONS TRANSMISES PAR LES GAFAM**

| | **Modifications au RGPD proposées par l'omnibus numérique** | **Propositions transmises par les Gafam ou leurs représentants d'intérêt** |
|---|---|---|
| **Définition des données personnelles** | Ajouter à l'article 4, paragraphe 1 du RGPD : « *Les informations ne revêtent pas de caractère personnel pour une entité donnée lorsque ladite entité ne peut identifier la personne physique à laquelle elles se rapportent, compte tenu des moyens raisonnablement susceptibles d'être utilisés par cette entité* » | **Digital Europe** a demandé de « *préciser que les données pseudonymisées ne constituent pas des données personnelles lorsque les destinataires ne sont pas en mesure, de manière raisonnable, de réidentifier les personnes concernées* » (1) |
| **Droit d'accès aux données** | Modifier l'article 12(5) ainsi :<br>« *Lorsque les demandes d'une personne concernée sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif,* ***ou également, lorsqu'il s'agit de demandes au titre de l'article 15, parce que la personne concernée abuse des droits conférés par le présent règlement à des fins autres que la protection de ses données****, le responsable du traitement peut :*<br>*a) exiger le paiement de frais raisonnables qui tiennent compte des coûts administratifs supportés pour fournir les informations, procéder aux communications ou prendre les mesures demandées ; ou*<br>*b) refuser de donner suite à ces demandes*. » | **Google** a proposé au gouvernement allemand l'amendement suivant :<br>« *Lorsque les demandes d'une personne concernée sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif,* ***ou lorsque, compte tenu de l'étendue du traitement et du coût de la mise en œuvre, répondre à la demande impliquerait un effort disproportionné****, le responsable du traitement peut soit :*<br>*a) exiger le paiement de frais raisonnables qui tiennent compte des coûts administratifs supportés pour fournir les informations, procéder aux communications ou prendre les mesures demandées ; ou*<br>*b) refuser de donner suite à ces demandes*. » (2) |
| **Utilisation des données personnelles pour entraîner des modèles d'IA** | Ajouter un article 88 *quater* :<br>« *Lorsque le traitement de données à caractère personnel est nécessaire aux intérêts du responsable du traitement dans le cadre du développement et de l'exploitation d'un système d'IA au sens de l'article 3, point 1), du règlement (UE) 2024/1689 ou d'un modèle d'IA, ce traitement peut être réalisé aux fins d'intérêts légitimes au sens de l'article 6, paragraphe 1, point f), du règlement (UE) 2016/679, le cas échéant (…)* ». | Le **CCIA** a souligné : « *Il est essentiel de réaffirmer le rôle de l'intérêt légitime en tant que fondement juridique au titre du RGPD pour une innovation responsable en matière d'IA, en allant au-delà de l'avis non contraignant du CEPD afin d'assurer une sécurité juridique harmonisée pour l'entraînement des modèles d'IA* » (3)<br>**Digital Europe** a appelé la Commission à « r*enforcer le recours à l'« intérêt légitime » comme fondement juridique du traitement des données à caractère personnel pour des cas d'utilisation clés tels que le développement de produits – y compris de modèles d'IA – et la sécurité* » (4) |
| **Intégration de e-privacy dans le RGPD** | Ajouter un article 88 *bis* « Traitement des données à caractère personnel dans l'équipement terminal des personnes physiques » qui intègre dans le RGPD les règles relatives aux cookies pour les données personnelles.<br>Modifier l'article 5, paragraphe 3, de la directive e-privacy en conséquence. | **Google** : « *La simplification la plus efficace consiste à supprimer l'article 5 (3) de la directive « vie privée et communications électroniques » et à régir l'ensemble des traitements de données liés aux cookies dans le cadre du RGPD, fondé sur l'évaluation des risques* » (5)<br>**Microsoft** : « *La « règle relative aux cookies » prévue à l'article 5 (3), de la directive ePrivacy pourrait être transférée dans le RGPD » (6)* |

| | Modifications au RGPD proposées par l'omnibus numérique | Propositions transmises par les Gafam ou leurs représentants d'intérêt |
|---|---|---|
| **Extension des exceptions au recueil du consentement pour les cookies** | Ajouter à l'article 88 *bis* :<br>« *Le stockage de données à caractère personnel, ou l'obtention de l'accès à des données à caractère personnel déjà stockées, dans l'équipement terminal d'une personne physique à défaut de consentement, ainsi que leur traitement ultérieur, sont licites dans la mesure où ils sont nécessaires pour :*<br>*a) effectuer la transmission d'une communication électronique par la voie d'un réseau de communications électroniques ;*<br>*b) fournir un service expressément demandé par la personne concernée ;*<br>***c) créer des informations agrégées sur l'utilisation d'un service en ligne afin de mesurer l'audience de ce service, lorsque cette action est effectuée par le responsable du traitement de ce service en ligne pour son propre usage exclusif ;***<br>***d) maintenir ou rétablir la sécurité d'un service fourni par le responsable du traitement et demandé par la personne concernée ou l'équipement terminal utilisé pour la fourniture de ce service***. » | **Google** : « *Une autre mesure importante en faveur de la simplification consisterait à modifier l'article 5, paragraphe 3, afin d'élargir le champ d'application des exemptions autorisées et d'inclure des activités de traitement spécifiques et à faible risque qui sont essentielles tant au bon fonctionnement d'un écosystème numérique sûr et durable qu'à l'expérience utilisateur. Cela permettrait d'établir des exemptions claires pour des fonctions telles que la mesure d'audience, la limitation de la fréquence publicitaire et les mesures de lutte contre la fraude* » (7)<br><br>**Microsoft** : « *si [la règle relative aux cookies] est maintenue, [elle pourrait être] assouplie en autorisant l'installation de cookies sans consentement dans un éventail plus large de situations, par exemple pour des raisons de sécurité, de mises à jour logicielles, de lutte contre la fraude et d'analyse*. » (8) |

(1) https://corporateeurope.org/sites/default/files/2026-01/DigitalEurope%20lobby%20paper.pdf

(2) https://www.lobbyregister.bundestag.de/media/f3/dc/633675/Stellungnahme-Gutachten-SG2510270013.pdf

(3) https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14855-Simplification-digital-package-and-omnibus/F33088547_en

(4) https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14855-Simplification-digital-package-and-omnibus/F33103770_en

(5) https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14855-Simplification-digital-package-and-omnibus/F33088017_en

(6) https://corporateeurope.org/sites/default/files/2026-01/Microsoft%20lobby%20paper%20data%20union%20strategy.pdf

(7) https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14855-Simplification-digital-package-and-omnibus/F33088017_en

(8) https://corporateeurope.org/sites/default/files/2026-01/Microsoft%20lobby%20paper%20data%20union%20strategy.pdf

*Source : Commission d'enquête à partir de Corporate Europe Observatory (CEO) et Lobby Control.*

### *c. Une absence d'étude d'impact malgré l'ampleur des modifications envisagées*

**Les représentants de la Commission européenne que la rapporteure et le président ont rencontrés à Bruxelles leur ont confirmé qu'aucune étude d'impact n'avait été réalisée pour évaluer les conséquences des modifications proposées au RGPD**. Cela s'expliquerait notamment par le choix du véhicule législatif, un règlement omnibus, censé être uniquement technique sans apporter de modifications de fond. Le calendrier a en outre été marqué par une certaine précipitation, liée à la priorité politique accordée par la Commission européenne à son agenda de simplification.

La consultation de l'appel à contributions diffusé par la Commission européenne le 16 septembre 2025 révèle qu'il n'était initialement pas prévu

d'inclure le RGPD dans le paquet législatif sur la simplification numérique [1]. En effet, la direction générale de la justice et des consommateurs (DG Just) indiquait, dans son rapport annuel de 2025 sur la simplification, la mise en œuvre et l'application, que son programme de travail de l'année 2026 serait notamment consacré à « *l'identification d'éventuels amendements ciblés du RGPD* ».

**Les amendements proposés au RGPD constituent donc « *des ajouts de dernière minute* »** qui « *répondent à des impulsions politiques de la Commission* », souligne M. Max Schrems [2].

**Leur élaboration dénote un manifeste manque de préparation** : sur les 200 pages du document de travail accompagnant la proposition de législation [3], seules 10 concernent les modifications apportées au RGPD. La Commission européenne n'avance aucun élément précis pour appuyer l'idée selon laquelle ces amendements « *renforceraient la compétitivité européenne et favoriseraient l'adoption des nouvelles technologies* », ou « *apporteraient des avantages réglementaires directs grâce à une meilleure efficacité opérationnelle et à une réduction des risques, ainsi qu'à un environnement plus propice à l'innovation et au développement* ». Elle reconnaît d'ailleurs qu'il ne lui est « *pas possible d'étayer ces affirmations par des chiffres précis* ». De façon paradoxale, la Commission va jusqu'à citer une consultation mettant en évidence que **96 % des organisations sondées ont estimé que les avantages liés aux investissements en matière de protection de la vie privée l'emportaient sur les coûts**.

**La mauvaise qualité juridique de l'omnibus numérique traduirait également une perte d'expertise au sein de la direction chargée du sujet**, selon M. Max Schrems : « *le principal problème est que l'unité de la Commission européenne chargée de rédiger les propositions de directive ne dispose tout simplement pas du personnel et de l'expertise nécessaires. C'est très regrettable. Même si je ne partageais pas forcément les options politiques de l'équipe précédente, en tant qu'avocat, force est de constater qu'elle était beaucoup plus compétente. L'équipe actuelle, elle, n'est pas forcément en mesure de produire des textes juridiquement valables – les acteurs économiques eux-mêmes hésitent à souscrire à ses propositions, car ils ne voient pas bien comment elles pourraient fonctionner en pratique*. »

**Aussi la rapporteure appelle-t-elle le gouvernement à s'opposer avec fermeté, au sein du Conseil de l'Union européenne, à toutes les modifications du RGPD qui risqueraient d'affaiblir la protection des droits fondamentaux**. La commission des affaires européennes du Sénat a également adopté une proposition de résolution européenne en ce sens le 13 mai 2026. Le rejet par le Conseil de la plupart des dispositions proposées par la Commission est à cet égard encourageant.

---

*(1) https://www.contexte.com/medias/pdf/medias-documents/2025/9/call-for-evidence-digital-omnibus.pdf*

*(2) Audition de M. Max Schrems, fondateur de l'association Noyb, le 26 mars 2026*

*(3) Document de travail de la Commission européenne accompagnant les propositions de règlements dits omnibus numérique et omnibus sur l'intelligence artificielle (SWD[2025] 836 final) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025SC0836*

## CHAPITRE 10 – LE FINANCEMENT DES ENTREPRISES NUMÉRIQUES : LA CHASSE À LA LICORNE

Le financement des entreprises est apparu comme le dernier facteur expliquant le retard des entreprises européennes sur leurs homologues états-uniennes. Le sujet doit être entendu dans une acception large : il s'agissait pour la commission d'enquête de comprendre comment les sociétés du numérique génèrent leurs revenus et financent le développement de leur technologie, dans une approche comparée des deux côtés de l'Atlantique. En effet, la question du financement, et notamment la faiblesse des marchés de capitaux européens, est souvent revenue comme une fatalité, qui expliquerait les limites des entreprises du numérique.

Si ce constat semble s'être imposé dans le débat public, a-t-il été suivi de la mise en place d'actions aux niveaux européen et français pour favoriser le développement des entreprises numériques du continent ? La rapporteure s'est ainsi penchée sur l'action de l'État en direction des entreprises du numérique. Quelle est l'ampleur des efforts de soutien réalisés et quels en sont les effets ?

### A. LES TROIS MOTEURS DU FINANCEMENT DES ENTREPRISES NUMÉRIQUES ÉTATS-UNIENNES : COMMANDE PUBLIQUE, REVENUS D'UN MARCHÉ UNIFIÉ, VENTURE CAPITAL

Au cours des auditions des acteurs du monde économique, trois facteurs sont revenus constamment pour expliquer la puissance actuelle des Gafam.

#### 1. Le soutien de la commande publique

Le premier facteur est le soutien historique de la puissance publique au secteur du numérique comme un prolongement de celui accordé à la défense. Ainsi que l'explique M. Henri Verdier [(1)] : « *Tout d'abord, rappelons qu'une des raisons de l'impact de l'achat public aux États-Unis est d'ordre structurel : à la fin de la guerre froide, le complexe militaro-industriel américain s'est reconverti en complexe numérique. Or la dépense militaire américaine s'élève à 1 000 milliards de dollars, tandis que la nôtre n'atteint que 2,6 milliards de dollars. Les ordres de grandeur, les masses financières et l'écosystème de financement aux États-Unis n'ont pas d'équivalent chez nous* ».

M. Robin Berjon dresse le même constat [(2)] : *« En matière de dépendances structurelles et de vulnérabilités systémiques, la situation dans laquelle nous nous*

*(1) Audition, ouverte à la presse, de M. Henri Verdier, directeur général de la fondation Inria, ancien ambassadeur pour le numérique, le 10 mars 2026.*

*(2) Table ronde, ouverte à la presse, réunissant M. David Chavalarias, directeur de recherche au CNRS, directeur au Centre d'analyse et de mathématiques sociales de l'EHESS, et directeur de l'Institut des systèmes complexes de Paris Île-de-France (ISC-PIF), M. Robin Berjon, informaticien et consultant, directeur de l'agence Supramundane, Mme Maud Quessard, directrice du domaine euratlantique à l'Institut de recherche stratégique de l'École militaire (Irsem), le 10 mars 2026.*

*trouvons n'est pas le fruit du hasard. Elle ne résulte pas d'une quelconque supériorité, culturelle ou autre, des Américains, mais d'un choix politique fait au début des années 1990 et assumé depuis par toutes les administrations.*

« *Au début des années 1990, les États-Unis se sont rendu compte que leurs investissements dans les systèmes militaires n'étaient plus justifiés, du fait de la fin de la guerre froide, et ont décidé de les réorienter vers le secteur de la technologie, particulièrement dans la Silicon Valley. Ces investissements très significatifs, qui s'élèvent à plusieurs centaines de milliards, ont été associés à une politique volontariste visant à permettre aux sociétés informatiques de se développer sans entraves nationales ou internationales, dans un modèle leur confiant la gouvernance de l'internet.* »

M. Yann Lechelle souligne en particulier l'impact du Small Business Act [(1)] : « *En effet, les États-Unis ont mis en place dès 1969 [en réalité dès 1953] un protectionnisme intelligent à travers ce Small Business Act, qui a permis de rediriger les flux publics vers des acteurs locaux devenus ensuite des entreprises majeures. Par exemple, la Defense Advanced Research Projects Agency (Darpa) a financé massivement, par la commande et non par la subvention, des projets à l'origine de l'émergence des hyperscalers, Google ayant par exemple bénéficié de budgets fédéraux considérables* ».

Ainsi que l'indique la Small Business Administration [(2)], l'agence fédérale américaine en charge du soutien aux petites entreprises, le gouvernement des États-Unis est le plus grand consommateur du monde et a l'obligation légale d'acheter à des petites entreprises pour au moins 23 % des achats fédéraux chaque année.

La première source de financement des entreprise américaines, dans leur phase de développement de technologies, est donc la commande publique. Les montants consacrés sont considérables, ainsi que le décrit Mme Maya Noël [(3)] : « *Le taux d'ouverture des marchés publics américains aux acteurs étrangers est de l'ordre de 30 %, tandis que celui des marchés européens est de 80 %. C'est une dynamique structurelle dans laquelle non seulement les États-Unis investissent plus d'argent dans la R&D, mais la commande publique suit davantage. S'ajoutent à cela d'autres initiatives américaines, telles que le Buy American Act, qui représente un investissement de 94 milliards pour favoriser des acteurs américains, ou le Chips and Science Act, qui inclut un plan d'investissement dans les semi-conducteurs et représente 50 milliards de dépenses directes – soit l'équivalent du plan France 2030. Il y a donc un fossé entre l'Europe et les États-Unis dans le soutien public à la recherche et à l'industrie.* »

---

*(1) Audition, ouverte à la presse, de l'association Eurostack, représentée par Mme Cristina Caffarra, économiste, et M. Yann Lechelle, président-directeur général de probabl.ai, le 26 mars 2026.*

*(2) https://www.sba.gov/federal-contracting/contracting-guide*

*(3) Audition, ouverte à la presse, de Mme Maya Noël, directrice générale de France Digitale, 16 avril 2026.*

Ce protectionnisme américain est également souligné par M. Yann Lechelle **:** « *Les États-Unis ont mis en place dès 1969 un protectionnisme intelligent à travers ce Small Business Act, qui a permis de rediriger les flux publics vers des acteurs locaux devenus ensuite des entreprises majeures. Par exemple, la Defense Advanced Research Projects Agency (Darpa) a financé massivement, par la commande et non par la subvention, des projets à l'origine de l'émergence des hyperscalers, Google ayant par exemple bénéficié de budgets fédéraux considérables. Ces mécanismes existent ; il suffit de s'en inspirer* ».

### 2. Une assise importante grâce à un marché unifié

Le second facteur expliquant la puissance des acteurs américains est la capacité à déployer immédiatement leurs produits sur un marché de plus de trois cents millions de consommateurs.

Un marché unifié permet, d'une part, de générer rapidement des revenus importants. Comme l'explique M. Thierry Breton, ancien commissaire européen au marché intérieur (1) : « *Les créateurs des Gafa se sont positionnés pour utiliser les données personnelles générées grâce à l'interconnexion, à l'internet, apparue au début des années 2000. Et si ces géants sont apparus aux États-Unis, puis en Chine, ce n'est pas parce que nous sommes plus idiots que les autres, mais parce que, eux, ils avaient accès à un marché très large avec une langue unique. Les États-Unis, c'est un marché de 330 millions de consommateurs ; nous, on était vingt-sept pays, avec autant de régulations ou de tentatives de régulation – souvent orthogonales d'un pays européen à l'autre, d'ailleurs –, dix-huit langues, des barrières.* »

D'autre part, un marché unifié est synonyme d'économies d'échelle dans les investissements, comme l'indique Mme Christel Heydemann, directrice générale du groupe Orange, « *Pour ce qui est du marché des télécoms, on peut le dire comme on veut, mais la concentration du secteur est essentielle. Il y a actuellement plus de quatre opérateurs dans chaque pays européen. Lorsque vous êtes numéro 1 sur un marché, comme nous le sommes en France, vous avez beaucoup plus de capacité à investir que si vous êtes le numéro 3 ou 4. Par conséquent, si vous n'êtes pas le premier – c'était notre cas en Espagne –, vous êtes condamné, pour pouvoir continuer à investir, par exemple dans la 5G, soit à fusionner avec un autre opérateur – comme nous l'avons fait en Espagne avec MásMóvil –, soit à vendre vos infrastructures pour vous désendetter.* » (2)

La profondeur économique du marché américain constitue ainsi un atout dans le déploiement rapide des entreprises innovantes, car ces dernières peuvent standardiser leur approche technique et commerciale, et générer rapidement les revenus qui leur permettent de financer leur développement.

---

*(1) Audition, ouverte à la presse, de M. Thierry Breton, ancien commissaire européen au Marché intérieur, ancien président-directeur général d'Atos SE, le 15 avril 2026.*

*(2) Audition, ouverte à la presse, de Mme Christel Heydemann, directrice générale du groupe Orange.*

Le constat d'un marché états-unien homogène dépeint en creux celui de la fragmentation du marché européen. Une entreprise qui développera un produit pour un État membre devra effectuer un travail important pour pénétrer un nouveau marché en Europe. M. Arthur Mensch décrit ainsi les problèmes pratiques auxquels est confrontée son entreprise lorsqu'elle souhaite opérer hors de ses frontières : « *Un des problèmes de l'Europe en matière réglementaire, c'est que, dès que l'on entre dans un pays européen, on doit ouvrir une nouvelle entité, comprendre un nouveau régime de stock-options, une nouvelle réglementation du travail… Par conséquent, il faut très vite une équipe sur place. J'ai moi-même signé des centaines de documents et ouvert des dizaines de comptes en banque pour ouvrir des entités dans une dizaine de pays d'Europe. Faute de réglementation unifiée, de droit social unifié, il faut s'adapter à chaque pays.*

« *(…) Cette absence de marché unifié constitue la principale lourdeur du système. (…) La fragmentation du marché n'est pas un atout. C'est plutôt un inconvénient parce qu'elle nécessite de composer des équipes différentes, qui vendent de façon différente selon les endroits. (…)* ».

Le même constat est dressé par M. Henri d'Agrain [(1)] : « *Lorsque j'évoque les conditions nécessaires, je parle de la création d'un véritable marché numérique européen. En effet, un marché fragmenté en marchés nationaux français, allemand, espagnol ou italien ne peut pas fonctionner durablement. Ce sont toujours les acteurs qui bénéficient d'un marché unifié qui s'imposent face aux autres. Pour les grandes entreprises, celles que je connais et que je représente, il est indispensable d'aboutir enfin à ce marché numérique unique, ce « digital single market » dont nous parlons depuis quinze ou vingt ans, sans jamais réellement le concrétiser. Il ne s'agit plus de raisonner en termes d'acteurs nationaux, mais d'identifier les grands opérateurs européens de cloud sur lesquels il conviendrait de concentrer des investissements massifs.* »

### 3. Le financement de la croissance des entreprises grâce à un marché financier structuré

Enfin, le troisième facteur de succès du numérique aux États-Unis est la présence d'acteurs financiers de premier plan capables de financer le développement d'entreprises qui « brûlent du cash » (*cash-burn*) pour financer une croissance très rapide, dans l'objectif de s'imposer face à la concurrence selon le principe du « *winner takes it all* ». C'est le fondement même du capital-risque ou *venture capital*.

D'une part, l'épargne disponible est abondante et drainée vers le financement de la tech. « *Nous avons face à nous une économie de capital-risque financée par des investissements considérables, dans un pays capable d'émettre autant de dollars qu'il le souhaite – puisqu'il peut en créer lorsqu'il en*

*(1) Audition de M. Henri d'Agrain, délégué général du Club informatique des grandes entreprises françaises (Cigref) le 30 avril 2026.*

*manque* » [1]. Selon Cédric O, « *La puissance financière américaine vient des fonds de pension. Lorsqu'un acteur comme Fidelity consacre seulement 1 % ou 2 % de ses actifs au capital-risque, ça représente des montants considérables.* » [2]

D'autre part, les marchés financiers sont structurés pour ces opérations, et sont soutenus par un écosystème très complet permettant de mener à bien des financements de taille très importante.

M. Arnaud Caudoux [3], directeur général adjoint de BPIFrance, explique de façon très précise dans quelle mesure le financement des levées de fonds repose sur des mécanismes croisés d'échanges de titres entre entreprises, dans des constructions financières qui s'autoalimentent : « *C'est le premier élément de différence entre les États-Unis et l'Europe aujourd'hui : la taille du segment du capital-risque. Cette taille vient de deux choses : la disponibilité des capitaux à s'investir dans le capital-risque – ce sont beaucoup les fonds de pension américains et les endowments des universités, que nous n'avons pas à la même échelle en Europe – et la capacité de ces fonds ensuite à vendre les entreprises.*

« *Effectivement, les fonds américains ont une capacité à vendre les entreprises à de très grandes entreprises américaines, beaucoup plus importante que notre capacité à vendre nos entreprises à de grandes entreprises européennes. On est effectivement dans ce cercle vertueux d'un côté et vicieux de l'autre. Est-ce à cause des dividendes ? Il me semble que c'est d'abord une question de valorisation de ces grandes entreprises. Beaucoup de ces rachats se font en titres, et donc avoir une valorisation très importante permet d'acheter des entreprises sur une valeur importante en échangeant des actions. La question clé numéro un, c'est la valeur de nos grandes entreprises, leur volonté de prendre du risque, et la capacité du marché actions à évaluer l'opportunité de ces acquisitions. Il y a une dimension de maturité du marché actions pour juger de la bonne valeur d'une entreprise et de l'opportunité de l'achat d'une start-up elle-même très bien valorisée* ». Le même phénomène est relevé par M. Arthur Mensch : « *Les start-up vendent, dans un premier temps, aux autres start-up – car la course à la réussite, dans sa version venture capitalist, fonctionne de façon circulaire – puis aux autres entreprises américaines, qui sont énormes et peuvent rapidement acheter. Une fois qu'elles sont ainsi passées à l'échelle, elles exportent vers l'Europe, où aucun acteur n'a émergé à temps, et rachètent les quelques boîtes qui ont développé des compétences, ce qui leur permet de se consolider. C'est ainsi qu'elles absorbent tout le marché* ».

---

*(1) Audition de M. Henri Verdier, directeur général de la fondation Inria, ancien ambassadeur pour le numérique.*

*(2) Audition, ouverte à la presse, de M. Cédric O, ancien secrétaire d'État chargé du numérique, le 13 mai 2026.*

*(3) Audition, ouverte à la presse, de M. Arnaud Caudoux, directeur général adjoint de BPIFrance, M. Lionel Chaine, directeur des systèmes d'information, Mme Sophie Rémont, directrice en charge de l'expertise et des programmes au sein de la direction de l'innovation et M. Thierry Sommelet, directeur au sein de la direction du capital-développement, le 21 avril 2026.*

Mme Maya Noël décrit elle aussi la nécessité de disposer d'acteurs couvrant toutes les tailles d'investissement à réaliser : « *Dans notre modèle économique, les acteurs qui financent les fonds d'investissement en capital-risque ont besoin d'un retour sur investissement – c'est-à-dire une sortie de leur argent – dans les dix ans. Il faut donc que quelqu'un d'autre, disposant de plus d'argent et capable de racheter les parts, prenne le relais pour accompagner la poursuite de la croissance de l'entreprise. Or nous n'avons pas su construire ce réseau d'acteurs privés du financement capables de prendre le relais. Les acteurs américains sont les seuls en mesure de contribuer au recyclage de l'investissement* ». L'écosystème de la tech américaine est désormais très complet : un soutien de l'administration à travers des contrats de commande publique, un marché largement unifié sur lequel les entreprises peuvent se déployer rapidement et des acteurs financiers prêts à prendre des risques pour financer des entreprises innovantes, les succès passés contribuant à crédibiliser la perspective de rendements très importants.

## B. LA COMMANDE PUBLIQUE : UN INSTRUMENT ENCORE MAL MOBILISÉ

### 1. L'impossibilité d'utiliser un critère de préférence nationale, ou même européenne

Premier sujet, **la préférence française ou européenne n'est pas compatible avec les règles applicables dans la très grande majorité des cas**. Ce sujet a été pleinement traité par la commission d'enquête du Sénat sur les coûts et les modalités effectifs de la commande publique et la mesure de leur entraînement sur l'économie française [(1)]. Le rapport d'enquête insiste notamment sur la nécessité d'appliquer l'accord sur les marchés publics (AMP) conclu en 1994 sous l'égide de l'OMC et qui s'impose aux acheteurs publics en vertu du premier alinéa de l'article L. 2153-1 du code de la commande publique : *« L'acheteur garantit aux opérateurs économiques ainsi qu'aux travaux, fournitures et services issus des États parties à l'Accord sur les marchés publics conclu dans le cadre de l'Organisation mondiale du commerce ou à un autre accord international équivalent auquel l'Union européenne est partie, dans la limite de ces accords, un traitement équivalent à celui garanti aux opérateurs économiques, aux travaux, aux fournitures et aux services issus de l'Union européenne ».*

Le rapport du Sénat met toutefois en valeur l'adoption, dans le cadre de la présidence française de l'Union européenne, du règlement (UE) 2022/1031 du 23 juin 2022, dit « instrument relatif aux marchés publics internationaux (Impi) ». « *Ce règlement dote l'Union européenne d'un nouvel outil permettant de dissuader les États non-signataires d'un accord de libre accès mutuel à la commande publique de restreindre l'accès des opérateurs économiques européens à leurs propres contrats de la commande publique et de les inciter à conclure avec elle de tels accords. Il donne enfin une base expresse à la possibilité, pour les acheteurs et les autorités concédantes, de mettre directement en œuvre des mesures de*

*(1)* Ibid.

*traitement différencié et de restriction d'accès à la commande publique envers les entreprises des pays qui n'ont pas conclu un accord de libre accès et les offres originaires de pays tiers non couverts par un accord d'ouverture des marchés publics ou dont les biens, services ou travaux, ne sont pas couverts par un tel accord. Il sécurise en conséquence l'utilisation [du second alinéa] de l'article L. 2153-1 du code de la commande publique* ». Ce cas peut concerner par exemple la Chine ou l'Inde, non signataires de l'AMP, mais pas les États-Unis.

La rapporteure s'interroge sur le maintien anachronique de telles dispositions dans les droits européen et français. Comment continuer à justifier de telles contraintes dans un monde où l'Union européenne est la seule à les respecter ?

Le seul cadre dans lequel une préférence européenne est généralisée est celui des marchés de défense ou de sécurité (MDS), pour lesquels la logique est inversée. Le recours à des prestataires européens est le principe, l'extension à des candidats extra-européens l'exception. L'article L. 2353-1 du code de la commande publique dispose ainsi que « *les marchés de défense ou de sécurité, exclus ou exemptés de l'accord sur les marchés ou d'un autre accord international équivalent auquel l'Union européenne est partie, sont passés avec des opérateurs économiques d'États membres de l'Union européenne. L'acheteur peut toutefois autoriser, au cas par cas, les opérateurs économiques d'un pays tiers à l'Union européenne à participer à une procédure de passation. La décision de l'acheteur prend notamment en compte les impératifs de sécurité de l'information et d'approvisionnement, la préservation des intérêts de la défense et de la sécurité de l'État, l'intérêt de développer la base industrielle et technologique de défense européenne, les objectifs de développement durable, l'obtention d'avantages mutuels et les exigences de réciprocité.* »

Dans certains cas, des critères objectifs peuvent être mobilisés pour justifier le recours à des offres souveraines. Ainsi, le ministère de l'éducation nationale souligne que « *des clauses d'immunité au droit non-européen à portée extraterritoriale ont cependant pu être utilisées dans des marchés récents de services à hébergement externalisé, sans contestation devant le juge à ce jour. Il faut cependant noter que l'existence du cadre de protection des données à caractère personnel (*Data Privacy Framework*) entre l'Europe et les États-Unis, entré en vigueur le 10 juillet 2023 et qui, contrairement aux deux accords précédents (Safe Harbor et Privacy Shield) n'a pas été invalidé par la Cour de justice de l'Union européenne (arrêts Schrems), rend juridiquement délicate l'exclusion d'une solution états-unienne pour des motifs d'incompatibilité au RGPD. L'article 31 de la loi SREN vient certes sécuriser le recours à des solutions en nuage souveraines labellisées SecNumCloud pour les SI traitant de données "d'une sensibilité particulière", mais il est limité à des cas très circonscrits nécessitant des très hauts niveaux de sécurité.* »

### 2. Les difficultés des PME et ETI à accéder aux marchés publics

**Second sujet, la part des PME et des ETI du numérique dans les achats publics est faible, empêchant ainsi d'en faire un tremplin pour elles.** Ainsi que l'ont montré les chiffres de Numeum, le tissu économique des fournisseurs de logiciels français est composé de peu de grandes entreprises. La participation des PME et de ETI aux achats publics devrait donc constituer une priorité pour soutenir le développement de la filière. Qu'en est-il dans la réalité ?

Le rapport de l'observatoire des relations entre start-ups et grands comptes, publié par le Médiateur des entreprises, fournit des indications chiffrées sur l'évolution des achats des administrations et des grands groupes auprès des start-up et des scale-up françaises (1).

Au rang des satisfactions, les achats publics auprès des start-up ont fortement augmenté entre 2022 et 2023, passant de 1,7 à 2,3 milliards d'euros. Ce montant est désormais comparable à celui des achats passés par les 39 grands groupes privés interrogés. Sur le périmètre de la direction des achats de l'État, la hausse est de près de 50 %. On note donc un effort significatif de rattrapage.

**ÉVOLUTION DES ACHATS AUPRÈS DES START-UP ENTRE 2022 ET 2023**

*En M€*

| | 2022 | 2023 | Progression |
|---|---|---|---|
| Achats publics | 1 746 | 2 329 | + 33 % |
| Ugap | 179 | 241 | + 35 % |
| Grands groupes | 2 330 | 2 441 | + 4 % |

*Source : Médiateur des entreprises.*

Toutefois, plusieurs indicateurs témoignent encore d'une relation distendue :

– si l'on s'intéresse au poids relatif des achats auprès des start-up, force est de constater qu'ils sont encore très marginaux dans le total des achats réalisés : 1,4 % des achats totaux des administrations, et 2,0 % des achats des grands groupes ;

– 49 % des entreprises numériques interrogées ne réalisent pas de chiffre d'affaires avec des administrations, et les achats publics comptent pour moins de 20 % de leur activité pour 73 % d'entre elles. Parmi les administrations concernées, ce sont les collectivités territoriales qui sont les plus actives, avec 44 % des acheteurs. Les ministères ne comptent que pour 20 % ;

– pour les contrats signés avec des administrations, la part des contrats de moins de 5 000 euros est majoritaire (56 %). Les contrats supérieurs à 100 000 euros ne représentent que 9 % du total.

---

*(1) Médiateur des entreprises, Rapport 2025 de l'observatoire des relations entre start-ups et grands comptes, février 2026*

*https://www.economie.gouv.fr/mediateur-des-entreprises/le-rapport-2025-de-lobservatoire-des-relations-entre-start-ups-et-grands-comptes*

Comment expliquer cet état de fait ?

La politique des achats des ministères ne comprend pas de dispositifs réellement ambitieux, taillés pour faciliter l'accès des marchés aux PME et aux ETI. Comme le décrivent les réponses aux questionnaires adressés aux administrations, le seul véritable effort réalisé est l'allotissement des marchés. « *[Les marchés publics conduits par le ministère] sont pour la plupart allotis, quand l'allotissement ne présente pas un risque dans l'exécution du marché. L'allotissement peut être fait par périmètres fonctionnel ou technique. Cet allotissement a pour objectif principalement d'ouvrir à la concurrence nos marchés mais également de favoriser l'accessibilité des marchés du ministère de la justice aux PME et ETI, si besoin, dans le cadre d'un groupement ou dans une relation de sous-traitance* » [(1)]. Pourtant des cadres juridiques tels que le partenariat d'innovation existent pour faciliter l'accès des PME et ETI ainsi que la commission d'enquête sénatoriale le démontrait.

Par ailleurs, il apparaît que la qualité technique des produits n'est pas du tout en cause. Bien au contraire, ces entreprises sont saluées pour leur expertise et leur capacité à développer des innovations technologiques à un rythme rapide, parfois davantage que les grands éditeurs internationaux.

Dans le secteur de la défense, par exemple, « *la qualité de l'offre française, que ce soit en innovation et qualité est jugée d'excellente facture pour les logiciels métiers. La France dispose d'un maillage relativement dense d'éditeurs spécialisés de défense, certes souvent de taille modeste mais prenant 44 % des dépenses des éditeurs et majoritaire sur les logiciels métiers. Masagroup (simulation), Preligens (IA) peuvent être cités. Cette offre logicielle est complétée par une offre de développement, d'intégrateurs et de tierce maintenance massivement française (+ de 80 %) et cette fois-ci de taille internationale (Capgemini, Sopra Steria, etc…)*

« *L'offre française se différencie également par une meilleure prise en compte des exigences de souveraineté, de sécurité et de conformité, ainsi que par une qualité de support plus proche et personnalisée.* » [(2)]

Selon la direction générale de la gendarmerie nationale, « *l'offre française se montre souvent compétitive, à des niveaux suffisants pour la sécurité intérieure, dans de nombreux domaines. Plusieurs éditeurs proposent ainsi des offres très concurrentielles pour le Low Code No Code (exemple de la PME française Ksaar retenue comme solution de référence par l'Anfsi)* ». Plusieurs entreprises françaises ont été retenues par le ministère de l'intérieur pour équiper les postes de travail : *The greenBow* déployant le « VPN français », *WAPT* – logiciel de déploiement, de mise à jour et de suppression automatisé des paquetages Windows, Linux et MacOS –, *Wallix* pour les bastions de sécurité, *PrimX* pour le chiffrement des postes.

---

*(1) Réponse aux questionnaires de la rapporteure, ministère de la justice.*

*(2) Réponses aux questionnaires de la rapporteure, Commissariat au numérique de défense.*

La faible présence des PME et des ETI du numérique dans la commande publique s'explique par l'incapacité de chacune des parties à répondre aux problématiques structurelles de l'autre partie.

Du côté des PME et des ETI, alors que le sujet de la trésorerie est capital dans des phases d'amorçage, celles-ci soulignent la lenteur du cycle de vente pour 65 % d'entre elles (1) ou encore des délais de paiement trop longs (28 %). Le délai entre le premier contact avec une administration et une contractualisation est de 32 semaines en moyenne, et de 46 semaines pour un premier paiement. Cela signifie que les entreprises doivent porter intégralement les coûts de démarchage commercial et de développement de produit pendant une durée de presqu'un an.

Du côté de l'administration, le principal frein tient à la crainte de confier la responsabilité du déploiement d'un produit à une structure n'en ayant pas les capacités techniques et financières. Les produits ne sont parfois pas suffisamment aboutis pour constituer le socle d'un déploiement industriel, et les équipes techniques peuvent ne pas être suffisamment armées pour affronter la complexité de systèmes d'information de très grande taille. Ainsi que l'indique l'AP-HP, « *globalement, nous disposons plutôt de logiciels métiers français ou européens, assez compétitifs en termes de coût – notamment poussés par la concurrence – mais parfois immatures en termes de produit ou d'innovation. Si certains marchés exigent une taille critique permettant d'éviter des échecs projet liés à des entreprises n'ayant pas la capacité de réussir opérationnellement, nous positionnons souvent ces seuils assez bas pour permettre aux ETI/PME de candidater, notamment en groupement ou comme sous-traitants. À titre d'exemple, l'AP-HP a octroyé un marché significatif (solution de gestion des lits) à un jeune éditeur nantais dénommé Silbo, non sans difficultés opérationnelles pour ensuite assurer un déploiement effectif à un niveau de taille et de complexité que celui de l'AP-HP* » (2). Le ministère de l'éducation nationale porte le même diagnostic (3) : *« L'offre française apparaît riche, diversifiée et globalement compétitive, avec un tissu d'acteurs allant des grands groupes aux PME et ETI innovantes. Elle présente des atouts structurants pour l'action publique : une maîtrise des architectures ouvertes et interopérables, largement fondées sur des composants open source, une expertise solide sur les technologies standards (Java, Python, etc.), permettant de concevoir des systèmes durables, une contribution directe aux enjeux de souveraineté numérique, en limitant les dépendances aux solutions propriétaires étrangères. Des différences existent néanmoins entre acteurs, notamment en matière de capacité industrielle de passage à l'échelle pour un ministère comme celui de l'éducation nationale, de spécialisation métier et de maturité sur les exigences de sécurité et de qualité de service. Ces écarts structurent les stratégies d'achat public.* »

---

*(1) France Digitale et EY, Baromètre sur la performance économique et sociale des start-ups et fonds de capital-risque français, édition 2023. Cité par Sénat.*

*(2) Réponse aux questionnaires de la rapporteure, AP-HP.*

*(3) Réponse aux questionnaires de la rapporteure, Ministère de l'éducation nationale.*

Le ministère de la culture souligne le handicap structurel que constitue la taille des équipes : « *Les PME sont parfois moins à l'aise avec les exigences de la commande publique et leur compréhension de ces standards de qualité. Leur taille les rend également structurellement moins apte à absorber des pics de charge et donc d'offrir un niveau support toujours réactif. En revanche, sectoriellement elles ont parfois des niveaux d'expertises que l'on ne retrouve pas chez les grandes entreprises du secteur du numérique. Les PME qui font l'effort de se conformer aux standards de qualité pour le ministère en tirent généralement un avantage concurrentiel auprès d'autres administrations.* » (1)

Les interrogations portent aussi sur la pérennité de la structure dans la durée. Les clauses destinées à protéger l'administration en cas de non-exécution ou de délais de réalisation trop longs (garanties bancaires, pénalités, etc.) peuvent être rédhibitoires. Ainsi que l'exprime la DGDDI, « *l'offre en France est très diversifiée, innovante et performante mais manque de maturité, avec une difficulté à contractualiser pour adresser un engagement de long terme (capacité d'intégration, de niveau de service en termes de support). Les exigences sont fortes et peuvent mettre en difficulté la santé de l'entreprise.* » (2)

M. Antoine Duboscq, président de Wimi, pointait également du doigt devant la commission d'enquête la crainte des grandes administrations à travailler avec des acteurs de petite taille (3) : « *Le dernier obstacle à franchir pour la France est culturel : c'est la capacité des grands acteurs à travailler avec les petits. Les Américains savent le faire. Ils savent favoriser leurs grands acteurs, mais ils savent aussi confier des contrats majeurs à de petites entreprises, comme on l'a vu en biotechnologie ou dans le numérique, grâce à des instruments tels que la Defense Advanced Research Projects Agency (Darpa). L'Allemagne le fait aussi, avec un modèle qui a permis l'émergence d'entreprises de taille intermédiaire (ETI), trois à quatre fois plus nombreuses qu'en France.*

« *Cette difficulté culturelle des grands à travailler avec les petits peut être surmontée avec un coup de pouce de l'exécutif et du législatif. Il faut encourager les décideurs de terrain – acheteurs, DSI, dirigeants – à oser franchir le pas. Les accords que Wimi a noués avec Atos, Thales, La Poste ou le Centre scientifique et technique du bâtiment (CSTB), avec qui nous avons créé une coentreprise, sont des exemples de succès qui montrent qu'il n'y a pas de fatalité. Il reste des réticences, des peurs, mais les raisons invoquées sont souvent des paravents. Lorsque l'on entend un haut fonctionnaire déclarer ne pas vouloir discuter avec des sociétés de moins de 2 000 personnes, on voit que ce frein est avant tout dans les esprits ».*

Faisant le même constat, le ministère de l'intérieur s'efforce de montrer des partenariats destinés à accompagner les entreprises françaises dans leur montée en puissance technique, dans une démarche « gagnant-gagnant » puisque le ministère

---

*(1) Réponse aux questionnaires de la rapporteure, ministère de la culture.*

*(2) Réponse aux questionnaires de la rapporteure, ministères économiques et financiers.*

*(3) Audition, ouverte à la presse, du collectif #Fab8, représenté par MM. Antoine Duboscq, président de Wimi, Thomas Fauré, président de Whaller et Alain Garnier, président de Jamespot, le 29 avril 2026.*

profite ainsi de produits alors très performants : « *En termes de compétitivité, les offres « éditeurs » françaises sont plutôt attractives car elles sont souvent représentées par des entreprises de tailles intermédiaires, voire de petites entreprises ou start-up. La croissance de celles-ci se fait soit sur un modèle très progressif, avec une exposition à des clients de plus en plus variés ou une spécialisation sur une typologie de clients (privé versus publics ; secteur banque assurance versus santé…), soit sur un modèle de croissance externe plus ou moins rapide [comme par exemple l'entreprise Chapsvision].*

« *Ces modèles en font des partenaires particulièrement intéressants pour la réalisation de POC (preuve de concept) mais sont parfois difficiles à monter à l'échelle en vue d'une industrialisation. Il existe cependant des partenariats qui nous permettent de tisser des relations durables et resserrées au profit d'un périmètre métier particulier, par exemple l'alerte aux populations, où nous faisons le choix d'investir sur une solution française au départ peu utilisée et dont nous co-construisons une solution pérenne et soutenable aux bénéfices et de l'État et de l'éditeur français.*

« *Enfin, il est à noter que* ***sur la majorité de nos périmètres métiers, ces petites entreprises sont particulièrement compétitives techniquement****. Elles sont en effet dotées d'une forte agilité, c'est-à-dire d'une capacité de prise en compte des demandes d'évolution de manière extrêmement rapide, ainsi que d'une forte ingénierie en recherche et développement, ce qui produit des solutions très innovantes les différenciant ainsi de beaucoup d'acteurs majors du marché.* »

La commande publique pourrait donc davantage recourir à des entreprises innovantes, puisque la qualité de leur offre technique est attestée.

### 3. Quelle articulation entre commande publique et soutien public au titre de la politique industrielle ?

La politique de soutien à la filière industrielle du numérique passe surtout par le soutien à l'amorçage, via des prises de participation ou des subventions. La commande publique vise quant à elle à répondre aux besoins de la puissance publique. L'enjeu est d'améliorer l'articulation entre ces deux politiques lorsque celles-ci ont des intérêts conjoints.

Les témoignages des ministères soulignent la nécessité de s'adresser à des entreprises de taille suffisante pour pouvoir mener à bien des projets de grande ampleur et donner des garanties de stabilité sur le long terme. Les financements d'amorçage devraient jouer précisément ce rôle : contribuer à solvabiliser les entreprises dont la technologie est jugée très prometteuse, de façon à ce qu'elle puisse s'adresser aux grands comptes à même de lui garantir des revenus suffisants pour entamer une croissance rapide.

**Tout d'abord, parmi l'ensemble des administrations d'État interrogées, seul le ministère de la défense indique collaborer avec la direction**

**générale des entreprises (DGE) pour préparer le tissu industriel en amont**. Le Commissariat au numérique de défense échange avec la DGE sur les besoins clés et les entreprises présentant les plus avancées technologiquement, participe aux comités de sélection et contribue éventuellement aux financements via des prises de participation ou d'autres moyens, en particulier la facilitation d'accès à des contrats-cadres [(1)]. « *Dans le domaine du numérique, comme dans tous les autres domaines économiques touchant à la souveraineté, le ministère des armées entretient des échanges réguliers avec la Direction générale des entreprises (DGE) ainsi qu'avec tous les autres organismes publics impliqués dans la politique industrielle, les relations avec les entreprises et le suivi des acteurs économiques par l'Etat. Ces échanges, assurés notamment par la direction de l'industrie de défense de la Direction générale de l'armement (DGA), contribuent à entretenir la vision du paysage industriel français, à optimiser les dispositifs de soutien industriel sur les priorités de sécurité du ministère, et à renforcer la performance et la résilience des filières critiques. Par ailleurs, ces échanges contribuent à l'optimisation de la commande publique et à la juste utilisation des moyens de l'Etat, tout en tenant compte des spécificités des besoins de la défense nationale et des armées comme des autres acteurs étatiques de la souveraineté.*

« *Afin de structurer sa relation avec la base de ses fournisseurs actuels et potentiels (entreprises du numérique de défense), le Collège défense et numérique (CND) s'appuie sur les fédérations et organisations professionnelles et associations existantes (notamment GICAT9, GIFAS10, GICAN11, Hexatrust, Collège Défense et Numérique), ainsi que sur les pôles de compétitivité dans le numérique (SYSTEMATIC, par exemple) pour organiser des échanges structurés autour des priorités stratégiques et technologiques.*

« *Il s'agit de permettre aux entreprises du numérique de défense, en particulier les PME offrant des solutions souveraines et innovantes, de mieux connaître l'organisation et les besoins du numérique de défense ainsi que les opportunités en termes de marchés publics et, le cas échéant, de se regrouper pour y répondre. À cet effet, le CND organise des webinaires de présentation du numérique de défense au profit de ces entreprises, ainsi qu'un évènement annuel, le Séminaire du numérique de défense, qui rassemblera plus de 500 entreprises et l'ensemble des entités du numérique de défense pour échanger autour des projets et besoins futurs* ».

Le ministère de l'Europe et des affaires étrangères fait même le constat : « *Les interactions entre la Délégation au numérique (DNUM) du ministère de l'Europe et des Affaires étrangères (MEAE) et la DGE sont actuellement très limitées. À ce jour, une seule interaction a eu lieu en novembre 2025 dans le cadre de la mission sur l'évolution des capacités d'hébergement numérique de l'État.*

« *Lors de cet échange, le MEAE a souligné la criticité de ses infrastructures, notamment en tant qu'opérateur SI de l'État à l'étranger, délégataire de service pour*

*(1) Réponse aux questionnaires de la rapporteure, Commissariat au numérique de la défense*

*le classifié à l'étranger par l'OSIIC, et dans un contexte de diffusion restreinte nécessitant des capacités de calcul IA interne. Nous avons également rappelé que, malgré la taille relativement modeste de nos locaux techniques, il était essentiel d'être considéré comme un opérateur critique pour l'État. Nous avons mis en garde contre une mutualisation qui pourrait s'avérer plus coûteuse au regard des systèmes d'information mis à disposition sur l'ensemble de nos emprises à l'étranger et du niveau de service apporté. À ce jour, nous n'avons reçu aucun retour concernant les conclusions de cette mission* ».

Ensuite, **parmi les sociétés ayant fait l'objet d'une prise de participation de la part de BPIFrance** (voir *infra* la liste des participations dans les domaines de l'intelligence artificielle, des logiciels et de la cybersécurité), **seules Mistral AI et Chapsvision ont été recensées par l'administration comme fournisseurs de logiciels métiers stratégiques**. La troisième société, Ciril group, présente la particularité de s'adresser spécifiquement aux administrations. BPIFrance note ainsi que ses participations « *rencontrent en effet très souvent une concurrence de la part de solutions non-européennes. Bpifrance a mis en place un dispositif d'accompagnement opérationnel auprès de ses participations permettant de leur apporter un appui : appui direct par la mise en relation avec des clients potentiels (appui de type "business development"), appui sur des consultants externes pour aider à l'amélioration de l'organisation et des process de vente et de marketing... De manière complémentaire, Bpifrance mène une action plus systémique auprès des directions achats des grands groupes (programme DAPI – Direction Achats Pour l'Innovation) visant à renforcer l'achat innovant et la collaboration entre grands groupes et startups innovantes.* » Toutefois, il n'existe pas de stratégie coordonnée entre l'État dans son rôle d'actionnaire et les administrations prescriptrices et futures acheteuses.

La rapporteure note qu'il aura cependant fallu un scandale international – la suppression de l'accès à Mythos 5 et Fable 5 – pour que le gouvernement mette fin à son partenariat avec Palantir et lui substitue une collaboration avec Chapsvision.

Dans d'autres domaines, les start-up soutenues par le ministère de l'économie ne correspondent pas toujours aux attentes, aux besoins ou aux moyens des acteurs publics. C'est le cas par exemple des technologies éducatives dont le modèle tarifaire ne correspond pas aux moyens du public, comme indiqué par M. Audran Le Baron lors de son audition [(1)] : « *En ce qui concerne les EdTech, il y a eu une politique interministérielle volontariste portée par la DGE, le secrétariat général pour l'investissement (SGPI) et le ministère de l'éducation nationale, pour créer un écosystème d'entreprises françaises privées en pointe en matière de numérique, au service de l'éducation et de la pédagogie. Pour l'heure, il est principalement constitué de petites start-up relativement fragiles d'un point de vue économique, mais offrant des services à l'état de l'art – voire en pointe –, qui rivalisent avec les autres offres, y compris à l'échelle internationale. Néanmoins, nous sommes confrontés à un problème budgétaire. Le modèle tarifaire des éditeurs*

*(1) Table ronde, ouverte à la presse, réunissant des directeurs de systèmes d'information de ministères, le 9 avril 2026.*

*privés, dont nous avons contribué à faire naître l'offre grâce à des Piia (partenariats d'innovation en intelligence artificielle) – nous avons de nombreux marchés publics innovants à cette fin –, est généralement fondé sur un abonnement annuel. Or, avec 900 000 professeurs, les chiffres ont tendance à monter très vite.* »

Enfin, **la question s'est posée, de manière assez vive, pour les projets faisant l'objet d'un soutien par des subventions. Le cas le plus emblématique est celui des suites collaboratives.**

En 2023, trois lauréats sont sélectionnés pour le développement de suites collaboratives dans le cas d'un appel à projets « Développement de suites bureautiques ». L'objectif est ainsi de se positionner comme des alternatives souveraines crédibles à Microsoft Office 365 et Google Workspace. Le montant total des aides attribuées aux trois consortiums s'élève à 23 millions d'euros, dont deux tiers de subventions et un tiers d'avances remboursables. À ce jour, le taux de décaissement est de 76 %, ce qui témoigne de l'avancement de chacun des trois projets. Ainsi que l'indique BPIFrance [(1)], « *globalement, l'avancement technique est conforme à ce qui était prévu, avec des avancées commerciales pour l'un des projets bien qu'il soit encore en cours.* »

La question de la potentielle concurrence entre les solutions souveraines portées par ces sociétés françaises et les produits développés par la Dinum a inévitablement été évoquée lors des différentes auditions de la commission d'enquête, témoignant d'une véritable crispation chez les acteurs de la filière. M. Alain Garnier, président de Jamespot, résume le point de vue des entreprises françaises développant des alternatives souveraines aux produits collaboratifs de Microsoft [(2)] : « *Je ne peux passer sous silence le fait qu'en 2022, l'État a initié une véritable politique industrielle en lançant un appel à projets France 2030, bien doté, pour les suites bureautiques alternatives. Trois lauréats ont été désignés : Wimi, Jamespot et Interstis. Cependant, alors que cette politique industrielle était enclenchée, l'État a opéré un changement de cap en développant une offre étatique unifiée, nommée LaSuite. Cette initiative a entraîné une réduction de fait de la place du marché, un manque de visibilité sur l'articulation des offres et d'importantes frictions, qui n'ont été que difficilement résolues par des arbitrages ministériels successifs. Pourquoi passer d'un modèle de soutien à un écosystème de filière, qui a fait ses preuves partout dans le monde, à un modèle de production centralisée ?*»

Les éditeurs de logiciel font valoir les arguments suivants :

– d'une part, ils questionnent la capacité de la Dinum à fournir le support nécessaire dans la durée, et à assurer le déploiement de solutions à de grandes échelles ;

---

*(1) Réponse aux questionnaires budgétaires.*

*(2) Audition, ouverte à la presse, du collectif #Fab8, représenté par MM. Antoine Duboscq, président de Wimi, Thomas Fauré, président de Whaller et Alain Garnier, président de Jamespot.*

– d'autre part, ils reprochent à cette dernière de capter une partie du marché que les éditeurs français pourraient utiliser afin de faire croître leur offre : « *L'enjeu n'est pas de chasser Microsoft de France ou d'Europe, mais de rééquilibrer sa position de domination dans les outils collaboratifs, mais aussi dans d'autres domaines, par exemple la gestion de l'identité ou les postes de travail équipés avec Windows. Pour cela, il faut aménager des zones protégées où la filière pourra reprendre des forces.* »

Cependant, le développement des outils de la suite numérique par la Dinum répond à des objectifs structurels, tel que l'expose M. Henri Verdier, initiateur de cette stratégie lorsqu'il dirigeait la Dinsic. « *Mon objectif était de réintroduire au sein de l'administration des méthodes agiles, des politiques publiques fondées sur la donnée (data-driven policies), le développement dit DevOps, ainsi que des pratiques de ressources humaines capables d'attirer une plus grande diversité culturelle et des profils rares ou atypiques. J'étais convaincu – et je le maintiens – que lorsqu'une organisation ne sait plus produire elle-même, elle ne sait plus acheter. Je pourrais citer des dizaines d'exemples de factures vingt fois trop chères, simplement parce que les achats avaient été réalisés à l'aveugle (…). L'État n'avait strictement rien produit lui-même. À un moment donné, la faiblesse insigne de l'État constitue en elle-même un problème.* » [(1)]

M. Henri Verdier signale également l'écart de coût entre les solutions que l'État est capable de développer et les propositions commerciales des acteurs privés : « *L'État n'a pas vocation à se substituer au secteur privé et il n'a jamais été question qu'il devienne, par exemple, un opérateur de cloud. En revanche, dans certaines situations, il faut être capable de faire bouger les lignes. J'en veux pour exemple la messagerie instantanée Tchap, que j'ai contribué à lancer. Ce service, réservé aux fonctionnaires, coûte aujourd'hui 11 centimes par an et par agent public. Il compte 400 000 utilisateurs hebdomadaires sur un potentiel de deux millions de fonctionnaires, dont tous n'ont pas besoin d'une messagerie. On peut considérer qu'il s'agit d'un succès raisonnable. À l'époque où je dirigeais la Dinum, la meilleure offre s'élevait à 20 euros par an et par agent public. Face à un tel écart, il me paraît légitime que l'État envisage une autre stratégie, en soutenant, par exemple, un éditeur de logiciel libre pour qu'il améliore son produit. S'il est évident que l'État a un rôle à jouer dans le dynamisme économique du pays en soutenant les entreprises françaises – je parle en connaissance de cause pour en avoir moi-même créé trois –, il doit les aider à réussir dans la compétition internationale, non les placer dans une situation protégée, à l'abri de toute concurrence, en pratiquant des tarifs trop éloignés des prix de marché. Dans un tel contexte, elles risqueraient de ne jamais trouver d'autres clients. L'exemple de Tchap n'est pas complètement honnête puisqu'il compare une offre datant d'une dizaine d'années avec un service aujourd'hui stabilisé. Néanmoins l'écart de prix était à l'époque considérable, de l'ordre d'un facteur dix.* »

---

*(1) Audition de M. Henri Verdier, directeur général de la fondation Inria, ancien ambassadeur pour le numérique, le 10 mars 2026.*

Pour Mme Stéphanie Schaer, directrice interministérielle du numérique, il est clairement établi que la Dinum n'a pas vocation à devenir un éditeur de logiciels à part entière. Les administrations sont ainsi laissées libres de choisir leurs propres solutions, qui peuvent embarquer des briques logiciels open source développées par la Dinum : « *Il a été clarifié auprès de la filière qu'il n'y avait pas d'exclusivité : chaque ministère peut acheter une solution de marché, nous n'allons pas imposer nos éléments. Docs et Grist, qui sont encore en phase expérimentale, ne remplacent de toute façon pas les outils bureautiques habituels, ils apportent un complément pour répondre aux usages spécifiques des administrations. Nous voulons simplement tirer l'offre vers le haut, en donnant sa place à chacun : c'est tout l'intérêt des connecteurs et de l'interopérabilité dont je parlais tout à l'heure. Les outils de la filière devront communiquer entre eux, ainsi qu'avec Visio et Tchap. C'est le cœur des travaux actuels.*

« *Il y a eu des incompréhensions sur la façon dont la Dinum avait construit son offre, qui permet à l'État d'avoir davantage de maîtrise sur les outils comme Tchap et Visio qui assurent la continuité de l'action publique grâce à une offre qui soit à la hauteur des enjeux de l'environnement géopolitique actuel. Pour cela, nous opérons des briques qui doivent ensuite s'articuler avec l'ensemble de l'écosystème. On a dit que la Dinum devenait un éditeur de logiciels. Ce n'est pas notre positionnement : la Dinum opère des briques en open source. En revanche, nous nous autorisons à contribuer à ces briques car il n'y a rien de mieux que cela pour maintenir l'expertise des équipes, renforcer l'attractivité du recrutement et garantir la maîtrise des outils et du code ».* C'est notamment le cas du produit développé par Linagora, et cité par la direction générale de la gendarmerie nationale : « *Pour les outils collaboratifs, l'ETI français Linagora apporte une solution avec un très bon niveau de maturité (plateforme Twake AI) tout en combinant des développements internes avec l'intégration de briques en logiciel libre existantes : OnlyOffice pour la coédition en ligne, Grist pour une solution évoluée de tableur en Low Code No Code, OpenProject pour la gestion de projets, ou les offres de la DINUM (eg Visio, Tchap).* » (1)

La rapporteure constate finalement que les administrations sont satisfaites des produits développés par la Dinum, qui viennent remplacer des briques de produit fournies par le marché. La contribution du ministère de la justice résume bien cette situation (2) : « *S'agissant des outils de la DINUM, même si des progrès sont évidemment possibles sur la qualité de service, le service fourni par les différents produits est de bonne qualité, et répond à un vrai besoin, tout en assurant un très bon niveau de souveraineté : réseau interministériel de l'État, FranceConnect pour l'authentification des usagers sur les services en lignes, ProConnect, Tchap, demarches-simplifiees, Sur d'autres produits plus émergents, la couverture des besoins et le niveau de qualité de service peut être moindre, mais il est bien compris que c'est normal, car en appliquant des méthodes de type « lean*

*(1) Audition, ouverte à la presse, de Mme Stéphanie Schaer, directrice interministérielle du numérique (Dinum), et M. Jérémie Vallet, son adjoint, le 14 avril 2026.*

*(2) Réponses au questionnaire de la rapporteure, Ministère de la Justice.*

*start-up » la DINUM privilégie dans un premier temps la recherche d'impact et d'adhésion des utilisateurs en remettant l'industrialisation et la complétude de la couverture des besoins à des phases ultérieures. Un des intérêts principaux des logiciels interministériels est la capacité pour les ministères à renoncer à toute solution ministérielle, ce qui permet une économie globale à l'échelle de l'État mais repose sur la fiabilité de l'offre DINUM, sa résilience et la confiance qu'elle peut donner.* ».

Aux dires des éditeurs de logiciels indépendants, le déploiement des outils de la Dinum aurait porté un coup important à leur activité. Il ne faut tout de même pas occulter le fait que les financements publics alloués aux trois consortiums s'élèvent à 17,6 millions d'euros, dont 11,7 millions de subventions. Le président de Jamespot a indiqué que sa société tirait 40 % de ses revenus du secteur public, grâce à des acteurs tels que la Cnam.

Le soutien à des projets et des entreprises innovantes comporte une part de risques, et il convient donc d'accepter par nature l'échec de projets qui auront été financés. L'attribution de subventions à des acteurs émergents ne doit pas valoir promesse de contrats publics, les besoins des administrations devant primer.

La rapporteure constate que l'État soutient de manière volontariste et pour des sommes significatives les éditeurs français. Elle souligne la nécessité dès lors d'une politique ouvrant davantage le marché de la commande privée à ces solutions souveraines, comme à l'ensemble des solutions bénéficiant d'aides publiques. En effet, la commande publique ne représentant qu'une faible part de l'ensemble du marché du numérique, elle ne pourra répondre seule au développement de solutions souveraines.

## C. LES PRISES DE PARTICIPATION DANS LES ENTREPRISES DU NUMÉRIQUE : LE RISQUE DE LA NAÏVETÉ

### 1. Le constat récurrent de l'insuffisance du marché des capitaux

À l'automne 2024, M. Mario Draghi, ancien président de la Banque centrale européenne, remettait à Mme Ursula von der Leyen son rapport sur le futur de la compétitivité de l'Europe [(1)]. Ce rapport pointait du doigt deux freins essentiels : la fragmentation du marché des capitaux à l'échelle européenne et la part insuffisante des fonds de pension, représentant seulement 32 % du PIB européen contre 142 % aux États-Unis. Cette situation conduisait à faire reposer le financement de l'innovation majoritairement sur des outils bancaires, peu adaptés à des actifs risqués et contraints par les règles prudentielles.

(1) *Mario Draghi,* Le futur de la compétitivité européenne, *septembre 2024* https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf

De façon convergente, les représentants des institutions publiques chargées du financement de l'économie conviennent de la difficulté à financer des opérations pour la phase dite de *scale-up*, c'est-à-dire celle durant laquelle les besoins en financement dépassent la centaine de millions d'euros. Mobiliser des fonds est ainsi devenu une priorité d'action.

Pour M. Thomas Courbe, directeur général des entreprises, « *le déficit massif de capital-risque privé en Europe est un fait largement documenté, dont les causes sont multiples. Pour y remédier, nous sommes convaincus de la nécessité d'une approche globale, agissant de front sur la mobilisation prudentielle des capitaux et sur l'orientation des investissements privés à travers des initiatives publiques. L'initiative Tibi a déjà produit d'excellents résultats et nous entrons désormais dans une phase d'européanisation, marquée notamment par le lancement d'un fonds par la Commission. En France, si l'amorçage et le stade A sont relativement bien pourvus par le marché privé, les difficultés apparaissent lors des phases de croissance, aux stades B et C. C'est précisément sur ce segment que nous concentrons nos efforts, car cette faille de marché influence directement les choix stratégiques des entreprises, et singulièrement leur localisation.* » (1)

Pour M. Benjamin Delozier, chef du service des politiques écologiques et sectorielles à la direction générale du Trésor, « c*oncernant le financement, je partage le constat selon lequel les principales difficultés de nos start-up technologiques dans leur passage à l'échelle se concentrent sur le late stage, malgré le dynamisme de notre écosystème entrepreneurial. Pour y répondre à l'échelle nationale, l'initiative Tibi, coordonnée par la direction générale du Trésor depuis 2020, mobilise l'épargne des investisseurs institutionnels français vers ce segment. Ce dispositif repose sur l'homologation de fonds spécialisés répondant à un cahier des charges exigeant, ce qui favorise l'acculturation des investisseurs à cette classe d'actifs. Les résultats sont probants puisqu'en 2026, l'initiative a mobilisé plus de 14 milliards d'euros d'investissements privés, avec un objectif porté à 15 milliards. Sur les 160 fonds homologués, une majorité se consacre au capital-croissance et à la deep tech, secteur qui capte désormais 27 % des investissements (biotech, énergie, cybersécurité, IA ou quantique) et a permis de décupler la part des levées de fonds en phase de scale-up. La deuxième phase, déployée entre 2023 et 2026, a élargi son périmètre à l'early stage ainsi qu'aux transitions écologique et numérique, avec plus de 7 milliards d'euros investis dès la fin 2025.* »

*(1) Audition commune, ouverte à la presse, de MM. Benjamin Delozier, chef du service des politiques écologiques et sectorielles à la direction générale du Trésor, et Victor Amoureux, chef du bureau concurrence, numérique, économie du logement, MM. Thomas Courbe, directeur général des entreprises (DGE), et Loïc Duflot, chef du service de l'économie numérique et de M. Florent Kirchner, directeur du pôle souveraineté numérique au secrétariat général pour l'investissement (SGPI), le 7 mai 2026.*

Enfin, pour Mme Catherine Mayenobe, directrice générale déléguée de la Caisse des dépôts [(1)], directrice des opérations et du pilotage de la transformation opérationnelle, « *[Le] manque de profondeur et [la] fragmentation des marchés de capitaux en Europe commencent à être assez bien documentés, je pense notamment aux rapports de MM. Draghi et Noyer. Il nous est difficile d'estimer les pertes en actifs stratégiques. Vous avez cité Criteo, mais ce que nous constatons de façon empirique, c'est qu'au-delà de 100 millions d'euros, une entreprise ne trouve pas sur les marchés européens de quoi financer sa croissance.*

« *Ce scale-up peut être compensé par des introductions en bourse (IPO), mais ce n'est pas une solution envisageable pour toutes les entreprises, qui n'ont pas toutes la maturité ou la solidité de gouvernance nécessaire. Pour vous répondre rapidement, cette fragmentation des marchés de capitaux, ce manque de profondeur et le fait que nous ayons autant de bourses que d'États membres nous semblent un véritable frein au développement des entreprises technologiques en Europe et à leur passage à l'échelle.* »

Malgré les différentes mesures pour favoriser la cotation des sociétés de la tech en France, les opérations d'introduction en bourse sont rares à Paris depuis 2021. Des facteurs exogènes liés à la conjoncture économique expliquent une partie de ce constat, mais des facteurs propres à la situation de ces sociétés sont également en cause. D'une part, les profils financiers sont souvent insuffisamment matures au regard des attentes des investisseurs boursiers. D'autre part, la période des années 2020-2022 a conduit à des niveaux de valorisation historiques, qui sont encore trop élevés comparés à ce que les marchés pourraient proposer aujourd'hui. Le tableau ci-après montre ainsi que le nombre d'introductions en bourse pour des entreprises de logiciels et de cloud sur Euronext Paris a fortement ralenti depuis la période 2020-2021. Entre juin 2022 et novembre 2024, seules trois opérations dans le domaine des logiciels et du cloud ont été conduites, contre six en six mois entre mai et octobre 2021.

*(1) Audition, ouverte à la presse, de Mme Catherine Mayenobe, directrice générale déléguée de la Caisse des dépôts, directrice des opérations et du pilotage de la transformation opérationnelle, M. Arnaud Martin, directeur des risques opérationnels, M. Patrick Laurens-Frings, directeur de la transformation opérationnelle, digitale et des systèmes d'information du groupe, et M. Philippe Blanchot, directeur des relations institutionnelles, internationales et européennes, le 18 mars 2026*

**LISTE DES INTRODUCTIONS EN BOURSE (IPO) RÉALISÉES SUR EURONEXT PARIS DEPUIS LE 1ER JANVIER 2020 DANS LE SECTEUR DES LOGICIELS ET DU CLOUD**

| Société | Activité de l'entreprise | Date | Capitalisation boursière (M€) | Montant de la levée de fonds (M€) |
|---|---|---|---|---|
| Lighton | Développement de de logiciels et de modèles d'intelligence artificielle générative | Novembre 2024 | 62 | 12 |
| Planisware | Fourniture de solutions SaaS pour le management de projet | Avril 2024 | 1 100 | 241 |
| Broadpeak | Composants de diffusion vidéo à destination des fournisseurs de contenus et des opérateurs réseau qui déploient des services de streaming vidéo sur des réseaux à haut débit, fixes, mobiles ou par satellite | Juin 2022 | 80 | 20 |
| OVH | Fournisseur de services cloud | Octobre 2021 | 3 488 | 350 |
| Exclusive networks | Solutions de cybersécurité et de cloud | Septembre 2021 | 1 830 | 260 |
| Spartoo | Plateforme de vente en ligne d'habillement | Juillet 2021 | 119 | 24 |
| AMA corporation | Plateforme vidéo, photo et audio pour travailleurs en mobilité | Juillet 2021 | 146 | 36 |
| namR | Plateforme de données sur les infrastructures et les bâtiments | Juin 2021 | 38 | 8 |
| Obiz | Plateformes web pour le marketing | Mai 2021 | 31 | 8 |
| Alchimie | Plateforme de streaming de vidéos à la demande par abonnement | Novembre 2020 | 71 | 18 |
| Energisme | Plateforme SaaS pour la gestion des consommations d'énergie | Juillet 2020 | 28 | 8 |
| Nacon | Jeux vidéo | Mars 2020 | 458 | 100 |
| Munic | Acquisition et traitement de données des véhicules automobiles | Février 2020 | 61 | 18 |

*Source : Euronext.*

### 2. Le rachat des entreprises françaises par des groupes extra-européens

Un nombre important d'entreprises se vendent à des groupes non européens, notamment en partie de l'insuffisance du capital-risque en France et en Europe. La revente à des investisseurs étrangers et la cotation sur un indice américain constituent ainsi le parcours obligé de toute entreprise de la tech qui réussit.

L'exemple le plus emblématique en est le changement de domiciliation de Criteo pour le Luxembourg, changement annoncé en octobre 2025. Criteo réalise aujourd'hui 1,8 milliard d'euros de chiffre d'affaires, soit à elle seule 8 % de l'activité des éditeurs français, selon le recensement réalisé par Numeum. Ainsi que l'explique la société, la domiciliation au Luxembourg est une première étape

permettant dans le futur d'organiser un transfert vers les États-Unis, et ainsi d'accéder à des financements très importants. *« Il s'agit également d'une évolution naturelle dans le parcours de Criteo visant à tirer pleinement parti des avantages de notre introduction en bourse aux États-Unis — une décision stratégique initialement prise par nos fondateurs afin de soutenir la croissance à long terme de l'entreprise. Depuis que Criteo est devenue une société cotée en bourse, le paysage du marché boursier américain a considérablement évolué, et nous sommes convaincus que, parmi d'autres avantages, cette initiative permettra de réduire la complexité de la structure actuelle de Criteo, d'accroître la flexibilité en matière de rachats d'actions et de favoriser une éventuelle intégration dans certains indices américains. Avec un siège social au Luxembourg, nous pourrions éventuellement envisager un transfert ultérieur vers les États-Unis, ce qui permettrait d'élargir notre éligibilité aux principaux indices boursiers américains et d'accéder aux énormes réserves de capitaux passifs qui suivent ces indices de référence ».* Le déménagement aux États-Unis est trop souvent présenté comme une trajectoire naturelle sur le chemin de la croissance, afin d'accéder à un marché boursier beaucoup plus structuré et à des capitaux bien plus importants.

Deux autres exemples similaires peuvent être cités :

– Dataïku, une entreprise proposant des solutions d'intelligence artificielle pour les entreprises, créée en 2013 à Paris, a désormais son siège social à New York. La société compte Capital G, le fonds d'investissement du groupe Alphabet, à son capital ;

– Talend, société développant des outils de gestion des donnés, était français avant son rachat par l'entreprise américaine Qlik en 2023.

Ces deux sociétés étaient françaises lorsqu'elles ont fait l'objet de contrats avec des administrations d'État. Les garanties de souveraineté fournies au moment de la signature de ces contrats sont-elles les mêmes dans ces conditions ? Comment s'assurer que la commande publique ne contribue pas *in fine* à nourrir les géants internationaux ?

L'action de la DGE « *vise prioritairement à sanctuariser sur notre territoire les instances de décision, la recherche et développement, la propriété intellectuelle et les infrastructures critiques. Cet ancrage local prévaut sur la nationalité des capitaux. Compte tenu de la persistance de la faille de marché, renoncer aux financements de pays tiers serait contre-productif et condamnerait ces entreprises à l'arrêt. Lorsque les dossiers sont particulièrement sensibles, notre cadre juridique de contrôle des investissements étrangers nous permet d'imposer des conditions de localisation, un outil que nous utilisons de manière très volontariste ».* Pour BPIFrance, *« En l'absence de grands investisseurs majoritaires dans le domaine de la technologie en France, Bpifrance intervient régulièrement en qualité d'actionnaire minoritaire aux côtés de fonds étrangers, souvent américains. Dans ce cadre, elle joue un rôle d'équilibrage de la gouvernance de la société entre les fondateurs ou les dirigeants de la société et ces actionnaires majoritaires. Elle*

*négocie par ailleurs des droits spécifiques dans la gouvernance visant à prévenir la délocalisation de la R&D de ces entreprises ».*

Enfin, à la question de savoir si « *demain les Américains pourraient (…) racheter Mistral AI ?* », M. Arthur Mensch répondait à la rapporteure : « *Nous avons avec nous quelques sociétés de VC (venture capital), qui représentent moins de 30 % de notre capital. Nous aurions été ravis de prendre des Européens, mais il n'y en avait pas ! On y perd sur le plan économique : la partie general partner du retour sur investissement dans Mistral repart aux États-Unis, par le biais des fonds américains. Quant à la partie limited partner (LP), elle revient partiellement en Europe, car les Américains lèvent dans le monde entier. Donc on perd du retour, parce qu'on n'a pas tout l'écosystème. C'est dommage mais c'est comme ça* ».

M. Charles-Antoine Beyney, directeur général de DataOne donne à la commission une réponse similaire sur la question du potentiel rachat [(1)] : « *Quelle garantie puis-je apporter que le projet restera 100 % français ? Je vais répondre très franchement : aucune. Pourquoi ? Parce que BSO n'est pas une association à but non lucratif. Pour le dire très clairement, si nous ne construisons pas un schéma de refinancement ou un schéma d'investissement fort en Europe, les Étatsuniens continueront à nous acheter à bas prix, comme ils le font depuis cinquante ans. Si j'ai vendu à Equinix, c'est parce que cette société m'a présenté la meilleure offre. Si j'ai vendu à Vantage en 2020, c'est aussi parce que la meilleure offre était américaine* ».

Dans les imaginaires et les motivations profondes des entrepreneurs de la tech, le développement est indissociable du modèle de la levée de fonds qui s'est imposé aux États-Unis et de la maximisation du gain à la revente. L'objectif est de croître le plus vite possible, en cannibalisant les concurrents, pour devenir une « licorne » ou une « décacorne », voire une « pentacorne » ou une « hectocorne » ou de revendre au meilleur prix.

### 3. Une stratégie volontariste de soutien pour faire de la France une vitrine pour ses licornes

Mme Anne Le Hénanff, ministre déléguée auprès du ministre de l'économie, des finances et de la souveraineté industrielle, énergétique et numérique, chargée de l'intelligence artificielle et du numérique présentait devant la commission d'enquête le résultat d'une politique constante lancée depuis désormais plus de quinze ans, qui conduisait à faire de la France le premier pays européen en matière de création de start-up.

*« Collectivement, (…) nous ne sommes pas restés les bras croisés face à ces dépendances. Je souhaite ainsi rendre hommage aux travaux de mes prédécesseurs. De longue date, le combat est mené pour soutenir le développement d'une offre tech*

*(1) Audition conjointe, ouverte à la presse, de MM. Laurent Choukroun, président-directeur général d'Oreus et Julien Lescoulié, directeur technique, et M. Charles-Antoine Beyney, directeur général de DataOne le 29 avril 2026.*

*en France et en Europe. Dès 2010 fut lancé le premier programme d'investissements d'avenir. En 2013 ont été créées BPIFrance et la mission French Tech. Cet effort connaît une forte accélération depuis 2017, avec des stratégies sectorielles ambitieuses : la Stratégie IA (stratégie nationale pour l'intelligence artificielle) en 2018, à la suite du rapport Villani, la stratégie nationale pour le cloud en 2021, promue par Bruno Le Maire et Cédric O, la stratégie nationale quantique lancée par le Président de la République en 2021 et, bien sûr, le plan France 2030, doté, fin 2021 également, de 54 milliards d'euros d'argent public ». (…).*

« *En parallèle, notre fiscalité encourage l'entreprenariat et l'innovation avec le crédit d'impôt recherche (CIR), véritable outil de soutien à la recherche et développement et d'attractivité du pays, ainsi qu'avec des dispositifs spéciaux pour les start-up comme le statut de jeune entreprise innovante (JEI), cher à votre collègue Paul Midy, dont je salue l'engagement auprès de cet écosystème (…)*

« *La France est le leader européen en matière d'innovations de rupture, avec des pépites notamment dans le quantique, le spatial, l'intelligence artificielle ou les biotech. C'est le résultat d'un effort de long terme, qu'il convient de maintenir.* » (1)

En France, le continuum de financement de l'innovation apparaît relativement bien structuré en amont, à travers le soutien à la recherche et à la maturation technologique, les fonds d'amorçage et de capital-risque *early-stage* ainsi que les dispositifs d'accompagnement non financiers (incubation, accélération, mise en réseau). Ce continuum est particulièrement visible dans la *deeptech,* avec des dispositifs publics permettant de réduire le risque scientifique et technologique via l'attribution de subventions, d'avances remboursables et d'investissements en fonds propres. **L'aide aux entreprises du numérique se déploie à travers France 2030**, dont BPIFrance est l'opérateur pour le compte de l'État. BPIFrance chiffre les aides à l'innovation dans le domaine du numérique distribuées dans le cadre de France 2030 (hors « santé numérique ») à 1,1 milliard d'euros en 2025, dont 470 millions d'aides régionales et 631 millions d'aides nationales. Les appels à projet du programme France 2030 contiennent en particulier des volets importants sur le cloud et l'intelligence artificielle, pour des montants contractualisés respectifs de 218 et 152 millions.

**MONTANTS D'AIDE ATTRIBUÉS DANS LE CADRE DES APPELS À PROJET CLOUD ET IA DU PROGRAMME FRANCE 2030**

| | Nombre d'appels à projets | Aides contractualisées (M€) | Nombre de projets aidés | Part des subventions | Taux de décaissement |
|---|---|---|---|---|---|
| Cloud | 5 | 218 | 83 | 77% | 58% |
| IA | 4 | 152 | 54 | 85 % | 37 % |

*Source : BPIFrance.*

*(1) Audition commune, ouverte à la presse, de M. David Amiel, ministre de l'action et des comptes publics, et de Mme Anne Le Hénanff, ministre déléguée auprès du ministre de l'économie, des finances et de la souveraineté industrielle, énergétique et numérique, chargée de l'intelligence artificielle et du numérique, le 20 mai 2026.*

**En ce qui concerne le capital-risque**, BPIFrance investit des montants pouvant aller de quelques millions à plusieurs dizaines de millions d'euros, pour une détention du capital allant de quelques pourcents à près de 20 %, selon la date d'entrée au capital et le montant investi. Dans le domaine du capital-développement, BPIFrance investit dans des entreprises rentables, pour des participations allant de quelques millions à des montants susceptibles de dépasser la centaine de millions d'euros, dans le cadre d'une doctrine d'investissement intégrant les enjeux de souveraineté numérique. Les secteurs concernés sont le quantique, le cloud, l'IA, la cybersécurité et la 5G/6G.

Le tableau ci-dessous présente les sociétés du portefeuille de participations de BPIFrance présentant un intérêt particulier en matière de souveraineté numérique.

**PORTEFEUILLE DE PARTICIPATIONS DE BPIFRANCE DANS LES DOMAINES DE L'INTELLIGENCE ARTIFICIELLE, DES LOGICIELS ET DE LA CYBERSÉCURITÉ**

| | |
|---|---|
| **Intelligence artificielle** | |
| **AMI Labs** | AMI Labs développe une nouvelle génération de systèmes d'IA dits "world models" se distinguant des LLM par leur capacité à comprendre le monde et étant dotés de capacités de mémoire persistante, de raisonnement et de planification. |
| **Mistral AI** | Mistral AI développe des modèles LLM généralistes multimodaux et open source pour répondre sur-mesure aux besoins complexes des grandes entreprises. |
| **Genesis** | Genesis développe des modèles d'IA appliqués à la robotique et aux systèmes autonomes, notamment en s'appuyant sur un moteur de simulation physique. Sa technologie vise à doter les machines de capacités de raisonnement et d'adaptation dans le monde réel. |
| **Altrove** | Altrove conçoit des modèles d'IA et développe des capacités de synthèse en laboratoire pour identifier des nouveaux matériaux et réduire leur cycle de développement. La société vise à développer des matériaux alternatifs à des matériaux actuellement critiques en termes d'approvisionnement pour l'Europe, et se concentre sur les matériaux inorganiques (métaux, cristaux, céramiques). |
| **Logiciel** | |
| **Chapsvision** | Chapsvision développe des solutions fondées sur la gestion de données et l'IA à grande échelle, à destination de clients privés et publics (en particulier régaliens), notamment dans le domaine de l'investigation, de la recherche et l'analyse de grands volumes de données, de la cybersécurité, de la gestion de crise, de l'open source intelligence (ou « OSINT »). La société mène une stratégie ciblée d'acquisitions, en complément de ses investissements R&D et commerciaux significatifs, ce qui en fait un des consolidateurs nationaux dans le domaine du logiciel. |
| **Doctolib** | Doctolib développe des logiciels à destination des professions médicales et de leurs patients afin d'optimiser la prise de rendez-vous et la gestion des informations de santé. |
| **CHR Groupe** | CHR Groupe édite des solutions SaaS pour les professionnels de la restauration et des métiers de bouche. Le groupe opère principalement via ePack Hygiene (HACCP et traçabilité sanitaire) et Adoria (gestion des achats, stocks et pilotage multi-sites). |
| **Ciril Group** | Ciril Group édite plusieurs logiciels utilisés par les collectivités territoriales françaises. |
| **Septeo** | Septeo développe des logiciels à destination de plusieurs secteurs, notamment les professions réglementées telles que les avocats ou les notaires. Les produits de Septeo sont utilisés dans un grand nombre d'études notariales françaises. |
| **Softway Medical** | Softway Medical est leader dans le domaine des logiciels critiques pour le fonctionnement des établissements de santé publics et privés (par ex. dossiers patients informatisés, gestion administrative des patients, imagerie, biologie etc.), en tant qu'éditeur, intégrateur et hébergeur de données de santé. Elle mène une politique de développement produit innovante, permettant une efficacité accrue de la chaîne de soin, une intégration et interopérabilité des outils, une sécurité renforcée pour les données sensibles, autour d'un hébergement dans des infrastructures certifiées HDS en France. |

| **Cybersécurité** | |
|---|---|
| **Sekoia** | Plateforme étendue de détection et de réponse aux cyberattaques de dernière génération, auto-apprenante, s'interfaçant avec toutes les solutions de cybersécurité déployées pour une détection de tous types de menaces dont les signaux faibles. |
| **Yes We Hack** | Leader européen des plateformes de *bug bounty* mettant en relation des entreprises et des hackers éthiques afin d'identifier des failles dans les systèmes d'information pour les protéger contre des cyberattaques. |
| **Seclab** | Solutions hardware permettant la ségrégation de réseaux. |
| **Gitguardian** | Détection des fuites de clés d'authentification à des APIs sur GitHub. |

L'ensemble du portefeuille dans le domaine du numérique (hors sociétés cotées) représente une valorisation (1) de 1 374 millions d'euros, à travers 95 participations. Deux sont supérieures à 100 millions et quatre supérieures à 50 millions.

Ces chiffres témoignent d'un effort important pour prendre des participations au capital d'entreprises du numérique et faciliter ainsi leur financement. Une accélération du financement est en cours dans le domaine de l'intelligence artificielle. Ainsi que l'indique BPIFrance, *« dans le cadre de son plan stratégique 2026-2030, Bpifrance prévoit de déployer 10 Md€ pour soutenir l'ensemble de la chaîne de valeur de l'IA : des infrastructures aux applications, en passant par les modèles de fondation responsables. Bpifrance ambitionne de structurer l'écosystème de financement de l'innovation en IA à tous les niveaux : en accompagnant les fonds partenaires français dans l'orientation de leurs investissements vers l'IA, en favorisant l'émergence de fonds sectoriels couvrant toute la chaîne de valeur, mais aussi en investissant dans des fonds européens et mondiaux qui affichent un fort intérêt pour le marché français. L'objectif : mobiliser 3 Md€ via l'ensemble des fonds partenaires. Bpifrance soutiendra également le développement de projets stratégiques en fonds propres, notamment dans le domaine des modèles de fondation, tout en investissant dans les infrastructures clés de l'IA : semi-conducteurs, data centers, MLOps, plateformes applicatives et composants spécialisés »* (2). Le financement public joue également un rôle important de crédibilisation des sociétés dans lesquelles l'État investit. Ces sociétés peuvent également bénéficier du soutien de l'appareil d'État à l'occasion des événements dans le cadre de la diplomatie économique (visites d'État dans d'autres pays, sommet Choose France, etc.). La question se pose des contreparties qui sont demandées par l'État actionnaire lorsqu'il prend des participations dans le numérique.

### 4. L'insuffisant contrôle des participations

Dans quelle mesure l'État utilise-t-il son portefeuille de participations pour défendre la souveraineté numérique ?

Tout d'abord, ces prises de participation ne permettent pas d'influencer les achats SI des entreprises du portefeuille de participations. Ainsi Doctolib, une

*(1) valeur d'acquisition.*

*(2) Réponses aux questionnaires de la rapporteure.*

entreprise gérant pourtant des données de santé hautement sensibles, stocke ses données dans des clouds AWS [1].

Lors de la déclaration liminaire à leur audition, les représentants de BPIFrance ont mentionné les entreprises dans lesquelles ils siègent. Ces déclarations permettent de mieux comprendre la diversité des entreprises dans lesquelles la banque est représentée : Technip Energies, Veolia, Younited (fintech spécialisée dans le crédit à la consommation), Orange, Worldline, Vantiva, Idemia, Campus IA, Soitec. BPIFrance siège également chez Kayrros ou STMicroelectronics. Le pouvoir au sein des conseils d'administrations de ces sociétés est limité, ce qui bride la possibilité d'imposer des solutions souveraines, comme l'expliquait M. Arnaud Caudoux [2] : « *En général, au conseil d'administration, nous surveillons ce qu'elles font, mais nous n'avons pas le pouvoir de leur interdire le recours à ce type de solution. Nous avons simplement le pouvoir de les avertir qu'elles se mettent en situation de dépendance excessive en y recourant.* »

De plus, l'entrée au capital n'est pas conditionnée à des exigences suffisamment fortes pour préserver les entreprises concernées du risque de rachat par des entités extra-européennes.

Le gouvernement n'a pas fait de la consolidation des entreprises numériques stratégiques une priorité. La commission d'enquête relative à la prédation des capacités productives françaises par les fonds spéculatifs s'est notamment penchée sur le cas d'ATOS. Ainsi, la rapporteure Aurélie Trouvé souligne-t-elle, « *le cas Atos est emblématique de l'échec de la puissance publique à défendre pleinement les capacités productives françaises face aux fonds prédateurs. Le groupe français spécialisé dans les services numériques, la cybersécurité et les infrastructures informatiques critiques pour les entreprises et les administrations publiques est passé fin 2024 sous le contrôle de plusieurs acteurs financiers, en particulier des fonds spéculatifs anglo-saxons. Alerté de longue date, l'État a choisi de limiter son intervention à certains actifs, laissant le reste d'un groupe stratégique aux mains de ses créanciers-actionnaires. Cette doctrine défensive et fragmentée n'a pas empêché – et a même rendu possible – la prise de contrôle d'un acteur de souveraineté par des fonds dont l'unique horizon est le remboursement de leurs créances.* ***Votre rapporteure considère que cette séquence engage la responsabilité politique des gouvernements successifs et appelle une évolution de la doctrine d'intervention de l'État dans un contexte marqué par de fortes tensions géopolitiques.*** » [3]

---

*(1)* https://doctolibpatient.zendesk.com/hc/fr/articles/4404181466002-O%C3%B9-sont-stock%C3%A9es-mes-donn%C3%A9es-personnelles

*(2) Audition, de M. Arnaud Caudoux, directeur général adjoint de BPIFrance, M. Lionel Chaine, directeur des systèmes d'information, Mme Sophie Rémont, directrice en charge de l'expertise et des programmes au sein de la direction de l'innovation et M. Thierry Sommelet, directeur au sein de la direction du capital-développement, le 21 avril 2026.*

*(3) Aurélie Trouvé, Rapport fait au nom de la commission d'enquête sur la prédation des capacités productives françaises par les fonds spéculatifs, juin 2026*

Deux exemples peuvent ainsi être donnés dans le portefeuille de BPIFrance de l'insuffisance des contreparties requises :

– Mistral AI : cette entreprise est désormais placée au centre de la stratégie de déploiement des modèles IA pour les administrations ; elle est décrite comme la seule véritable alternative aux géants américains et chinois dans le domaine des grands modèles de langage. Elle développe des outils critiques pour les administrations. Pourtant, l'État n'a assorti sa prise de participation au capital d'aucune condition.

– Chaps Vision : cette société a été choisie tout récemment par l'État comme alternative à Palantir. Le pacte d'actionnaires prévoit que si l'actionnaire majoritaire cède ses parts, BPIFrance ne dispose d'un droit de véto que pour les États membres de l'OCDE, ce qui inclut notamment la Corée du Sud, les États-Unis, Israël, le Japon ou la Turquie.

La puissance publique ne doit pas rester démunie face à ces nombreuses reventes qui fragilisent la réalisation d'une véritable politique industrielle. L'effort de l'État pour soutenir les entreprises innovantes est à signaler, que ce soit directement via des prises de participation ou indirectement à travers l'appui à la constitution de fonds de financement. Mais quelles sont les contreparties lorsqu'une société, qui s'est développée sur des fonds publics ou grâce à des commandes publiques, ou a tout simplement bénéficié d'un support politique (participation aux délégations présidentielles, appui dans les instructions administratives, etc.), décide de s'expatrier ?

Enfin, le soutien aux entreprises innovantes, que ce soit via des subventions ou des prises de participation, doit être l'occasion d'orienter les choix techniques des sociétés soutenues, de façon à favoriser la diffusion des technologies open source et de standards interopérables.

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

### D. L'ABSENCE DE RÉACTIONS SIGNIFICATIVES AU NIVEAU EUROPÉEN

En examinant les conditions de développement des entreprises françaises du logiciel et du cloud, le constat est sombre. Alors que les géants de la tech n'ont jamais été aussi puissants, l'Europe et la France ne semblent pas prendre la mesure du risque que cela représente, tant en termes de souveraineté politique que de développement économique.

Face à ce constat de la fragilisation de l'économie européenne sur le plan technologique, l'écart est abyssal entre les discours et les actes de l'Union européenne. Le constat est désormais partagé, mais aucune initiative ne témoigne d'un réel changement d'échelle.

Les politiques de soutien à l'innovation menées par l'Union européenne sont insuffisantes. Les États membres sont contraints financièrement dans leurs investissements par le pacte de stabilité et de croissance et sont également limités sur le plan juridique par la réglementation sur les aides d'État. Les financements européens ne prennent pas le relais des aides nationales. Comme le constate le rapport Draghi, « *le soutien de l'UE aux investissements publics et privés est limité par la taille du budget de l'UE, par son manque d'orientation ainsi que par une attitude trop prudente à l'égard des risques. Le budget annuel de l'UE est peu élevé, puisqu'il ne représente qu'un peu plus de 1 % du PIB de l'Union, tandis que les budgets des États membres en représentent collectivement près de 50 %.* »

S'agissant de la mise en œuvre d'une préférence nationale dans les achats publics, la Commission européenne a annoncé l'adoption d'un texte sur les achats publics au second semestre 2026. La référence à une préférence européenne est désormais assumée, mais ses contours sont encore incertains : « *Dans ses orientations politiques, la présidente de la Commission, Ursula von der Leyen, a promis une révision de la législation relative aux marchés publics. Elle a souligné que cette révision « permettra de privilégier les produits européens dans les marchés publics de certains secteurs stratégiques ». Lors de son discours sur l'État de l'Union de 2025, la présidente von der Leyen a de nouveau promis d'« introduire un critère « made in Europe » dans les marchés publics* ». (1)

Il reste cependant une incertitude sur ce que recouvrira ce critère « *made in Europe* ». Les représentants du collectif Eurostack, Mme Cristina Caffarra et M. Yann Lechelle, décrivent les différences de positionnement qui restent à surmonter. Ainsi, Mme Caffara affirme : « *À cela s'ajoutent des différences de positionnement entre États membres, qui compliquent la convergence. La France est historiquement pionnière sur le sujet de la préférence européenne], mais cette position est caricaturée par les lobbyistes, qui la qualifient de protectionniste. D'autres pays revendiquent une posture plus modérée, plus conservatrice, notamment l'Allemagne. (…)*

« *La position néerlandaise est plutôt favorable et alignée, tout comme celle du Danemark. Il existe donc un ensemble de pays globalement d'accord, malgré des différences de discours liées à des traditions nationales distinctes. En réalité, un certain alignement existe, mais le principal problème réside dans l'intensité du lobbying, qui crée un climat de peur et freine toute décision ambitieuse.* »

M. Yann Lechelle ajoute : « *Je confirme qu'il existe des sensibilités qui, selon les moments, s'alignent ou se contestent. Nous ne pourrons pas parvenir à un résultat à vingt-sept. Cela n'est pas réaliste. En revanche, certaines alliances, une coalition of the willing, des entités qui se rejoignent volontairement, peuvent déplacer le curseur et produire des changements significatifs. (…) Il suffit d'imaginer que, sur les 260 à 300 milliards d'euros de flux qui quittent chaque*

---

*(1) https://www.europarl.europa.eu/legislative-train/theme-a-new-plan-for-europe-s-sustainable-prosperity-and-competitiveness/file-public-procurement-act, traduit de l'anglais.*

*année l'Europe, nous parvenions à rediriger seulement 1 %, 2 % ou 3 % vers des acteurs locaux. Immédiatement, leur chiffre d'affaires serait multiplié par deux ou trois. Des entreprises autrefois petites deviendraient moyennes, des moyennes deviendraient grandes. À partir de là, un cercle vertueux pourrait s'enclencher, permettant aux acteurs de consolider le marché. C'est pourquoi il est indispensable de créer un changement dynamique avec les pays qui partagent cette analyse et qui considèrent, comme nous, qu'il faut modifier la trajectoire. Nous n'y parviendrons pas à vingt-sept, car si Bruxelles exige un consensus absolu, certaines nations refuseront, ayant trop à perdre et trop peu à offrir.*

« *En revanche, la France et l'Allemagne ont naturellement des choses à faire ensemble, de même que les Pays-Bas ou le Danemark, d'autant plus que ce dernier pays a été directement menacé dans sa souveraineté, y compris territoriale, et commence à mesurer l'enjeu. Il faut désormais opérer un basculement psychologique.*

« *Nous sommes un certain nombre à travailler sur la souveraineté numérique depuis plus de dix ans, mais nous étions trop peu nombreux et il n'existait pas de prise de conscience collective. Je pense que ce point de bascule est désormais atteint.*

« *Des alliances européennes sont possibles, notamment autour d'un dispositif équivalent au Small Business Act américain. (…) Le Small Business Act européen existe théoriquement, mais il n'est pas fonctionnel.* » (1)

En conclusion, le modèle de financement des entreprises est un levier fort de différenciation entre les États-Unis et l'Europe. Malgré un constat qui a été établi maintes fois, les lignes de la réglementation européenne bougent à un rythme désespérément lent. Comment expliquer que nous soyons encore la seule région du monde à nous appliquer à nous-mêmes des contraintes transgressées par les autres grandes puissances ? Les travaux sur la préférence européenne doivent aboutir de façon urgente.

La France se distingue par un soutien important à ses entreprises de la tech, avec l'objectif affiché de faire émerger les prochaines licornes. Cette politique souffre de deux défauts : d'une part, l'ambition de copier le modèle américain s'accompagne d'une adoption de ses pires défauts. Ainsi, au prétexte de créer de nouveaux géants européens, il faudrait affaiblir la régulation qui s'applique à eux. D'autre part, les prises de participation ne s'accompagnent pas de contreparties suffisantes, ce qui laisse grandes ouvertes les portes du capital d'entreprises désormais stratégiques à des investisseurs extra-européens.

*(1) Audition du collectif Eurostack représenté par Mme Cristina Caffarra, économiste, spécialiste de la concurrence et de la régulation des plateformes numériques et M. Yann Lechelle, entrepreneur, président-directeur général de probabl.ai, le 26 mars 2026.*

## CHAPITRE 11 – LE DÉPLOIEMENT DE L'IA : LE RISQUE D'UNE PERTE DÉFINITIVE DE TOUTE MAÎTRISE

### A. LES CONSÉQUENCES ÉCONOMIQUES

Comme le soulignait M. Arthur Mensch devant la commission d'enquête, « *la situation est, je pense, assez explosive : à cause de l'intelligence artificielle, il y a des destructions d'emplois – en tout cas, des modifications très rapides de la structure de l'emploi en Europe ; il y a ensuite des conflits d'usage de l'électricité – tout le monde en veut, mais il n'y en a pas assez –, et donc une inflation ; il y a enfin une explosion du déficit commercial qui, dans le domaine des services, sera multiplié par cinq dans les cinq prochaines années. Une situation comme celle-ci est révolutionnaire. Il faut la prendre en compte, en parler davantage et avoir un point de vue de plus long terme sur ce qu'elle implique pour l'économie, pour la société et pour les équilibres géopolitiques. Si on ne le fait pas assez rapidement, on n'aura plus aucun choix – une situation que l'on ne voudrait pas voir advenir.* » (1)

En créant cette commission d'enquête, l'Assemblée nationale montrait que ce sujet était au premier rang des préoccupations de la représentation nationale. Il était clair que l'examen des conséquences économiques de la dépendance à des outils extra-européens existants trouvait son prolongement logique dans la réflexion sur les conséquences économiques de nouvelles dépendances à des modèles d'intelligence artificielle générative. La rapporteure a souhaité réaliser cet examen selon une approche la plus objective possible. Pour cela, plusieurs questions doivent ainsi être traitées :

– Quelles sont les perspectives réelles de l'intelligence artificielle ? Assiste-t-on réellement à une profonde révolution de notre économie, ou bien à un changement du même type que ceux connus par le passé (bulle internet de la fin des années 1990 – début des années 2000) ?

– Que montrent les premiers travaux économiques sur les conséquences de l'IA sur l'emploi et la croissance ?

#### 1. Révolution ou évolution ? Bulle ou pas bulle ?

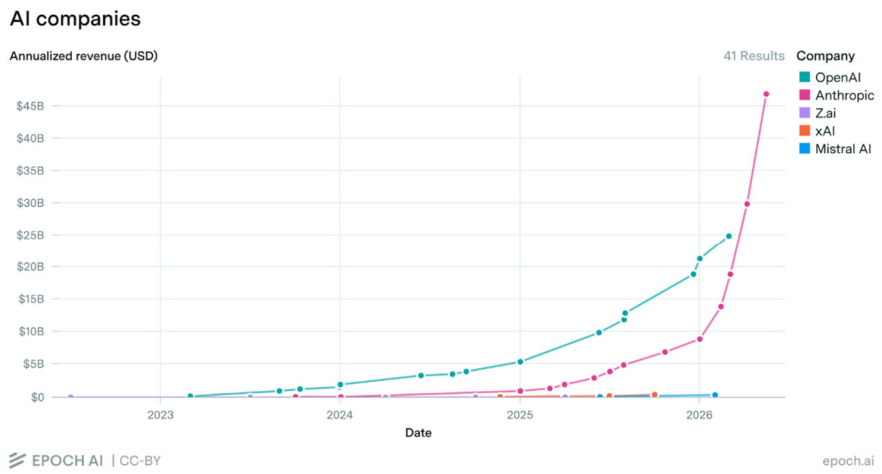
Il est impossible de répondre avec certitude à la question sur la magnitude de la transformation engendrée par l'intelligence artificielle sur l'économie mondiale. Une question dérivée de celle-ci est l'adéquation des valorisations des entreprises de l'IA et du numérique avec les revenus futurs qu'elles génèreront. En d'autres termes, existe-t-il une bulle sur l'intelligence artificielle ? Il convient de se prémunir contre la tentation de prendre pour vérité les discours des entreprises dont

*(1) Audition de M. Arthur Mensch, cofondateur et directeur général de Mistral AI , le 12 mai 2026.*

les levées de fonds reposent sur des prévisions de croissance et de taille de marché très importantes. Le niveau de réalisation de ces prévisions est aujourd'hui inconnu.

Les débats sur la bulle de l'IA se sont multipliés depuis l'automne 2025, alimentés par les levées obligataires des *hyperscalers* – 121 milliards de dollars en 2025 – pour financer leurs investissements dans les infrastructures et les levées de fonds record des principaux laboratoires d'IA portées en partie par les *hyperscalers* et fournisseurs de puces. En septembre 2025, OpenAI et Nvidia signaient une lettre d'intention pour le déploiement d'au moins 10 gigawatts (GW) de systèmes Nvidia, avec une intention d'investissement progressif de Nvidia dans le capital d'OpenAI allant jusqu'à 100 milliards de dollars. En novembre 2025, dans le cadre d'un partenariat stratégique tripartite Microsoft–Nvidia–Anthropic, Nvidia s'engageait à investir jusqu'à 10 milliards et Microsoft jusqu'à 5 milliards dans Anthropic, tandis qu'Anthropic s'engageait à hauteur de 30 milliards de dollars d'achats de services fournis par Microsoft Azure (1).

Les fondements de ces opérations sont confirmés par la progression très rapide des revenus des principaux acteurs de l'IA, illustrée par le graphique ci-dessous (2).




L'entreprise Anthropic a ainsi vu son chiffre d'affaires dépasser les 45 milliards de dollars en 2026. À titre de comparaison, la société Orange a réalisé un chiffre d'affaires de 40,4 milliards d'euros en 2025. Anthropic a ainsi levé 65 milliards de dollars, dans le cadre d'une opération de valorisation la société à 965 milliards (3).

---

*(1) https://www.anthropic.com/news/microsoft-nvidia-anthropic-announce-strategic-partnerships*

*(2) https://epoch.ai/data/ai-companies?view=graph&tab=revenue*

*(3) Communiqué de l'entreprise Anthropic, mai 2026 https://www.anthropic.com/news/series-h*

Dans son rapport sur la stabilité financière mondiale, datant d'avril 2026, le Fonds monétaire international examine le potentiel risque créé par les mouvements boursiers autour des géants du numérique et de l'intelligence artificielle [(1)]. Dans un premier temps, **le FMI considère que les investissements des *hyperscalers*, bien que très importants, s'appuient sur des bilans solides et la capacité à générer des revenus.** « *Pour les principaux hyperscalers, la croissance des bénéfices a suivi le rythme des dépenses d'investissement, les flux de trésorerie disponibles se maintenant à des niveaux élevés. À l'avenir, les bénéfices et les réserves de trésorerie des hyperscalers pourraient s'avérer insuffisants compte tenu des dépenses d'investissement liées à l'IA estimées à 3 400 milliards de dollars d'ici 2029, ce qui pourrait exercer des pressions sur leur bilan dans les années à venir. En prévision de ces dépenses futures, les hyperscalers ont levé plus de 100 milliards de dollars par le biais d'émissions obligataires depuis janvier 2025 (…). Cela dit, l'appétit pour les émissions obligataires des hyperscalers liées à l'essor des dépenses d'investissement (capex) en IA sur le marché des titres notés « investment grade » est très soutenu. La qualité de crédit moyenne des hyperscalers est solide compte tenu de la robustesse de leur situation financière, soutenue par leur capacité à générer d'importants flux de trésorerie disponibles. Par conséquent, même si le rythme des émissions obligataires s'est accéléré et devrait rester élevé par rapport aux années précédentes, les risques liés à la stabilité financière restent maîtrisés* ».

Les revenus dégagés par la vente des services d'intelligence artificielle sont en forte progression, mais cette progression n'est pas à l'échelle des valorisations et des investissements astronomiques des géants américains de la tech. La soutenabilité économique de la trajectoire d'investissements des sociétés d'intelligence artificielle repose sur une potentielle croissance exponentielle des revenus, et cela, dans un **délai correspondant aux attentes des investisseurs**. Or des doutes importants existent à ce sujet, qu'ils soient liés à l'offre (délais de construction de data centers ou des raccordements électriques, disponibilité des puces) ou à la demande (délais dans l'adoption de la technologie au sein des entreprises). L'horizon temporel de retour sur investissement pourrait donc être plus faible et plus lent qu'envisagé.

Dans son *Technology report*, publié en septembre 2025, la société de conseil Bain souligne que les besoins en capacité de calcul liés à l'IA sont multipliés par 4,5 chaque année, ce qui est deux fois supérieur à l'augmentation de l'efficacité des puces (loi de Moore) [(2)]. Pour répondre à ces besoins, une capacité de production électrique supplémentaire de 200 gigawatts devrait être construite d'ici 2030, dont 100 gigawatts aux États-Unis. Cela représente un investissement estimé à 500 milliards de dollars par an. Pour être en mesure de financer de tels investissements en maintenant des ratios de solvabilité suffisants, les hyperscalers devraient dégager des revenus annuels de 2 000 milliards de dollars.

---

*(1) Fonds monétaire international,* Rapport sur la stabilité financière mondiale, *avril 2026, https://www.imf.org/-/media/files/publications/gfsr/2026/april/english/text.pdf*

*(2) Bain, Technology report, septembre 2025 https://www.bain.com/insights/how-can-we-meet-ais-insatiable-demand-for-compute-power-technology-report-2025/*

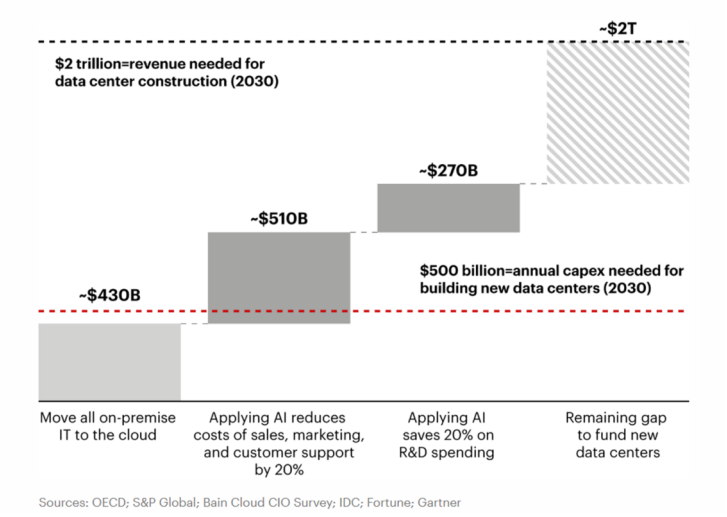
Pour estimer les potentiels revenus générés par la monétisation de l'IA, la société de conseil additionne :

– le passage de l'intégralité du stockage de données des entreprises du *on-premise* au cloud ;

– la réduction de 20 % des coûts de marketing et commercial ;

– la réduction de 20 % des coûts de R&D.

Selon les estimations de Bain, ces postes additionnés représentent 1 210 milliards de dollars, correspondant ainsi à une estimation maximaliste des revenus possibles des entreprises d'intelligence artificielle. Y compris dans un tel scénario, les revenus générés ne seraient pas suffisants pour financer l'ensemble des investissements nouveaux – sans même prendre en compte les besoins de maintenance et de renouvellement du matériel. L'écart entre le revenu et les besoins de financement s'élèverait donc *a minima* à 800 millions de dollars annuels.




*Source : Bain, Technology report.*

Les défis financiers se doublent de défis techniques et industriels, comme les contraintes sur l'approvisionnement des équipements (GPU, mais aussi équipements pour les systèmes de refroidissement et la connexion électrique) et la construction de capacités additionnelles de production électrique et de réseaux de transport et de distribution d'électricité.

Plusieurs signaux d'alerte témoignent des doutes sur la soutenabilité de la trajectoire actuelle, en raison de la difficulté des entreprises à rentabiliser leur investissement.

D'un côté, la course à la conquête des utilisateurs par un accès à des versions gratuites ou ne reflétant pas les coûts complets de fonctionnement des modèles

trouve ses limites lorsque ces coûts sont trop importants. Pour la première fois Open AI a dû arrêter un de ses produits phares, Sora. Destiné à la génération de vidéos par intelligence artificielle, il avait entraîné des pertes importantes pour l'entreprise. Ainsi que le rapporte Mediapart, citant le Wall Street Journal « *Sora coûtait en moyenne 1 million de dollars par jour et n'a rapporté, depuis son lancement, qu'un peu plus de 2 millions de dollars.* » (1)

De l'autre, après une phase d'enthousiasme pour un produit nouveau, de nombreuses entreprises questionnent l'apport économique de l'IA au regard de l'envolée des factures de tokens. Ainsi, alors que les coûts liés à l'IA chez Uber ont été multipliés par six depuis 2024, un article de *Next* rapporte que le directeur des opérations, Andrew Macdonald, considère qu'« *il est de plus en plus difficile de justifier les coûts liés à l'usage de l'IA générative. Invité du podcast Rapid Response, il a expliqué qu'une consommation élevée de tokens n'aboutissait pas nécessairement à une augmentation proportionnelle des fonctions utiles pour le consommateur.* » (2) Le même article mentionne que « *le directeur technique de la plateforme VTC, Praveen Neppalli Naga, s'était étonné chez The Information d'avoir explosé son budget IA de l'année en seulement quatre mois.* »

Une étude menée par des chercheurs du Massachussets Institute of Technology (3), basée sur des interviews avec des représentants d'entreprise, montre que 95 % des entreprises ayant investies dans l'IA générative sont « coincées du mauvais côté », et qu'elles ne bénéficient d'aucun retour sur investissement. Des résultats confirmés par lors des différentes auditions de la commission, où il a été communément admis qu'il n'existait aucune étude macroéconomique mesurant le niveau de retour sur investissement des projets de déploiement d'intelligence artificielle.

Deux phénomènes additionnels pourraient menacer l'équilibre économique du secteur.

**Le premier est la circularité des investissements entre les entreprises de ce que le FMI appelle le « cercle de l'intelligence artificielle »**, composé d'Amazon, AMD, Alphabet (Google), Intel, Microsoft, Nvidia et Oracle. Entre septembre et décembre 2025, les sociétés appartenant à ce cercle ont vu leur capitalisation boursière augmenter de 40 milliards de dollars par cet effet, ce qui représente une augmentation moyenne de 7 points. « *Depuis 2025, les mécanismes de financement circulaire au sein de l'écosystème de l'IA se sont généralisés. Dans le cadre de ces mécanismes, les développeurs d'IA, les fabricants de puces et les*

---

*(1) Romaric Godin, « L'incertaine viabilité économique de l'IA générative », Médiapart, 4 avril 2026* https://www.mediapart.fr/journal/economie-et-social/040426/l-incertaine-viabilite-economique-de-l-ia-generative

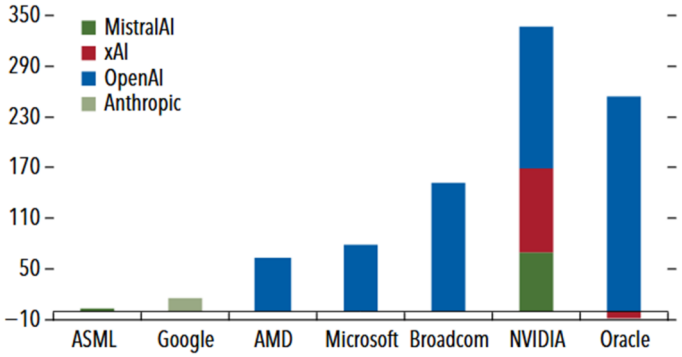
*(2) Mickael Bazoge, « Uber commence à trouver l'addition de l'IA un peu salée », Next, le 26 mai 2026* https://next.ink/brief-article/uber-commence-a-trouver-laddition-de-lia-un-peu-salee/

*(3) Aditya Challapally, Chrise Pease, Ramesh Raskar, Pradyumna Chari, MIT Nanda, The GenAI Divide, State of AI in business 2025, juillet 2025*

https://mlq.ai/media/quarterly_decks/v0.1_State_of_AI_in_Business_2025_Report.pdf

*grandes entreprises technologiques jouent simultanément le rôle de clients, d'investisseurs et de bailleurs de fonds. La structure de ce financement circulaire forge des liens étroits entre les entreprises cotées en bourse (par exemple, Nvidia, Oracle) et celles non cotées liées à l'IA (par exemple, OpenAI, xAI), qui présentent des niveaux de vulnérabilité financière variables et des modèles économiques divers. Ces liens étroits entraînent des risques d'opacité.* » (1) Les entreprises concernées peuvent chacune se prévaloir de prévisions de chiffre d'affaires gonflées, augmentant ainsi le risque de surévaluation de leurs cours et de leur valorisation. Le graphique ci-dessous montre la hausse des capitalisations boursières consécutives à des annonces d'accords croisés.

**1. Change in Market Capitalization after AI Deal Announcements**
*(Billions of dollars, based on deals in 2025)*




*Source : Fonds monétaire international.*

**Second risque**, **les dépréciations brutales d'actifs liées à l'obsolescence technique.** Les investissements réalisés pourraient subir des dépréciations comptables au regard de la rapidité de l'évolution technologique. Le FMI souligne ainsi que les *hyperscalers* pourraient être amenés à devoir lever des fonds supplémentaires à cause d'une surestimation de la durée de vie de leurs équipements. « *Sur la base des chiffres d'amortissement comptable publiés par les principaux hyperscalers, les estimations de notre équipe suggèrent que la durée de vie utile moyenne implicite actuelle des « immobilisations corporelles » est d'environ sept ans. Cependant, les GPU et les puces de pointe — qui représentent une part importante des coûts liés aux serveurs et aux infrastructures d'IA — pourraient devenir obsolètes dans des délais plus courts, en raison de la rapidité des progrès technologiques dans le domaine de l'IA.* » (2)

Au regard de l'ensemble de ces éléments, les forts investissements dans l'IA restent risqués et donc sous la surveillance des autorités de régulation macroprudentielles. Ainsi, le chef économiste du Fonds monétaire international,

*(1) Traduit de l'anglais.*

*(2) Traduit de l'anglais.*

M. Pierre-Olivier Gourinchas, déclarait à Reuters en octobre 2025 : « *Il y a de nombreuses similitudes entre la bulle boursière liée à Internet de la fin des années 1990 et l'essor actuel de l'intelligence artificielle : ces deux périodes ont propulsé les valorisations boursières et la richesse issue des gains en capital vers de nouveaux sommets, alimentant ainsi une consommation qui a renforcé les pressions inflationnistes.* » (1)

Les revenus générés par l'intelligence artificielle n'ont pas encore atteint les montants envisagés, mais l'ampleur du boom de l'IA est moindre que celle de la bulle internet du début du siècle : les investissements dans l'IA ont crû de moins de 0,4 % du PIB américain, contre 1,2 % entre 1995 et 2000, selon des données compilées par le FMI. L'impact sur la stabilité financière internationale ne serait pas aussi fort, ce qui n'exclurait pas les risques économiques systémiques liés au dégonflement de la bulle de l'IA.

Dans un article de décembre 2025, le *Financial Times* comparait les situations de Cisco Systems et Nvidia (2) : *« Si l'on revient loin dans le temps, le 27 mars 2000, Cisco avait brièvement dépassé Microsoft pour devenir l'entreprise la plus valorisée au monde, avec un cours de l'action record (..) de 80,06 dollars. Cela a pris un looooooooooong moment, mais hier, Cisco a atteint un nouveau record à 80,25 dollars. Hourra ! ».* Selon le journal, la qualité de la société et des produits développés n'était pas en cause. Les attentes du marché étaient démesurées en l'an 2000 et mirent finalement vingt-cinq ans à se concrétiser.

### 2. L'impact économique de l'intelligence artificielle sur l'emploi : la nécessaire vigilance

L'arrivée des modèles d'intelligence artificielle générative dans les entreprises et les administrations aura-t-elle pour effet de détruire ou de créer de nouveaux emplois ? M. Aiman Ezzat, directeur général de Capgemini, a témoigné de la situation dans la société qu'il dirige (3) : « *Nous devons nous adapter en permanence aux évolutions technologiques comme au changement de la demande de nos clients. Nous envisageons effectivement environ 2 400 suppressions de poste. Ce ne sont pas 2 400 licenciements : nous avons lancé un plan de départs volontaires. C'est lié à des évolutions. Ainsi, le contrôle qualité des logiciels était très intensif et très manuel. Aujourd'hui, grâce à l'intelligence artificielle, il est de plus en plus automatisé. Il est évident que les besoins ne sont plus les mêmes. Nous cherchons donc à faire évoluer les compétences de nos collaborateurs, ou nous proposons des départs volontaires, parce que nous avons besoin de moins de*

---

*(1) David Lawder, «AI investment boom may lead to bust, but not likely systemic crisis, IMF chief economist says », Reuters, octobre 2025*
*https://www.reuters.com/legal/transactional/ai-investment-boom-may-lead-bust-not-likely-systemic-crisis-imf-chief-economist-2025-10-14/?utm_source=chatgpt.com, traduit de l'anglais.*

*(2) Robin Wigglesworth, « Cisco finally did it », The Financial Times, 11 décembre 2025 Cisco finally did it*

*(3) Audition de M. Aiman Ezzat, directeur général de Capgemini, et Mme Karine Brunet, directrice mondiale des opérations et du delivery et membre du comité de direction générale du groupe, le 26 mars 2026*

*personnes dans ce domaine précis. Il y a un grand plan d'investissement dans les compétences lié à cette évolution.* »

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 : 1 800 emplois supprimés en France par la Société générale,1 200 postes dans le monde pour BNP Paribas (1), jusqu'à 20 000 postes chez HSBC d'ici cinq ans (2).

De la même manière, le secteur de la presse est fortement affecté : 400 postes supprimés au sein du groupe EBRA (*Le Dauphiné libéré, L'Est Républicain, Les dernières nouvelles d'Alsace,* etc.), 261 postes supprimés par Prisma Media (*Capital, Femme actuelle, Géo, Voici*, etc.), et 19 postes de rédacteurs supprimés au sein du groupe Infopro Digital (*Le Moniteur, la Gazette des communes, Usine nouvelle*, etc.) (3).

Qu'en est-il de l'impact économique de l'intelligence artificielle ? Les travaux économiques qui mesurent l'impact de l'intelligence artificielle ne sont encore qu'à leurs débuts. Toutefois, certaines études présentent d'ores et déjà des résultats intéressants.

La commission de l'intelligence artificielle, installée par Mme Elisabeth Borne en 2023 et présidée par M. Philippe Aghion et Mme Anne Bouverot, en a réalisé une première synthèse dans son rapport de mars 2024 (4). Pour la commission, l'effet de l'intelligence artificielle est d'automatiser certaines tâches, ce qui crée deux effets contradictoires sur l'activité et l'emploi. D'un côté, l'automatisation remplace l'humain et réduit ainsi l'activité. De l'autre, elle augmente la productivité des individus, ce qui pourrait conduire à diminuer le coût des produits, à la condition que les gains économiques bénéficient effectivement au consommateur et ne soient pas captés par des structures monopolistiques. Ainsi que l'indique le rapport de Philippe Aghion, « *pour comprendre l'effet d'une nouvelle technologie sur l'emploi et le marché du travail, il faut donc comprendre qui de ces deux effets l'emporte Pour cela, deux principales approches ont été retenues. Premièrement, en étudiant directement les effets de l'adoption de l'IA au sein des entreprises ou des secteurs. Deuxièmement, en étudiant les effets de l'IA sur les différentes tâches composant l'économie.* »

---

*(1) « Intelligence artificielle : Société générale et BNP Paribas prévoient des milliers de suppressions de postes », France info, 23 janvier 2026 Intelligence artificielle : Société Générale et BNP Paribas prévoient des milliers de suppressions de postes – franceinfo*

*(2) Nicolas Madelaine, « Intelligence artificielle : HSBC viserait des suppressions d'emplois massives », Les Echos, 19 mars 2026 Intelligence artificielle : HSBC viserait des suppressions d'emplois massives - Les Echos*

*(3) Xavier Eutrope, « IA générative et destructions d'emplois : premier bilan dans la presse française », La Revue des médias, 30 juin 2026 IA générative et destructions d'emplois : premier bilan dans la presse française | la revue des médias*

*(4) Commission de l'intelligence artificielle,* IA : notre ambition pour la France, *mars 2024, https://www.economie.gouv.fr/files/files/directions_services/cge/media-document/commission-IA.pdf*

Deux articles récents, de l'Insee [1] et de la direction générale du Trésor [2], effectuent également une revue de littérature des études économiques sur le sujet.

Les développements ci-après s'appuient, notamment sur la revue de littérature effectuée par la commission de l'intelligence artificielle, et la complètent avec d'autres travaux économiques pertinents sur le sujet, sans néanmoins prétendre à l'exhaustivité.

***a. IA : quel effet sur l'emploi ?***

Sur la base d'une enquête réalisée annuellement par l'Insee, la commission de l'intelligence artificielle réalise un premier travail de comparaison entre 312 entreprises ayant adopté l'intelligence artificielle (non générative) et 897 ne l'ayant pas fait. « *On constate que l'emploi total dans les premières augmente davantage que dans les secondes, alors que ces deux groupes suivaient une tendance antérieure similaire. L'effet résulte principalement de la création de nouveaux emplois, plutôt qu'un maintien plus important d'emplois existants*. (…) *En particulier, certains échelons au sein de l'entreprise ou certains métiers risquent de subir des réductions nettes d'emplois, comme la gestion administrative ou le marketing*. » [3]

La rapporteure note trois éléments sur ce travail de comparaison. Tout d'abord, ce travail est réalisé de 2018 à 2020 alors que l'usage de l'IA est encore peu généralisé. On peut donc supposer que cette étude porte sur des secteurs très spécifiques. Ensuite elle constate que la référence à l'étude de l'Insee n'est pas indiquée. Enfin, une autre étude de l'Insee datant de 2025 et portant sur l'intelligence artificielle dans les entreprises [4], constate que « *l'usage de l'IA augmente avec la taille de l'entreprise : 9 % des entreprises de moins de 50 salariés et 15 % des entreprises de 50 à 249 salariés y ont recours, contre 33 % de celles de 250 salariés ou plus. Ainsi, les entreprises utilisant l'IA concentrent la moitié du chiffre d'affaires total et représentent deux cinquièmes de l'emploi total.* » En l'absence de précisions méthodologiques, la rapporteure s'interroge sur la neutralisation d'autres facteurs pouvant influer sur la dynamique de création d'emplois au sein des deux groupes comparés, et notamment la taille de l'entreprise ou encore la capacité à investir dans des outils numériques.

Une étude américaine publiée en janvier 2024 dans le *Journal of Financial Economics* par Tania Babina, Anastassia Fedyk, Alex He et James Hodson [5] se sert des annonces d'emploi pour identifier les entreprises qui emploient des spécialistes

---

*(1) Raphaële Adjerad, Gaston Vermersch,* Avec l'essor de l'intelligence artificielle générative, l'investissement numérique tire davantage la croissance aux États-Unis qu'en France, tandis que l'emploi recule dans les activités informatiques des deux côtés de l'Atlantique, *Insee, Note de conjoncture, mars 2026*

*(2) Martin Chopard, Elisa Cotet, Tristan Gantois, Eloïse Villani,* L'intelligence artificielle, quels effets sur l'emploi ?, *Direction générale du Trésor, Trésor-Eco, juin 2026*

*(3) Commission de l'intelligence artificielle, ibid.*

*(4) Insee références,* Intelligence artificielle dans les entreprises*, octobre 2025*

*(5) Tania Babina, Anastassia Fedyk, Alex He, James Hodson,* Artificial intelligence, firm growth, and product innovation, *Janvier 2024*

en intelligence artificielle – une façon de disposer de données très larges sur le déploiement de l'IA au sein des entreprises américaines. Les résultats de l'analyse montrent qu'un investissement dans l'IA sur une période de huit ans induit une augmentation des ventes de 19,5 %, de l'emploi de 18 %, et de la valorisation de 22 %. Surtout, l'étude montre que l'effet par lequel l'IA produit ces résultats est une amélioration de l'innovation technologique. En revanche, les auteurs ne trouvent pas de résultat significatif pour l'innovation dans les process, que ce soit pour le chiffre d'affaires généré par employé ou pour l'évolution de la productivité totale des facteurs : « *Dans le cas de l'IA, l'étude de cas détaillée de l'usage de l'IA dans les entreprises révèle l'étendue de ses applications ; d'un point de vue empirique, l'effet de substitution du travail n'apparaît pas comme le principal moteur dans notre analyse. À l'inverse, la relation entre les investissements dans l'IA et la croissance des entreprises semble être déterminée par l'innovation, qui permet aux entreprises de créer davantage de produits, et donc d'accroître leur taille.* » [(1)]

L'étude menée par Erik Brynjolfsson, Danielle Li et Lindsey R. Raymond, publiée en mai 2025 dans le *Quarterly Journal of Economics* [(2)], adopte une approche microéconomique et vise un cas précis : l'adoption d'un outil à base d'IA générative permettant d'assister 5 172 employés du service de support d'une entreprise commercialisant des logiciels à destination des entreprises. Ces employés disposent d'un agent fondé sur le modèle GPT-3 d'Open AI. Le nombre de demandes résolues par heure est accru de 15 % en moyenne. Cette augmentation est essentiellement due à la capacité qu'ont les employés de traiter davantage de demandes, l'amélioration de la capacité à résoudre les demandes étant en revanche faible. L'augmentation de productivité est particulièrement importante pour les employés novices, qui voient leur productivité horaire augmenter de 30 %, alors que l'effet est en revanche faible pour les employés les plus expérimentés. Enfin, ils mettent en valeur les effets positifs en termes de formation : la durée nécessaire pour que les nouveaux employés parviennent aux mêmes performances que les autres employés est abaissé de six à deux mois. De plus, lorsque les employés n'ont plus accès à l'outil pour des raisons de panne, leur productivité continue à être meilleure que lors de la période précédant la mise à disposition de l'outil.

Une autre étude, publiée par Xiang Hui, Oren Reshef et Luofeng Zhou en août 2023 [(3)], montre que l'arrivée de ChatGPT a eu un effet négatif sur l'emploi et la rémunération des travailleurs américains indépendants recrutés sur une plateforme dédiée à l'emploi de travailleurs *freelance* pour des missions de courte durée, en particulier pour la rédaction de textes. Le nombre de missions proposées sur la plateforme diminue de 2 % chaque mois et les revenus touchés par les travailleurs indépendants de 5,2 %. Ceux d'entre eux qui sont les plus expérimentés sont tout aussi touchés. Selon les auteurs, ces résultats suggèrent que l'utilisation

*(1) Traduit de l'anglais.*

*(2) Erik Brynjolfsson , Danielle Li , Lindsey Raymond,* Generative AI at work, *Février 2025*

*(3) Xiang Hui, Oren Reshef, Luofeng Zhou,* The Short-Term Effects of Generative Artificial Intelligence on Employment: Evidence from an Online Labor Market, *août 2023*

des modèles d'IA générative a tendance à niveler les écarts de productivité entre les travailleurs qualifiés et les autres.

Une étude menée par Margueria Lane, Morgan Williams et Stijn Broeck, du département de l'emploi du travail et des affaires sociales de l'OCDE, se base sur une enquête réalisée auprès de 5 300 travailleurs et 2 000 entreprises dans le secteur manufacturier et de la finance dans sept pays (Autriche, Canada, France, Allemagne, Irlande, États-Unis et Royaume-Unis) [(1)]. Si la plupart des employeurs ont déclaré que l'IA n'avait entraîné aucun changement en matière d'emploi au sein de leur entreprise, le nombre de ceux ayant signalé une baisse de l'emploi a dépassé celui des employeurs ayant signalé une augmentation. Dans les entreprises ayant adopté l'IA, 20 % des employés du secteur financier et 15 % des employés du secteur manufacturier déclarent connaître quelqu'un dans l'entreprise qui a perdu son emploi à cause du déploiement d'outils d'intelligence artificielle. 29 % et 24 % ont déclaré connaître quelqu'un qui avait changé de poste à cause de l'IA. Ces baisses pourraient indiquer que l'IA a automatisé davantage d'emplois qu'elle n'en a créés, bien que l'enquête n'ait recueilli aucune donnée sur l'ampleur des pertes et des gains d'emplois – les gains pourraient concerner un nombre plus petit d'entreprises, mais dans des proportions plus grandes.

Enfin, la note de conjoncture de l'Insee précitée revient sur les impacts de l'essor de l'intelligence artificielle. Pour la première fois, elle reconnaît un lien possible entre le développement de l'IA et la baisse de l'emploi des jeunes dans le domaine de l'informatique : « *Plus précisément, les ajustements liés à l'IA pourraient, à court terme, se concentrer moins sur l'emploi total que sur la structure des embauches, en particulier sur les positions d'entrée dans certains métiers (fonctions support, administratif, conseil, certaines tâches de développement et d'analyse), et pénaliser fortement les jeunes. (…)*

« *En France, une analyse semblable est possible à partir des séries d'emploi par âge dans les secteurs des activités informatiques et services d'information, de l'édition et des activités des sièges sociaux et conseil en gestion (…). Elle met en évidence un ajustement de l'emploi concentré sur les jeunes : au quatrième trimestre 2025, l'emploi salarié des 15-29 ans (hors alternants) recule en glissement annuel de 7,4 % dans les activités informatiques, de 5,8 % dans l'édition, et de 3,7 % dans les activités de conseil en gestion, quand l'emploi salarié privé de l'ensemble du secteur marchand non agricole baisse de 0,7 %. (…)*

« *Il est évidemment impossible d'attribuer directement cette évolution à la seule arrivée de l'IA générative car d'une part, l'emploi est globalement en ralentissement en France et d'autre part, ces secteurs peuvent être concernés par un coup de frein conjoncturel. Toutefois, les indicateurs d'activité continuent d'être correctement orientés dans des secteurs qui connaissaient en outre une croissance*

*(1) Margarita Lane, Morgan Williams, Stijn Broecke,* The impact of AI on the workplace: Main findings from the OECD AI surveys of employers and workers, *OECD Social, Employment and Migration Working Papers No. 288, mars 2023*

*régulière de leurs effectifs depuis 20 ans : le retournement paraît ainsi brutal et plutôt concomitant de l'arrivée de cette nouvelle technologie.* »

***b. Quelle est la proportion de tâches de l'économie pour lesquelles les travailleurs sont susceptibles d'être remplacés par des outils d'IA ?***

En complément de l'approche examinant *ex post* les effets de l'adoption de l'IA sur l'activité et l'emploi, une autre approche vise à quantifier, pour chaque métier, *ex ante*, les effets potentiels de l'IA via un « indice d'exposition » à cette dernière, de façon à en déduire des effets potentiels sur l'économie.

Il est intéressant de comparer les travaux publiés au cas de l'entreprise Mistral AI. Son dirigeant M. Arthur Mensch considère « *qu'il n'y a pas encore beaucoup d'études macroéconomiques parce qu'on manque de recul : la délégation de tâche à un agent pendant toute la journée n'est possible que depuis six mois. Je le disais, avec 10 % de notre masse salariale consacrés à l'équipement de notre personnel, nous avons fait un gain de productivité de facteur 2 par rapport à il y a six mois. Ce n'est pas une étude macroéconomique, c'est vrai, mais on parle d'un gain de productivité pour un coût représentant 10 % à 20 % des opex (dépenses d'exploitation) ou de la masse salariale dans le monde.*

« *Certes, la productivité ne sera pas multipliée par deux partout ; chez nous c'est assez facile car, compte tenu de la faible empreinte physique de notre activité, l'utilisation des agents suscite peu de frictions. Dans l'industrie lourde, c'est un peu plus difficile, parce qu'il faut tester des systèmes physiques. Mais pour 10 % de la masse salariale – sachant qu'en général, un client achète une technologie lorsque celle-ci ne lui prend pas plus de 50 % de la valeur –, il y a 20 % de gains de productivité. Il faut avoir en tête que ce ne sera pas forcément 20 % de croissance en plus : il y aura de la croissance mais aussi des destructions d'emplois – du moins une modification des emplois existants.* »

Ce gain de productivité de 20 % à partir d'une dépense de 10 % de la masse salariale, applicable à une entreprise de développement informatique, peut-il être généralisé à l'ensemble de l'économie ?

Une étude de l'Organisation internationale du travail d'août 2023 (1) effectue un premier travail de classification des tâches substituables par le modèle GPT-4. L'intérêt de l'étude est de quantifier l'exposition à l'IA pour chaque poste dans l'économie, mais également de créer une différenciation entre professions « remplaçables » et professions « augmentables ». Si une part importante des tâches qu'exige une profession peuvent être effectuées par l'IA, cette profession a un potentiel de remplacement par l'IA. En revanche, si une profession comprend quelques tâches automatisables, mais une majorité de tâches difficiles à automatiser, elle a un potentiel d'amélioration par l'IA : l'automatisation de certaines tâches permet de libérer du temps pour d'autres.

---

*(1) Pawel Gmyrek, Janine Berg, David Bescond,* Generative AI and Jobs: A global analysis of potential effects on job quantity and quality, *ILO working paper 96, août 2023*

Première conclusion, seules les tâches administratives sont substantiellement exposées à l'IA, à 24 % fortement et à 58 % de façon modérée, soit un total de 72 %. Le reste des catégories d'emplois n'est exposé de façon forte qu'à 4 % au maximum et la part d'exposition modérée demeure inférieure à 25 %.

Seconde conclusion, dans l'ensemble du monde, y compris dans les pays développés, le nombre d'emplois ayant un potentiel d'amélioration par l'IA (13 %) est bien plus élevé que celui ayant un potentiel de remplacement par l'IA (5,1 %).

Au total, seulement 5,5 % de l'emploi total serait concerné par des effets de remplacement au moyen de l'automatisation.

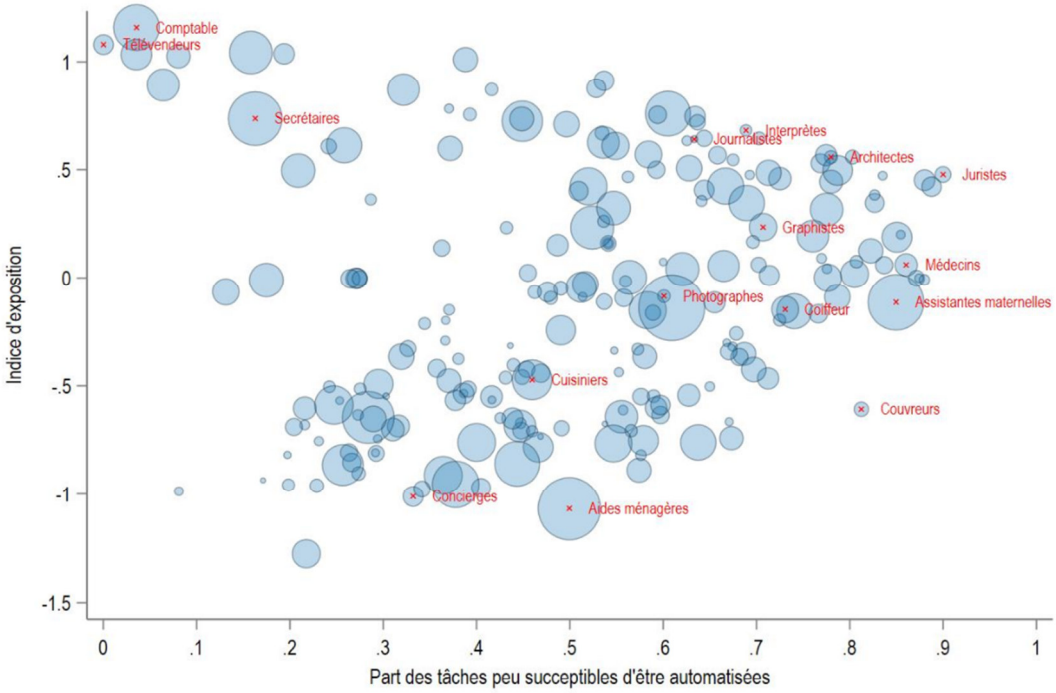
Une étude du Fonds monétaire international adoptant une méthodologie relativement proche aboutit à des taux plus élevés : 60 % des emplois seraient fortement exposés à l'IA, environ la moitié de ces emplois pouvant profiter d'un potentiel d'amélioration par l'IA tandis que l'autre moitié ferait face à un potentiel de remplacement par l'IA.

Le rapport conclut que le développement de l'IA comporte un risque de remplacement d'emplois en raison de l'automatisation, mais comporte également des opportunités en termes de productivité et de complément du travail humain.

Une note d'Antonin Bergeaud de janvier 2024 [(1)], publiée pour le Laboratoire de l'innovation et du futur du travail de HEC, restitue un travail similaire sur des données françaises, afin de dresser un panorama des effets attendus de l'IA sur les familles professionnelles (FAP) définies par la nomenclature du ministère du travail.

*(1) Antonin Bergeaud,* Exposition à l'intelligence artificielle générative et emploi : une application à la classification socio-professionnelle française, *janvier 2024*

**FIGURE 1 : POSITIONNEMENT DE CHAQUE FAP DANS UN REPERE EXPOSITION (AXE DES ORDONNEES) ET PART DES TÂCHES DIFFICILE A AUTOMATISER (AXE DES ABSCISSES). LA TAILLE DE CHAQUE CERCLE EST PROPROTIONNELLE A L'EMPLOI TOTAL DANS LA FAP EN FRANCE EN 2017**




Le graphique positionne ces familles professionnelles sur deux axes : l'exposition à l'IA et la part des tâches peu susceptibles d'être automatisées. Chaque cercle représente le nombre de personnes appartenant à la famille considérée en 2017. Certaines professions comme les juristes, les médecins ou les architectes, évolueront fortement avec l'apparition d'applications basées sur l'intelligence artificielle, mais conserveront néanmoins une part importante de tâches non substituables. Enfin, et de façon assez intuitive, certaines professions comme les cuisiniers, les concierges ou les aides ménagères, sont peu susceptibles d'être fortement exposées.

Enfin, l'Observatoire des emplois menacés et émergents a mené une étude sur les effets de l'intelligence artificielle sur l'emploi à partir d'une analyse fine des tâches au sein de 923 professions. « *L'étude met en évidence une rupture majeure avec les vagues précédentes d'automatisation : l'intelligence artificielle ne prolonge pas les vagues précédentes d'automatisation comme la robotique ou le logiciel, mais en déplace leur centre de gravité vers les tâches cognitives, complexes et non répétitives. Son impact est profondément hétérogène : il se joue d'abord au niveau des tâches, puis se répercute de manière inégale sur les métiers, les familles de métiers et, au-delà, les secteurs qui les concentrent.*

« *Dans le scénario central étudié portant sur le déploiement de l'intelligence artificielle agentique, environ une profession sur huit franchit le seuil de 30 % de tâches automatisables, que l'étude retient comme un seuil de transformation profonde du métier sans pour autant signifier sa disparition. Les professions les plus exposées se concentrent dans les univers à forte intensité cognitive et informationnelle : ingénierie, informatique, fonctions administratives, finance, droit ou encore certains métiers créatifs et analytiques. À l'inverse, les professions les moins exposées restent largement ancrées dans le monde physique ou dans des interactions humaines difficiles à standardiser : production, construction, maintenance, transport, restauration, nettoyage, ou encore certaines activités de soin et d'accompagnement.* » (1)

Mme Axelle Arquière, économiste au Centre d'études prospectives et d'informations internationales et animatrice de l'Observatoire des emplois menacés et émergents, revient dans une interview au *Monde* sur sa perception de la trop faible prise en compte par les responsables politiques du possible impact de l'IA sur l'emploi : « *J'ai le sentiment que les responsables politiques et les économistes ne prennent pas la mesure de ce qui pourrait se passer sur le marché du travail. Ils n'abordent la question que sous l'angle des gains productivité, et minimisent les effets potentiels sur l'emploi. Ce que l'on vit est pourtant peut-être un phénomène comparable à la révolution industrielle. Évidemment, il est impossible d'avoir des certitudes sur son ampleur. Mais une catastrophe sociale, susceptible d'entraîner des répercussions politiques majeures, fait partie des scénarios possibles.* » (2)

### *c. Quel est l'impact global sur l'économie : croissance ou décroissance ? réduction du nombre d'emplois ou diminution ?*

L'approche par l'exposition des tâches à l'IA a l'avantage de permettre de déduire des effets agrégés au niveau de l'économie dans son ensemble. Un document de travail de l'OCDE, publié en novembre 2024, procède à une estimation sur la base d'un modèle d'équilibre général. Les effets dans chaque entreprise, puis dans chaque secteur, sont ensuite remontés au niveau macro-économique : des effets globaux de réallocation des facteurs de production se produiront entre les secteurs touchés négativement et ceux bénéficiant de l'IA.

L'étude présente également une comparaison intéressante des hypothèses en termes d'effet microéconomique de l'IA sur la productivité, de taux d'exposition à l'IA des différents métiers et de taux d'adoption de l'IA. Les auteurs retiennent pour leurs propres travaux les hypothèses suivantes : taux potentiel d'exposition à l'IA – mesurant le pourcentage de tâches pouvant être remplacées par des automatismes – variant de 12 à 50 % avec une moyenne à 35 %, taux d'adoption réel entre 23 et 40 %, gains de productivité de 30 % sur les tâches concernées.

---

*(1) Observatoire des emplois menacés et émergents et COFACE, La nouvelle frontière de l'automatisation, Etude, avril 2026 https://observatoire-emplois-menaces.com/la-nouvelle-frontiere-de-lautomatisation-etude-oem-coface/*

*(2) Axelle Arquié, économiste : « Une catastrophe sociale causée par l'IA fait partie des scénarios possibles », propos recueillis par Pascal Riché, Le Monde, 1er mars 2026*

Les principaux résultats de l'étude montrent bel et bien un accroissement de la productivité globale des facteurs de production compris entre 0,25 et 0,6 point aux États-Unis, à comparer avec le taux de croissance qui est de 1 point de pourcentage en moyenne au cours des vingt dernières années. Il s'agit donc d'une contribution significative, mais toutefois inférieure à celle qui avait été connue au cours de la période 1995-2005 grâce aux nouvelles technologies.

La direction générale du Trésor rassemble les estimations des effets de l'IA sur l'emploi agrégé dans le tableau suivant :

**Tableau 1 : Panel des estimations des effets de l'IA sur le niveau d'emploi agrégé**

| Références | Réaction de l'emploi | Zone géographique |
|---|---|---|
| Hartley *et al.* (2025)[a] | 0 | États-Unis<br>2010-2023 |
| Teeselink (2025)[b] | – | Royaume-Uni<br>2021-2025 |
| Lebastard *et al.* (2026)[c] | 0/+ | Europe<br>2025 |
| Baslandze *et al.* (2026)[d] | 0 | États-Unis<br>2025 |
| Yotzov *et al.* (2026)[e] | 0 | États-Unis, Royaume-Uni, Allemagne et Australie<br>2022-2025 |

a. Hartley J., Jolevski F., Melo V., Moore B. (2025), "The Labor Market Effects of Generative Artificial Intelligence", *SSRN Working Paper*.
b. Teeselink B. (2025), "Generative AI and Labor Market Outcomes: Evidence from the United Kingdom", *SSRN working paper*.
c. Lebastard L., Sondermann D. (2026), "Artificial intelligence: friend or foe for hiring in Europe today?", *ECB Blog*, 4 mars.
d. Baslandze *et al.* (2026), "Artificial Intelligence, Productivity, and the Workforce: Evidence from Corporate Executives", *NBER Working Paper*, 34984.
e. Yotzov *et al.* (2026), "Firm Data on AI", *NBER Working Paper*, 34836.

*Source : Direction générale du Trésor.*

Les auteurs notent qu'« *au niveau agrégé, les gains de productivité peuvent aussi se diffuser via des effets d'équilibre général (baisse des prix, hausse du pouvoir d'achat, redéploiement de la demande vers d'autres secteurs), qui compensent les destructions d'emplois liées à la substitution.* » En l'occurrence, les effets sont nuls ou proches d'être nuls dans quatre études sur cinq recensées, et négatifs dans une seule étude, portant sur le Royaume-Uni.

### *d. Les limites actuelles des travaux économiques*

L'ensemble des travaux présentés fournissent des premiers éléments permettant de conceptualiser les effets de l'introduction des modèles d'IA générative dans l'économie, et de disposer de premières évaluations de leurs effets. Du fait des limites inhérentes aux études économiques (disponibilité des données, difficulté à construire des modèles fournissant une vision complète de l'économie, etc.) et du faible recul historique sur l'adoption de l'IA, quatre réserves doivent être signalées.

Premièrement, les travaux réalisés examinent les chances de disparition de tâches existantes en fonction des technologies disponibles. Elles ne peuvent donc pas tenir compte des tâches qui pourraient être créées à la suite du développement de l'IA ou de futures évolutions dans le domaine de l'IA. Comme l'indique le rapport de la commission de l'intelligence artificielle, *« pour faire un parallèle, il était difficile d'imaginer que le métier de data scientist puisse prendre une telle place au début de la révolution numérique dans les années 2000, ou que le métier de dépanneur en électroménager puisse exister avant l'adoption massive de*

*l'électricité au milieu du XX*ème *siècle ».* De la même manière, il est à ce stade difficile d'identifier toute l'ampleur des tâches automatisables lors des futurs développements de l'IA et des coûts que cela représentera *in fine* pour l'employeur.

Deuxièmement, ces travaux reposent sur une estimation de la probabilité de remplacement par l'IA des différentes tâches, qui est aujourd'hui très subjective. Les études expérimentales se concentrent sur des tâches simples et bien définies, ce qui crée une lacune importante dans la recherche concernant l'impact de l'IA sur les tâches complexes, courantes dans les environnements professionnels. Du fait de l'importance prise par le sujet de l'impact de l'intelligence artificielle sur l'emploi, les travaux économiques ont progressivement affiné leurs méthodes de classification des professions. Une note de travail de l'OCDE, datant du 26 mai 2026 (1), publie ainsi une nouvelle méthode de mesure de l'exposition à l'IA en adoptant une approche complète des compétences requises par chaque profession. Neuf catégories de compétences sont prises en compte, réparties en trois groupes (compétences cognitives, sociales et physiques). Les auteurs présentent leur indicateur non pas comme une mesure directe de l'adoption de l'IA dans les différentes professions, mais plutôt comme un indicateur mesurant des probabilités de déploiement. Utiliser un panel plus complet fait apparaître que l'exposition potentielle à l'IA serait la plus forte dans les métiers dont les tâches sont plus standardisées et codifiables, tandis que des lacunes importantes subsistent dans des domaines tels que l'interaction sociale, la résolution de problèmes et de nombreuses autres tâches nécessitant une incarnation. Les métiers diffèrent non seulement par leur degré d'exposition, mais aussi par les capacités qui déterminent cette exposition.

Troisièmement, le remplacement est comparé tâche par tâche ou profession par profession et ne tient pas compte du contexte et de l'effet d'organisation, propre à chaque entreprise et à chaque secteur. Les facteurs juridiques (ai-je le droit de mettre les données de mes clients à la disposition d'un agent IA sur le cloud ?), éthiques (est-il souhaitable de réaliser de la détection faciale pour fluidifier le passage de la sécurité dans un aéroport ?) et sociaux jouent un rôle essentiel dans la rapidité et la probabilité d'adoption de ces nouvelles technologies.

Quatrièmement, le secteur de l'IA lui-même produit des effets macroéconomiques importants au regard des investissements et des coûts de consommation d'électricité, ce qui peut avoir un impact majeur. La probabilité de remplacement des tâches n'intègre ainsi pas explicitement de fortes variations des coûts d'utilisation de l'IA. Par exemple, les auteurs de l'étude macro-économique citée précédemment indiquent expressément qu'ils n'intègrent pas ces coûts dans leur modélisation. La trajectoire de développement de l'IA pourrait ainsi être fortement enrayée par ses coûts, puisque même M. Bryan Catanzaro, vice-président de l'apprentissage profond appliqué chez Nvidia, reconnaissait dans une interview

*(1)* The OECD AI exposure measure, Mapping the OECD AI capability indicators to occupations, *OECD artificial intelligence papers n° 59, mai 2026*

accordée à Axios : « Pour mon équipe, le coût du calcul dépasse largement celui des employés » (1).

Au-delà des résultats chiffrés auxquels peut parvenir chaque étude, l'ensemble de ces éléments montrent que les mécanismes à travers lesquels l'IA produira un impact sur l'économie sont complexes et difficiles à anticiper. Les travaux économiques sur le sujet sont nombreux et leurs résultats peuvent être parfois contradictoires. L'Insee indique travailler à une étude exploratoire des impacts de l'adoption de l'IA sur l'emploi et la productivité, dont la parution est attendue au premier trimestre 2027.

Que conclure de l'ensemble de ces études ? Si certains secteurs semblent d'ores et déjà touchés largement du fait d'une adoption rapide couplée à l'existence des postes qui se prêtent particulièrement à de la substitution, l'effet global est encore loin de pouvoir être déterminé. La prise de conscience des vrais coûts de l'IA agira aussi comme un fort modérateur des effets de cette technologie sur l'emploi.

Dans ce contexte, la rapporteure comprend les inquiétudes qui montent actuellement sur les impacts économiques de l'IA. Elle s'inquiète également de l'instrumentalisation du sujet pour masquer la volonté de réaliser des profits toujours plus importants. Comme le note la direction générale du Trésor, « *Une partie des annonces de licenciements pourrait aussi relever d'un phénomène de « labellisation ». L'IA servirait alors de justification pour des décisions motivées en réalité par des difficultés structurelles, des ajustements d'effectifs post-Covid ou des considérations de communication financière. Ainsi, 59 % des entreprises américaines admettent utiliser l'IA pour expliquer des gels d'embauche et, dans plusieurs annonces de licenciement, l'IA servirait de prétexte.* »

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

Une telle cellule aurait vocation à rassembler l'État, les partenaires sociaux, France Travail, l'Insee et des chercheurs pour : anticiper les évolutions potentielles de l'emploi liées au déploiement de l'intelligence artificielle ; mettre en place les actions correctives nécessaires.

### 3. Déploiement de l'IA : impacts pour l'économie française dans la compétition européenne et mondiale

Dans l'estimation des impacts de l'IA pour l'économie française, il convient également d'adopter une vision stratégique. La France est-elle bien positionnée ? Quels sont les risques et les opportunités, eu égard des caractéristiques de notre économie et des acteurs concernés par le déploiement ?

(1) *Madison Mills, « AI can cost more than human workers now », Axios, 26 avril 2026* https://www.axios.com/2026/04/26/ai-cost-human-workers

La rapporteure a noté deux phénomènes qui pourraient être source de vulnérabilité : un décrochage technologique et une captation de valeur par des entreprises extra-européennes.

### *a. Les gains économiques sont-ils réels ?*

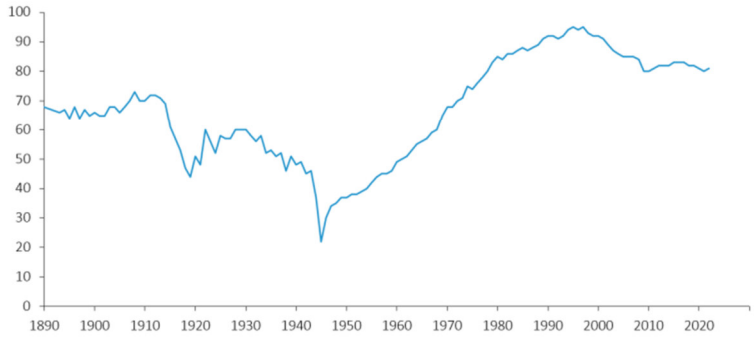
Le lien entre développement technologique et croissance des différentes zones économiques mondiales a déjà fait l'objet de nombreux travaux. L'adoption des technologies numériques est notamment pointée du doigt pour expliquer de l'écart de productivité entre l'Europe et les États-Unis. Par exemple, Robert Gordon et Hassan Sayed [(1)] montrent que la hausse de la productivité aux États-Unis entre 1995 et 2005 fut tirée par les industries fortement intensives en technologies numériques, et par le secteur de la fabrication d'équipements informatiques. Par comparaison, dans dix pays de l'Union européenne, la croissance a connu un ralentissement entre 1995 et 2005 en raison d'une pause dans les investissements en télécommunications, ainsi que de difficultés à capter les facteurs d'efficacité générés par les nouvelles technologies. Après 2005, les économies des deux côtés de l'Atlantique connaissent toutes les deux un ralentissement de leur croissance, ce qui témoignait du caractère provisoire des effets de l'évolution technologique.

Le constat est établi fermement par le rapport Draghi : « *Si la productivité du travail de l'UE a convergé en passant de 22 % du niveau des États-Unis en 1945 à 95 % en 1995, cette croissance a ensuite connu un ralentissement plus marqué qu'aux États-Unis et est repassée en dessous de 80 % du niveau des États-Unis (…)* ».

GRAPHIQUE 1

**Comparaison de la productivité du travail entre l'UE et les États-Unis (1890-2022)**

*Indice (États-Unis = 100)*




*Source : Bergeaud, A., Cette, G., et Lecat, R., «Productivity Trends in Advanced Countries between 1890 and 2012», cité par rapport Draghi.*

« *Le principal facteur expliquant l'écart de productivité croissant entre l'UE et les États-Unis a été la technologie numérique (…) et l'Europe semble actuellement prendre encore plus de retard. La principale raison pour laquelle la*

*(1) Gordon et Sayed,* Transatlantic Technologies: The Role of ICT in the Evolution of U.S. and European Productivity Growth, *NBER, 2020.*

*productivité de l'UE a pris du retard sur celle des États-Unis au milieu des années 1990 a été l'incapacité de l'Europe à tirer parti de la première révolution numérique déclenchée par l'internet — tant en ce qui concerne la création de nouvelles entreprises technologiques qu'en ce qui concerne la diffusion des technologies numériques dans l'économie. De fait, si l'on excluait le secteur technologique, la croissance de la productivité de l'UE au cours des vingt dernières années serait globalement comparable à celle des États-Unis.* »

Selon l'étude de l'Insee précitée, l'économie américaine est aujourd'hui très majoritairement entrainée par la surenchère des géants de la tech dans le domaine de l'IA, à travers deux effets : la haute valorisation boursière des entreprises du numérique et surtout le montant colossal des investissements dans la construction des data centers. « *En dépit d'un marché du travail atone, l'économie américaine a continué de croître (+2,1 % après +2,8 %), entraînée par les investissements massifs dans l'intelligence artificielle et les valorisations galopantes des entreprises du secteur, qui nourrissent la consommation des ménages par effet de richesse* ».

Mais ce phénomène serait plutôt conjoncturel que structurel, et ne traduirait pas une amélioration globale de la productivité de l'ensemble de l'économie. Dans un article, publié par *Mediapart*, « L'IA ou la chasse aux gains de productivité fantômes » [(1)], M. Romaric Godin apporte des éléments permettant de relativiser les apports positifs des investissements numériques sur la productivité : « *Selon une étude de la Réserve fédérale de San Francisco, si l'on exclut les effets de l'investissement dans l'IA du PIB, les gains de productivité de l'économie états-unienne en 2025 sont nuls. Alors même que, selon une étude de mars 2026 du Bureau national de la recherche économique (NBER), la moitié des entreprises états-uniennes avaient déjà investi dans l'IA.*

« *Cette dernière analyse, qui se fonde sur une enquête réalisée auprès de 750 entreprises, tire deux conclusions importantes. D'abord, les gains de productivité « ressentis » sont très supérieurs aux gains de productivité réels de l'IA. Cela est le cœur même du « paradoxe de la productivité » de l'économie contemporaine : l'impact des technologies est surévalué par la « hype » (la forte pression marketing) qui l'entoure. Mais les effets concrets sont relativement faibles.*

« *C'est le produit d'un système circulaire mis en avant par le sociologue Juan Sebastián Carbonell dans son dernier ouvrage Un taylorisme augmenté (Amsterdam, 2025) : la « hype » est nécessaire pour justifier les investissements gigantesques, mais elle produit un écart entre le « ressenti » et la réalité. Les « miracles » vendus par la technologie ne se traduisent pas en production finale de valeur. »*

En Europe se pose une double question : quelle sera la réelle production finale de valeur via l'IA ? Qui captera cette valeur créée si nous dépendons majoritairement d'acteurs américains ?

---

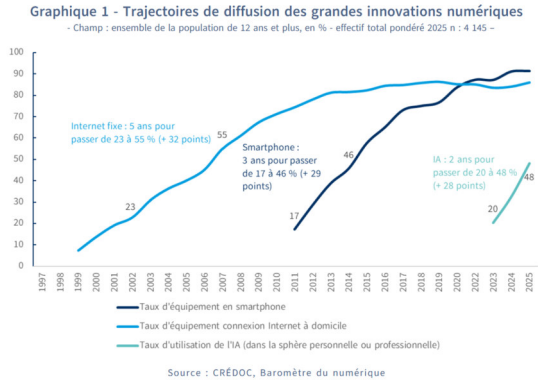
*(1) Romaric Godin, « L'IA, ou la chasse aux gains de productivité fantômes »,* Mediapart, *6 avril 2026*

### *b. Une captation de valeur par les hyperscalers, qui renforceront leur domination*

Avec le déploiement des outils d'IA, les schémas qui ont prévalu lors de l'installation des géants d'aujourd'hui sont en train de se reproduire. La rapidité et la facilité de déploiement est privilégiée au choix de solutions européennes et ouvertes, sans anticipation des situations d'enfermement inévitables.

S'agissant des **outils à destination des particuliers, tout d'abord, l'offre américaine domine fortement le marché des outils d'IA générative.**

Selon le Baromètre du numérique publié par l'Arcep, le Conseil général de l'économie, l'Arcom et l'Agence nationale de la cohésion des territoires (1), la diffusion des outils d'IA au sein de la population est très rapide, davantage que ce qui avait été observé pour internet ou les smartphones. 48 % des Français de plus de 12 ans utilisent aujourd'hui ce type d'outils, ce qui représente 29 millions d'utilisateurs (2).




ChatGPT est utilisé par 79 % des Français utilisant l'IA – soit 22 millions d'utilisateurs d'ores et déjà –, dont 63 % en premier choix, contre seulement 14 % pour Le Chat de Mistral IA – 4 millions d'utilisateurs.

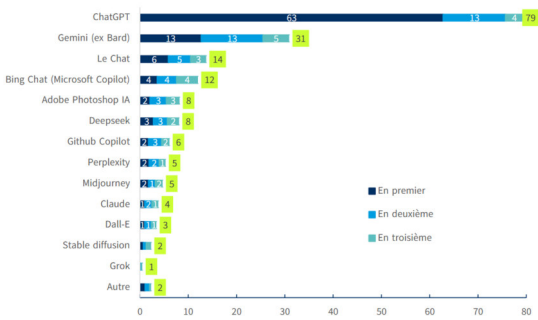
---

*(1) Arcep, Conseil général de l'économie, Arcom et Agence nationale de la cohésion des territoires,* Baromètre du numérique, *février 2026*

*(2) Pour le calcul de la population française âgée de 12 ans ou plus, voir https://www.insee.fr/fr/statistiques/8719824*

Graphique 5 – Fréquence d'utilisation des principaux outils d'intelligence artificielles génératives

- Champ : ensemble de la population de 12 ans et plus qui utilise l'IA, en % - effectif total pondéré 2025 n : 2 002-




L'usage des technologies numériques états-uniennes est donc d'ores et déjà généralisé dans les ménages français.

**S'agissant des outils à destination des professionnels, le déploiement d'outils d'IA non-européens peut avoir des répercussions structurelles importantes.** Dans un article publié en septembre 2025 dans la revue du National Bureau of Economic Research (NBER) (1), Susan Athey et Fiona Scott Morton développent un modèle économique pour tenter de décomposer l'ensemble des effets sur l'emploi et l'activité induits par une captation de valeur des entreprises proposant les modèles d'IA. Cet article ne propose pas de quantification des phénomènes et suppose que le remplacement des tâches réalisées préalablement par des salariés est réel. Dans ces conditions, il met en valeur l'importance du pouvoir de marché dont disposent les entreprises fournissant les modèles. **Lorsque les gains économiques réalisés par ces dernières ne sont pas réinjectés dans l'économie nationale, alors le pays importateur des technologies d'IA souffre de plusieurs conséquences négatives** : les prix des produits ne diminuent pas, car la valeur générée est captée par une entreprise située à l'étranger, et les employés « remplacés » ne peuvent être absorbés dans d'autres secteurs qu'à la condition que les conditions économiques le permettent dans ces secteurs. Il s'agit d'un véritable problème de politique publique, dans la mesure où les entreprises déployant de l'IA ne prennent pas en compte les impacts macro-économiques de ce choix.

L'intérêt principal de l'article est de **mettre en valeur la nécessité de penser d'ores et déjà une régulation de l'accès aux outils d'intelligence artificielle, afin d'éviter des situations dans lesquelles les sociétés fournissant les modèles captent l'essentiel de la valeur, au détriment de l'économie des pays important les outils**. Du point de vue des États, un facteur clé réside dans la localisation de la valeur ajoutée générée par l'IA. Si les entreprises nationales en tirent les bénéfices et que ceux-ci sont largement réinjectés dans l'économie, ils augmentent le revenu national et contribuent à soutenir la demande générale. « *La politique de la concurrence et la politique industrielle pourraient permettre d'améliorer le pouvoir de négociation d'un pays vis-à-vis des fournisseurs*

(1) *Susan Athey, Fiona Scott Morton,* Artificial intelligence, competition and welfare*, NBER, novembre 2025*

*extérieurs. Par exemple, un pays peut être en mesure de contrôler l'accès aux données ou aux systèmes financiers. Il pourrait se demander si les modèles ouverts (tels que Llama de Meta) devraient être réglementés pour des raisons de sécurité nationale (même si l'arrivée de DeepSeek a démontré qu'il peut être difficile d'empêcher les pays de s'inspirer rapidement des innovations d'autrui), compte tenu du rôle que l'open source peut jouer pour limiter les prix de l'IA et favoriser la concurrence dans les services d'IA.* » [(1)]

Le risque que les acteurs existants bénéficient de leur position pour renforcer leur présence sur les services du numérique est très fort.

Dans son avis de juin 2024 relatif à l'IA générative [(2)], l'Autorité de la concurrence met en évidence des barrières à l'entrée très élevées : la nécessité de recourir à des processeurs spécialisés pour l'IA, très coûteux et dont l'accès est réservé à quelques entreprises seulement ; l'importance du contrôle des services cloud ; la nécessité de disposer de larges volumes de données ; la maîtrise des compétences pointues en apprentissage automatique et apprentissage profond ; et un besoin de financement important. Les grandes entreprises du numérique « *bénéficient d'un accès privilégié aux intrants nécessaires pour l'entrainement et le développement des modèles de fondation. Ces avantages ne sont pas aisément réplicables par les développeurs de modèles de fondation concurrents qui n'ont pas accès à ces intrants dans les mêmes conditions* ». Elles bénéficient également d'avantages liés à leur intégration verticale et conglomérale.

Enfin, elles déploient nativement leurs propres outils d'IA dans leurs écosystèmes de produits et de services. « *Ainsi, Microsoft déploie ses propres modèles et ceux de son partenaire OpenAI dans la fonction « Copilot » afin d'améliorer la fonctionnalité de recherche de Microsoft Bing et propose un assistant IA conçu pour fonctionner avec l'offre Microsoft 365*. »

La contribution écrite de Microsoft France sur les atouts concurrentiels de Google dans le domaine de l'IA corrobore en tous points des éléments d'analyse de l'Autorité de la concurrence, puisqu'elle décrit exactement les mêmes phénomènes de présence renforcée sur toute la chaîne pour son concurrent : « *La concurrence dans le cloud n'est pas alimentée par d'anciens logiciels comme Windows Server. Cela n'a jamais été aussi évident qu'aujourd'hui. Dans ce nouveau paradigme de cloud computing piloté par l'IA, Google bénéficie au contraire d'avantages uniques : un marché plus important et un chiffre d'affaires annuel supérieur à Microsoft ; ses propres puces IA (TPU) ; une empreinte mondiale massive de centres de données qui fournit du calcul à la demande ; le plus grand parc de données au monde, alimenté en continu par les services grand public les plus utilisés au monde ; Deep Mind, un laboratoire de recherche en IA de premier plan acquis il y a des années ; et une capacité inégalée à atteindre les consommateurs*

*(1) Traduit de l'anglais*

*(2) Autorité de la concurrence, Avis 24-A-05 du 28 juin 2024 relatif au fonctionnement concurrentiel du secteur de l'intelligence artificielle générative*

*via Android et Chrome. Ce sont tous des atouts plus importants pour l'avenir de l'informatique en nuage que les logiciels comme Windows Server* » [1]. Plus que toute autre entreprise, les *hyperscalers* sont les mieux placés pour bénéficier du boom de l'intelligence artificielle : par leur accès aux données et aux clients, leurs ressources financières, et le maillage extrêmement étroit de l'écosystème américain de la tech.

En conclusion, l'irruption de l'IA pourrait produire des effets durables sur notre économie, qu'il est toutefois difficile de quantifier aujourd'hui. L'éclatement d'une bulle est tout à fait possible, si les revenus tardent à se matérialiser ou si l'économie physique ne parvient pas à suivre le rythme du numérique. Mais le déploiement de l'intelligence artificielle générative aura quoiqu'il arrive un impact sur une partie de la population active, à moyen et long terme. Les enjeux systémiques pour la France sont de quatre ordres :

– identifier les limites physiques au déploiement de l'IA, qu'elles soient technologiques ou climatiques ;

– déterminer les secteurs où l'IA apporte un effet réellement positif ;

– suivre les impacts de l'IA sur l'emploi ;

– créer un cadre favorable à la création et au déploiement d'outils européens, afin d'être capables de définir nos propres règles et d'éviter une captation de valeur et l'enfermement dans des solutions propriétaires.

### B. LES RISQUES TECHNIQUES

Les transformations économiques structurelles induites par le déploiement de l'intelligence artificielle se doublent d'enjeux techniques qui pourraient conduire à devoir repenser la régulation de l'ensemble des secteurs de l'économie.

#### 1. Risques généraux liés à la diffusion généralisée de l'IA, et en particulier de l'IA agentique

De manière générale, le déploiement de l'IA pose la question du contrôle humain face à des modèles dont il est par construction impossible de prédire le résultat des actions. C'est en particulier le cas de l'IA agentique, dont l'objectif est de venir remplacer des personnes dans la mise en œuvre d'actions ayant des conséquences concrètes. Ainsi que le relève Mme Meredith Whittaker, « *s'agissant de l'IA agentique et de son intégration dans les systèmes d'exploitation, qu'elle soit mise en œuvre directement par les fournisseurs ou par l'intermédiaire de dispositifs qui incitent les utilisateurs à accorder à ces agents des permissions extrêmement intrusives leur ouvrant l'accès à l'ensemble de leurs données, notre inquiétude est, évidemment, très vive. Voilà en effet plusieurs années que nous exprimons nos*

*(1) E-mail de M. Lionel Benatia, directeur des affaires publiques France de Microsoft adressé à la rapporteure et au président, 10 juin 2026.*

*réserves face à ces évolutions nouvelles. Nous observons en effet une pression croissante en faveur d'une intelligence artificielle appelée à exercer toujours davantage de contrôle sur nos vies et à agir de manière autonome, alors même que le paradigme agentique entre en contradiction directe avec les exigences de cybersécurité et de protection de la vie privée. Le terme même d'agent, qui n'a rien d'anodin sur le plan technique, désigne en réalité un système qui remplit deux fonctions. D'une part, pour pouvoir agir en votre nom, l'IA doit accéder à votre univers, à votre environnement, à votre contexte, autrement dit à vos données, de sorte qu'une masse considérable d'informations devient soudainement accessible. Ces données sont, très vraisemblablement, transmises ailleurs, car la puissance de calcul disponible sur la machine de l'utilisateur ne suffit généralement pas à les traiter localement. D'autre part, l'agent exploite ces données pour agir sans solliciter votre autorisation, puisqu'il doit précisément disposer d'une capacité d'action autonome. S'il devait demander une validation à chaque étape, il ne s'agirait plus d'un agent. Ce paradigme est donc déjà porteur de tensions, et nous constatons des pressions croissantes en faveur de l'intégration de ces agents, soutenues par des investissements massifs en capitaux et par la recherche du modèle adéquat pour le marché grand public.* » (1)

Les « tensions » évoquées par Mme Whittaker joueront un rôle déterminant dans l'ampleur de la dissémination de l'IA au sein de l'ensemble des systèmes. Laisser une grande autonomie aux outils agentiques pourrait permettre d'améliorer la productivité grâce à l'automatisation complète d'un grand nombre de tâches (avec des risques sur l'emploi à ce stade non étudiés). Mais cela suppose de se priver de la possibilité de tout contrôle compte tenu de l'opacité du fonctionnement des modèles, y compris pour leurs propres créateurs et utilisateurs.

Le cas du secteur financier constitue un exemple intéressant à cet égard. L'adoption massive de l'IA peut être à l'origine de risques pour la stabilité du système financier dans son ensemble (risques « macroprudentiels »). Outre le risque cyber (voir *infra*), au plan microprudentiel, c'est-à-dire pour chaque institution prise individuellement, l'utilisation d'IA peut engendrer des risques pour la solidité de l'établissement. Un modèle de tarification mal calibré peut générer des pertes. Globalement, la complexité et la nouveauté de certaines modélisations peuvent en effet donner lieu à davantage d'erreurs, soit dans la conception, soit dans l'utilisation des systèmes.

Pour la clientèle, l'utilisation d'IA fait courir le risque d'un traitement inapproprié – y compris discriminatoire –, des risques pour la vie privée lorsqu'il y a traitement de données personnelles, mais aussi des risques de mauvaise information, voire de manipulation, dans la relation commerciale.

L'opacité des décisions algorithmiques, générant un phénomène de boîte noire, pose la question de la protection de la clientèle, car un client doit pouvoir comprendre la décision automatisée prise à son égard. C'est aussi un enjeu de

*(1) Audition, ouverte à la presse, de Mme Meredith Whittaker, présidente de la fondation Signal, le 25 mars 2026.*

gouvernance : un établissement qui comprend mal les décisions que prennent ses systèmes d'IA ne peut prétendre en maîtriser les risques. À l'inverse, l'utilisation d'outils destinés à la lutte contre le blanchiment ou le financement du terrorisme peut constituer un cas d'usage bénéfique.

### 2. Le sujet critique de la cybersécurité

Le 12 juin 2026, le gouvernement américain exigeait d'Anthropic la suspension de l'accès des étrangers à ses modèles Fable 5 et Mythos 5 (1). Cette décision met en lumière les impacts globaux que pourrait avoir le déploiement de l'IA sur la cybersécurité.

Le cas d'une fermeture de l'accès des modèles aux non-États-uniens crée un déséquilibre flagrant. Il est particulièrement alarmant de constater que la sécurité de l'ensemble de nos systèmes d'information dépend de la décision unilatérale de la société Anthropic de fermer l'accès à ses modèles pour l'ensemble de ses clients, y compris états-uniens. Mais au-delà du choc médiatique et politique que constitue cet épisode, il faut en réalité considérer Mythos comme le premier de la catégorie des modèles frontière. Ainsi que l'indique une note du Campus cyber, « *Mythos doit donc être dé-« mythifié » : prendre le modèle moins pour ce qu'il est et ce qu'il est capable de faire, que pour ce qu'il dit et ce qu'il révèle des grandes lignes de force qui refaçonnent le paysage de la cybersécurité sous nos yeux. L'essentiel n'est pas dans la manifestation du phénomène à un instant T, mais dans la pente de la courbe. Il faut appréhender Mythos moins comme une rupture technique que comme le dernier signal en date d'une accélération très forte des modèles* » (2). Mythos sera ainsi suivi par de nombreux modèles aux performances qui ne cesseront de s'améliorer.

Devant la commission d'enquête, M. Vincent Strubel, directeur général de l'Anssi, dressait le constat suivant : « *Nous n'avons pas accès à Mythos. Comme la plupart des observateurs, nous l'analysons à partir de témoignages indirects, ce qui invite à une certaine prudence. Ce qui en ressort, au-delà du discours porté par Anthropic, c'est moins une rupture qu'une étape marquante dans une trajectoire déjà engagée. L'évolution était prévisible et elle va se poursuivre. En cela, Mythos ne constitue pas un cas isolé appelé à dominer durablement le paysage car d'autres acteurs atteignent déjà des niveaux comparables, et les prochaines générations de modèles iront plus loin. Nous sommes face à une dynamique d'amélioration continue, dont l'accélération impose de raisonner à moyen terme plutôt qu'en termes de rupture ponctuelle.*

« *Dans ce contexte, l'intelligence artificielle devient effectivement de plus en plus apte à identifier des vulnérabilités et à produire du code permettant de les exploiter. Cela ne signifie pas qu'un modèle comme Mythos soit aujourd'hui*

---

*(1) Communication de l'entreprise Anthropic, juin 2026, https://www.anthropic.com/news/fable-mythos-access*

*(2)* Mythos et autres modèles-frontière : implications des progrès de l'IA pour la cyber en France et en Europe, *Campus cyber, note d'analyse, mai 2026*

*capable de conduire de manière autonome une cyberattaque de bout en bout, mais il peut fournir à un attaquant humain des éléments crédibles, tant pour la détection des failles que pour leur exploitation. La conduite complète de l'attaque, avec la compréhension de l'infrastructure et l'enchaînement des actions, demeure en revanche du ressort humain. Il s'agit d'une évolution significative et la réponse à votre deuxième question est donc positive : il faut intégrer ces évolutions dans nos logiques de certification et, plus largement, dans la production logicielle. Nous sommes déjà, collectivement, en difficulté face aux vulnérabilités puisque des dizaines de milliers sont découvertes chaque année, non pas seulement à la sortie des logiciels, mais sur des systèmes déjà en circulation, et elles peuvent être exploitées très rapidement. Cela impose de traiter un flux continu de correctifs, que la plupart des organisations ne parviennent pas à absorber dans les délais, même sans l'apport de l'IA. Des architectures de défense en profondeur permettent d'en atténuer les effets, mais elles ne dispensent pas de traiter le problème à la source, dès la conception des logiciels.* »

Ce constat appelle plusieurs commentaires. Tout d'abord, il convient de préciser que Mythos est capable de conduire une attaque de bout en bout pour des systèmes mal protégés. C'est ce qui ressort de l'évaluation du modèle effectuée par l'AI Security Institute, une agence de recherche du ministère des sciences, de l'innovation et des technologies britannique (1) : « *Le succès de Mythos Preview sur un champ d'entraînement cyber montre qu'il est au moins capable d'attaquer de manière autonome des systèmes d'entreprise de petite taille, faiblement défendus et vulnérables, pour lesquels l'accès au réseau a été obtenu (…) Nos tests démontrent que Mythos Preview peut exploiter des systèmes présentant une posture de sécurité faible, et il est probable que d'autres modèles dotés de ces capacités soient développés.* »

À mesure que les performances des modèles s'amélioreront, ces derniers seront en mesure de s'attaquer à des systèmes d'information de mieux en mieux protégés, y compris ceux sur lesquels repose le fonctionnement d'infrastructures et services critiques. De telles capacités nouvelles pourront être mises à disposition dans des échelles de temps très rapides, ne laissant pas la possibilité de mettre en place les corrections nécessaires.

Selon le Campus cyber, « *les dirigeants d'organisations doivent se préparer à une vague (certains experts n'hésitent pas à parler de « déluge ») de découverte massive de zero days mises au jour par l'IA, avec un effet de purge - en un seul bloc - de vulnérabilités anciennes logées dans des logiciels largement répandus et dans des systèmes complexes et plus anciens (ex. environnements bancaires legacy, systèmes industriels …). Ce pic, que les experts jugent possible d'ici 3-6 mois, pourrait être suivi de plusieurs répliques, par paquets de plus petite taille, puis par une longue traîne de disclosures au compte-gouttes. (…) Le jour où la vague arrivera, l'agenda opérationnel des équipes informatiques sera bouleversé. Les organisations se retrouveront face à la nécessité de corriger en urgence un volume*

(1) https://www.aisi.gov.uk/blog/our-evaluation-of-claude-mythos-previews-cyber-capabilities, *traduit de l'anglais*

*potentiellement considérable de vulnérabilités, pour laisser aux attaquants aussi peu de prise et de temps que possible pour les exploiter, dans un contexte où le TTE (time-to-exploit) ne fait que baisser depuis de nombreuses années. À ce moment-là, c'est l'ensemble de la chaîne logicielle, et plus largement de la chaîne opérationnelle de l'IT, qui sera mise sous une tension inédite, du fournisseur à l'intégrateur jusqu'au client (…) En raison des goulets d'étranglement prévisibles sur la chaîne d'approvisionnement des patchs logiciels et sur la capacité des utilisateurs finaux à adopter les cadences requises pour éliminer tout risque d'exploitation des vulnérabilités,* ***il faut s'attendre à un accroissement structurel du nombre de cyberattaques réussies, y compris sur des systèmes critiques****, sauf à imaginer un système dans lequel l'IA met à disposition de l'ensemble des équipes cyber, en tous points et à tout instant, les solutions correctives en même temps qu'elle révèle les failles, ce qui est illusoire.* »

Aucun garde-fou mis en place par les sociétés développant les modèles ne peut garantir que ces derniers ne soient utilisés pour mener des attaques. Il s'agit bien de la raison invoquée par le gouvernement américain pour justifier la suspension des modèles Mythos et Fable d'Anthropic. L'obligation de coupure d'accès à Mythos de la part de Donald Trump se produit alors qu'Anthropic s'apprêtait à partager ce modèle avec 150 organisations dans plus de quinze pays dans le cadre de son projet Glasswing [(1)]. Eu égard au comportement du président américain à l'égard de l'Europe et du reste du monde, cette rupture d'accès doit être perçue comme une marque d'hostilité.

La société précisait dans son communiqué [(2)] : « *Notre compréhension est que le gouvernement estime avoir découvert une méthode permettant de contourner les restrictions de Fable 5 » (« jailbreaking »)* ». Anthropic considère que les garde-fous (« *safeguards* ») mis en place sur ses modèles sont extrêmement forts : « *Nous avons mis en place des garde-fous robustes qui réduisent considérablement le risque que Fable soit utilisé à mauvais escient pour des tâches liées à la cybersécurité (entre autres). En effet, garde-fous sont si robustes que de nombreux utilisateurs se sont plaints de leur portée trop large* ». Toutefois, l'entreprise reconnaît, d'une part, que toute mesure de protection est vulnérable à un contournement des garde-fous non universel. D'autre part, « *il est probable qu'un contournement universel des garde-fous sera finalement trouvé dans le futur* ». **C'est pourquoi Anthropic a imposé aux utilisateurs du modèle Fable que l'ensemble de leurs données (prompts et sorties) soient conservées pendant une durée de trente jours sur toutes les plateformes sur lesquelles ces modèles sont déployés [(3)].**

En conclusion, la dépendance aux solutions extra-européennes n'a jamais été un enjeu aussi critique en matière de cybersécurité :

---

*(1) Sébastien Gavois, « La Fable, le Mythos et la raison d'État », Next, 15 juin 2026 https://next.ink/235941/la-fable-le-mythos-et-la-raison-detat/*

*(2) Communiqué de l'entreprise Anthropic, ibid.*

*(3) https://support.claude.com/en/articles/15425996-data-retention-practices-for-mythos-class-models*

– les Européens n'ont pas à leur disposition aujourd'hui les modèles frontière ;

– s'ils y avaient accès, la mise en place de mesures de sauvegarde impliquerait une vulnérabilité sur leurs données, et l'impossibilité d'opérer ces modèles sur des infrastructures sécurisées ;

– lorsque les modèles détecteront des blocs entiers de vulnérabilités anciennes dans les logiciels utilisés, les utilisateurs européens seront dépendants du rythme des mises à jour de leurs fournisseurs états-uniens sur les logiciels qu'ils utilisent ; dans un contexte de forte tension, le risque est de ne pas être traités de façon prioritaire ;

– la localisation des leaders internationaux en termes de modèles d'IA aux États-Unis ou en Chine rend impossible une régulation du déploiement de ces outils, que ce soit via une interdiction ou une diffusion plus lente.

Face à cette situation, le Campus cyber appelle l'Europe à « *positionner offensivement ses entreprises les plus avancées de l'IA en B2B (au premier chef Mistral AI) en priorité sur les cas d'usage cyber, en leur mettant à disposition davantage de puissance de calcul pour construire une IA souveraine et performante pour la cybersécurité* ». Cette recommandation ne peut qu'aller de pair avec un contrôle extrêmement fort du développement de ce type de technologies. Qu'il soit américain, chinois ou européen, un modèle frontière sera toujours vulnérable à un contournement des garde-fous.

### C. DE NOUVELLES VULNÉRABILITÉS SOCIALES ET CULTURELLES

Enfin, le déploiement de l'intelligence artificielle doit être examiné au regard de ses potentielles conséquences sociales et culturelles.

Le recours généralisé à des outils d'IA pourrait conduire à une déshumanisation du travail.

Comme l'indique M. Henri Verdier, « *c'est grave car cela se traduit par une domination économique, avec une évasion de valeur puisqu'on achète à l'extérieur, mais surtout par une domination sur les chaînes de valeur, à laquelle nous ne prêtons pas assez attention. Vous souvenez-vous du rapport publié en mars 2025 par l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (Anses) sur la condition des livreurs Deliveroo ? Il met en lumière la vie infernale de ces travailleurs qui ne rencontrent plus ni collègues, ni supérieurs hiérarchiques. Soumis à un management algorithmique, ils reçoivent des stimulus de data (données) toute la journée et leur salaire horaire a diminué de 35 % en deux ans. Nous sommes tous en passe de devenir des chauffeurs Deliveroo !* »

Mme Lou Welgryn, secrétaire générale de Data for Good, alerte aussi sur les risques liés à l'irruption de l'IA dans notre quotidien [1] : « *Je voudrais aussi revenir sur le terme d'« amélioration du quotidien ». Sans nier que l'intelligence artificielle puisse avoir des impacts positifs dans certains domaines précis, il faut clarifier qu'il n'est pas du tout acquis qu'elle améliore globalement notre quotidien. Si je prends l'exemple du travail, ce que nous observons aujourd'hui est plutôt une intensification pour certaines personnes, avec une concentration accrue des tâches et davantage de sollicitations, ainsi qu'une précarisation pour de nombreuses autres. Les plus jeunes rencontrent des difficultés d'emploi, et certains métiers, comme la traduction, sont massivement précarisés. Tous ces éléments doivent être considérés lorsqu'on évalue les impacts généraux de ces infrastructures et de leur hégémonie dans la société.* »

Les premières études, telles que le document de travail de l'OIT précédemment cité, mettent en valeur l'impact potentiellement plus important pour les femmes.

La généralisation de modèles d'IA non européens pourrait également mener à une situation dans laquelle la sphère informationnelle n'est plus contrôlable, à la merci de contenus imposés par les États-Unis ou la Chine. Ainsi que l'indique M. Arthur Mensch : « *l'intelligence artificielle, parce qu'elle génère du contenu, façonne les représentations culturelles, la langue, l'éthique. En effet, les modèles que nous créons ont une certaine politique ; ils actionnent certains leviers, ils écrivent un certain type de code, etc. Tout cela devient une médiation de l'information et une médiation de l'action. Faute de solution alternative européenne, nous serons contraints d'importer des modèles, donc nous dépendrons de choix faits par d'autres, les États-Unis et la Chine en particulier, et des biais qui en découlent* ».

De manière plus générale, M. Bastien Le Querrec, juriste à l'association La Quadrature du net, souligne l'enjeu de la souveraineté informationnelle : « *si la notion de souveraineté financière ou politique est désormais bien identifiée, et si la question de l'utilisation de services en ligne, de solutions d'hébergement ou de logiciels entretenant un lien direct avec des pays étrangers est régulièrement soulevée, celle de la souveraineté informationnelle me paraît, pour sa part, devoir faire l'objet d'une attention particulière aujourd'hui. Il s'agit de s'interroger, indépendamment de l'origine ou du contrôle des capitaux, sur les effets produits en matière d'information et de représentation du réel par l'usage des outils numériques. Tel est notamment le cas des réseaux sociaux qui, à travers leurs mécanismes de hiérarchisation algorithmique des contenus, sont susceptibles de déformer la réalité ou de proposer une vision particulière de la société et du monde qui nous entoure. Cette problématique est particulièrement manifeste s'agissant de X, réseau social dont les dérives en matière de manipulation algorithmique sont désormais largement documentées, mais elle concerne, plus largement, l'ensemble des plateformes sociales commerciales.* » [2]

---

*(1) Table ronde, ouverte à la presse, sur les infrastructures numériques, 2 avril 2026*

*(2) Table ronde, ouverte à la presse, réunissant des associations sur le thème de la protection des données personnelles, le 25 mars 2026.*

Enfin, se pose la question du respect de nos règles, au premier rang desquelles figure le respect du droit d'auteur. Le développement des modèles d'IA repose sur l'absorption de données sans aucun regard pour les droits de celles et ceux qui ont produits ces données, qu'elles soient littéraires, journalistiques, ou scientifiques. Une proposition de loi adoptée au Sénat à ce sujet a été l'objet d'un lobbying intense lors de son passage à l'Assemblée nationale. Les acteurs de l'IA générative, au premier rang desquels Mistral AI, ont largement plaidé contre son adoption et son examen en séance. Le texte n'a à ce jour pas été examiné par l'Assemblée nationale. L'opposition ferme à la réaffirmation d'un principe de droit montre les limites d'un modèle qui reviendrait uniquement à copier le modèle américain. La souveraineté ne peut être uniquement économique. Cette dernière doit permettre le développement d'un écosystème numérique qui répondrait aux règles et aux valeurs européennes.

## CHAPITRE 12 – LES DATA CENTERS : INSTRUMENTS CLÉS DE LA DOMINATION DES GAFAM ?

La démultiplication des projets de data centers de grande taille est directement liée à la perspective d'un développement de l'intelligence artificielle. En effet, les infrastructures physiques sont une composante essentielle de l'IA, puisqu'elles sont la condition de fonctionnement des modèles. Le Sommet de l'IA à Paris en février 2025, voulu par le Président de la République, a été l'occasion de lancer une politique offensive de déploiement de data centers sur le territoire. Cette politique pose plusieurs questions :

– la trajectoire d'augmentation de la consommation électrique des data centers est-elle soutenable, et assistera-t-on à des phénomènes de captation de la capacité électrique par certains acteurs ?

– la localisation physique des data centers est-elle un moyen de retrouver un contrôle sur l'activité de l'IA de façon à en diriger les bénéfices vers le pays d'implantation ?

### A. POURQUOI IMPLANTER DES DATA CENTERS EN FRANCE ?

Les caractéristiques du réseau internet font que le développement de l'IA, tant pour l'entraînement des modèles que pour l'inférence, peut s'effectuer de façon distribuée, en recourant à un réseau de câbles interconnectés et de data centers répartis sur l'ensemble de la planète. Toutefois, plusieurs raisons peuvent justifier la localisation d'un data center d'IA dans un pays en particulier.

#### 1. Raisons techniques

Il existe tout d'abord une raison technique : utiliser des capacités de calcul qui sont éloignées des lieux où sont effectués les requêtes crée un délai de latence de quelques millisecondes qui peut pénaliser certaines applications. Cela peut concerner par exemple l'utilisation d'assistants vocaux ou encore des usages industriels associant des capteurs à des commandes. Le critère important sera alors la distance géographique, et pas nécessairement l'implantation sur le territoire national (un data center à Amsterdam pourrait être plus intéressant pour un industriel français basé à Dunkerque qu'un data center à Marseille).

Toutefois, la localisation sur le territoire de grandes capacités de traitement de données serait de nature à favoriser l'implantation d'activités nécessitant les temps de latence les plus réduits.

### 2. Raisons économiques

Ensuite, il s'agit de capter l'activité économique générée par les data centers, qui peut être décomposée en plusieurs éléments :

– l**a construction** (incluant la préparation de site, le génie civil, le montage et les tests de recette) **et l'exploitation des infrastructures** : ces activités sont peu délocalisables. Si elles sont intensives en emploi au moment de la construction, elles le sont peu lors des phases d'opération. Ainsi que l'indiquait M. Fabrice Coquio, président-directeur général de Digital Realty, « *Quant à l'impact direct de ces infrastructures pour le territoire concerné, il s'observe d'abord pendant la phase de construction : le chantier en cours à Marseille emploiera 400 à 450 compagnons pendant deux ans, sans parler des machines que nous sommes susceptibles d'acheter à des fabricants français ou européens (…). Contrairement à ce qu'on pense parfois, on pourrait presque dire qu'un data center fourmille : en moyenne, dans chacun de nos quatre centres marseillais, 120 à 170 personnes entrent et sortent par tranche de vingt-quatre heures.*

« *(…)* ***Il est vrai que les data centers restent des infrastructures : ils sont intensifs en capital plus qu'en salariés***. » Une autre estimation du nombre d'emplois directs créés par l'activité des data centers est fournie par AWS : *« Selon nos estimations internes élaborées dans le cadre de nos dossiers de demandes de permis, chaque 1 000 m² de surface de centre de données génère environ 2,5 équivalents temps plein internes et 4,8 équivalents temps plein externes. Ces ratios sont indicatifs et sont susceptibles d'évoluer au fil de l'avancement d'un projet, de la finalisation des choix technologiques et de l'intégration de nouvelles innovations* ». [(1)]

M. Yoann Ferron, spécialiste chez Randstad du recrutement dans le domaine technologique, indique que les principaux métiers recherchés sont ceux de la maintenance hardware et du génie climatique, et compare les data centers aux plateformes logistiques en termes de densité d'emplois. Il estime qu'un data center avec une puissance installée de 100 mégawatts (MW) crée une trentaine d'emplois liés à l'exploitation [(2)].

Les retombées en termes d'emploi seront donc probablement bien plus limitées que le nombre d'emplois annoncés par les constructeurs.

– la **fourniture des équipements**, qui comprend les serveurs et les autres équipements, en particulier électriques. La valeur ajoutée localisée en France dépend ainsi de la part et de la provenance de chaque équipement dans le montant total des investissements. Les puces sont aujourd'hui intégralement achetées auprès de Nvidia, donc avec une valeur ajoutée quasi inexistante en France.

---

*(1) Audition de M. Fabrice Coquio, président-directeur général de Digital Realty, le 12 mai 2026.*

*(2) https://www.banquedesterritoires.fr/centres-de-donnees-un-ratio-coutemplois-qui-interroge*

– la **fourniture d'électricité** [1]. D'après M. Arthur Mensch, « *dans la chaîne qui va de l'électron au token, l'électron représente à peu près 10 % du coût total* ». La valeur ajoutée est essentiellement française, même si des volumes peuvent être achetés à des producteurs localisés à l'étranger dans le cadre du marché européen de l'électricité. Il est également important de mentionner que l'augmentation des volumes d'électricité vendus permet de rémunérer les actifs de réseau. Elle est donc bénéfique à l'économie globale du système électrique, à la double condition que cette augmentation n'accroisse pas les besoins en renforcement de réseau dans des proportions supérieures et que les consommateurs raccordés acquittent l'intégralité des tarifs de transport d'électricité.

– le **financement des infrastructures, en dette bancaire et en fonds propres** (*equity*). Lorsque les projets de data centers ou les installations en activité sont détenus par des fonds d'investissement, les sociétés jouant le rôle de *general partner* sont celles qui sont impliquées directement dans la gestion de la société. Elles prélèvent des frais de gestion (*management fees*, représentant 2 % des montants investis) et une part des profits réalisés (*carried interest*, 20 % des profits réalisés) [2]. Les sociétés impliquées en tant que *limited partner* sont des fonds d'investissements internationaux, mobilisant des fonds issus de l'ensemble des pays. Comme démontré plus haut, les fonds proviennent majoritairement d'acteurs extra-européens, limitant ainsi les impacts positifs pour l'économie.

– qu'en est-il de **l'activité de vente du calcul** à proprement parler ? Il s'agit de la partie principale, qui constitue le cœur de la valeur ajoutée du modèle économique de l'intelligence artificielle, la transformation de l'électron en token. De ce point de vue, la localisation du data center n'assure pas le retour de cette valeur dans le pays, ni l'utilisation par des clients nationaux. Interrogé sur la part que représentaient ses clients extra-européens, M. Coquio indiquait [3] : « *Elle est grosso modo de 50 %. C'est le cas en France comme, du reste, dans chacun des pays européens où nous sommes implantés, sauf à Marseille, où la part des clients étrangers est plutôt de 60 % à 70 %. En effet, dans l'organisation mondiale de la donnée, trois zones métropolitaines – Singapour, Miami et Marseille – sont, du fait de leur situation géographique, des gateways, c'est-à-dire, des portes d'entrée et de sortie. Si Marseille est devenue très rapidement le sixième hub mondial et croît d'environ 30 % par an, c'est parce qu'elle se situe à l'interface entre, d'un côté, l'hinterland, c'est-à-dire le cœur européen – Paris, Francfort, Londres, Amsterdam –, et, de l'autre, l'Afrique, le Moyen-Orient, l'Inde et l'Asie. Un peu plus de 5 milliards d'êtres humains sont connectés à Marseille ! C'est pourquoi les clients étrangers sont surreprésentés dans ce hub (…) À Marseille, par exemple, 20 % des flux traités concernent l'Inde* ».

---

*(1) Les autres intrants représentent un poids économique marginal par rapport à l'électricité*

*(2)* https://www.investopedia.com/terms/t/two_and_twenty.asp

*(3) Audition de M. Fabrice Coquio, président-directeur général de Digital Realty, le 12 mai 2026*

Selon les modalités de fourniture des services d'IA, la part de valeur localisée en France peut évoluer fortement :

– dans le cas d'un service d'IA fourni par un *hyperscaler* à partir d'un data center localisé à l'étranger, la part de valeur localisée en France est nulle ;

– la localisation en France du data center utilisé pour l'inférence (réponse aux requêtes post-entrainement) permet *a minima* de relocaliser l'activité d'achat d'électricité et de construction-exploitation. Toutefois, si ce data center est utilisé par un *hyperscaler,* la grande majorité de la valeur part hors de l'Union européenne ;

– pour faire basculer la majeure partie de la valeur dans l'Union européenne, les services doivent être fournis par un fournisseur d'IA localisé en Europe, utilisant ses propres modèles ou des modèles ouverts, et financé au moins en partie par des fonds européens.

Concernant les recettes fiscales, les taxes locales et les taxes de fonctionnement (éventuelles taxes spécifiques sur l'activité) peuvent être appliquées sur le territoire. S'agissant de l'impôt sur les sociétés, la part revenant dans le pays de fourniture du service dépend des modèles de répartition du bénéfice taxable retenus par le fournisseur.

#### 3. Raisons juridiques

La territorialisation des capacités de calcul peut être envisagée pour des raisons de souveraineté politique. L'intelligence artificielle induit nécessairement un accès aux données de l'utilisateur : les données nécessaires pour le réglage fin du modèle, mais aussi les données d'entrée et sortie. Comme il a été montré dans le chapitre 4, la localisation sur le territoire n'est pas une condition suffisante pour assurer la maîtrise des données, du fait de l'application extraterritoriale du droit. Toutefois, c'est une condition nécessaire à un contrôle des administrations, des entreprises et des citoyens sur leurs propres données.

La pénétration croissante de cette technologie dans les process économiques pourrait faire de l'IA une infrastructure vitale pour le fonctionnement d'un pays, et la localisation territoriale des data centers la seule façon d'assurer une forme de contrôle sur cette infrastructure.

### B. ÉTAT DU DÉPLOIEMENT : DES PROJETS QUI BÉNÉFICIERONT EN GRANDE MAJORITÉ AUX HYPERSCALERS

La rapporteure souhaitait réaliser un état des lieux du déploiement des data centers en France pour comprendre les prises de position des acteurs et déterminer dans quelle mesure le développement des projets sur notre territoire contribuait à renforcer notre souveraineté ou, au contraire, renforçait nos dépendances. Pour cela, 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 [1]. Les puissances de raccordement sont présentées de façon agrégée, afin de ne pas divulguer d'informations commercialement sensibles.

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

#### *a. Data centers en service*

La France héberge actuellement 352 data centers, dont 70 % se situent en région Île-de-France [2]. La très grande majorité de ces installations sont raccordées au réseau électrique de distribution, opéré par Enedis. Les data centers connectés directement au réseau de transport, opéré par RTE, sont ceux dont la puissance de raccordement est supérieure à 40 mégawatts (MW). C'est le cas de huit d'entre eux, qui mobilisent une puissance de raccordement de 612 MW. Les opérateurs les plus importants sont Cloud HQ (site des Lisses), Data 4 (site de Marcoussis), Digital Realty (sites des Ulis et de Marseille), Equinix (site d'Argenteuil), et OVH (site de Roubaix).

Le délai moyen pour leur raccordement a été de quatre à cinq ans. Les procédures administratives ont été menées en parallèle de celles des data centers, pendant deux à trois ans. Ensuite, la durée moyenne des travaux réalisés par RTE a été de l'ordre de dix-huit mois à deux ans.

#### *b. Data centers en construction ou en état avancé*

Pour définir les projets entrant dans cette catégorie, le critère retenu est de la signature d'une convention de raccordement au réseau de transport public d'électricité. Lorsqu'un opérateur signe sa convention de raccordement, on peut affirmer que la demande est suffisamment mature : le porteur de projet dispose généralement des autorisations, comme RTE ; les recours contentieux ont été purgés et il a versé à RTE une avance correspondant à environ 30 % du coût du raccordement attestant de sa volonté d'investir.

Les projets entrant dans cette catégorie représentent une puissance de 1 200 MW : deux projets sont portés par des sociétés qui sont spécialisées dans l'immobilier ou la logistique, cinq par des *pure players* des data centers dont trois extra-européens et deux français.

#### *c. Data centers en projet*

Les données de RTE font apparaître une forte croissance de l'évolution des demandes de raccordement, dans des proportions bien supérieures aux besoins réels et aux capacités d'absorption du réseau électrique.

---

*(1) Le choix a été fait de se concentrer sur le réseau de transport d'électricité, sur lequel sont effectués les raccordements des projets de grande taille (puissance de raccordement supérieure à 40 MW), susceptibles de concerner l'intelligence artificielle.*

*(2) ADEME,* Prospective d'évolution des consommations des data centers à court, moyen et long terme de 2024 à 2060, *janvier 2026*

Afin d'avoir un élément de comparaison, la puissance des réacteurs nucléaires installés en France est comprise entre 900 et 1 450 MW, et celle de l'EPR de Flamanville est de 1 600 MW. La puissance installée totale du parc nucléaire en France s'élève à 61,4 GW (1).

Le tableau ci-dessous représente l'évolution des capacités de connexion au réseau réservées par des développeurs de projet (incluant les projets pour lesquels une convention de réservation a été signée). La réservation de capacité se traduit juridiquement par la signature d'une proposition technique et financière (PTF). Lorsqu'il signe une PTF, le demandeur commence à engager des frais d'études, ce qui signifie que son projet est sérieux. Toutefois, ce dernier peut ne pas parvenir à son terme si les débouchés commerciaux ne sont pas suffisants ou si le projet rencontre des difficultés.

Le stock total de capacités réservées s'élève désormais à près de 15 gigawatts (15 000 MW), dont 7,7 GW contractualisés en 2025 et 3,1 GW en 2026. L**a puissance actuellement réservée pour les projets de data centers représente donc 24 % de la puissance nucléaire française.**

La croissance est très forte depuis trois ans, et rien ne témoigne aujourd'hui d'un ralentissement : sur les quatre premiers mois de l'année, RTE a reçu un volume très important de demandes d'études exploratoires et de nouvelles demandes de raccordement.

**ÉVOLUTION DE LA CAPACITÉ RÉSERVÉE ANNUELLEMENT SUR LE RÉSEAU DE TRANSPORT PAR LES DATA CENTERS**

| Année | Capacité réservée |
|---|---|
| 2021 | 275 |
| 2022 | 965 |
| 2023 | 1 445 |
| 2024 | 1 455 |
| 2025 | 7 715 |
| 2026 | 3 067 |
| Total | 14 922 |

*Source : RTE.*

(1) https://www.edf.fr/groupe-edf/comprendre/production/nucleaire/nucleaire-en-chiffres

Sans surprise, l'Île-de-France est la région la plus concernée avec 7 GW de puissance demandée, soit la moitié du total, suivie des Hauts-de-France (2,9 GW), puis de l'Est (1,3 GW).

| Département | Capacité réservée (en MW) |
|---|---|
| Seine-et-Marne | 1 845 |
| Essonne | 1 475 |
| Nord | 1 340 |
| Indre | 1 310 |
| Seine-Saint-Denis | 1 170 |
| Moselle | 1 049 |
| Pas-de-Calais | 830 |
| Yvelines | 820 |
| Bouches-du-Rhône | 790 |
| Val-d'Oise | 780 |
| Oise | 750 |
| Val-de-Marne | 550 |
| Gironde | 500 |
| Rhône | 430 |
| Hauts-de-Seine | 369 |
| Autres départements | 914 |
| Total | **14 922** |

*Source : RTE.*

### 2. Les data centers développés en France seront-ils utilisés par des opérateurs européens ?

Les porteurs de projet peuvent être classés en cinq catégories distinctes :

– les développeurs et exploitants de data centers ;

– les énergéticiens français, qui préparent des projets clé en main pour de futurs repreneurs ;

– les hyperscalers : AWS, Microsoft et Google ;

– les promoteurs immobiliers et logistiques ;

– les investisseurs internationaux (fonds d'investissement internationaux et sociétés familiales).

Le tableau suivant indique les capacités réservées et nationalités des développeurs de projets pour chacune de ces catégories – la nationalité du développeur n'étant pas nécessairement une indication sur la nationalité de l'utilisateur final.

**CAPACITÉ RÉSERVÉE ANNUELLEMENT SUR LE RÉSEAU DE TRANSPORT PAR CATÉGORIE DE DÉVELOPPEUR DE PROJETS**

| Catégorie | Capacité réservée (MW) |
|---|---|
| **Développeurs et exploitants de data centers** | **3 868** |
| États-Unis | 1 340 |
| France | 1 259 |
| Extra-UE hors États-Unis | 1144 |
| UE hors France | 125 |
| **Énergéticiens** | **1 899** |
| France | 1 899 |
| **Hyperscalers** | **1 980** |
| États-Unis | 1 980 |
| **Promoteurs immobiliers et logistiques** | **6 420** |
| France | 3 300 |
| Extra-UE hors États-Unis | 1 930 |
| États-Unis | 880 |
| UE hors France | 310 |
| **Investisseurs internationaux** | **755** |
| Extra-UE hors États-Unis | 580 |
| France | 125 |
| UE hors France | 50 |
| **Total général** | **14 922** |

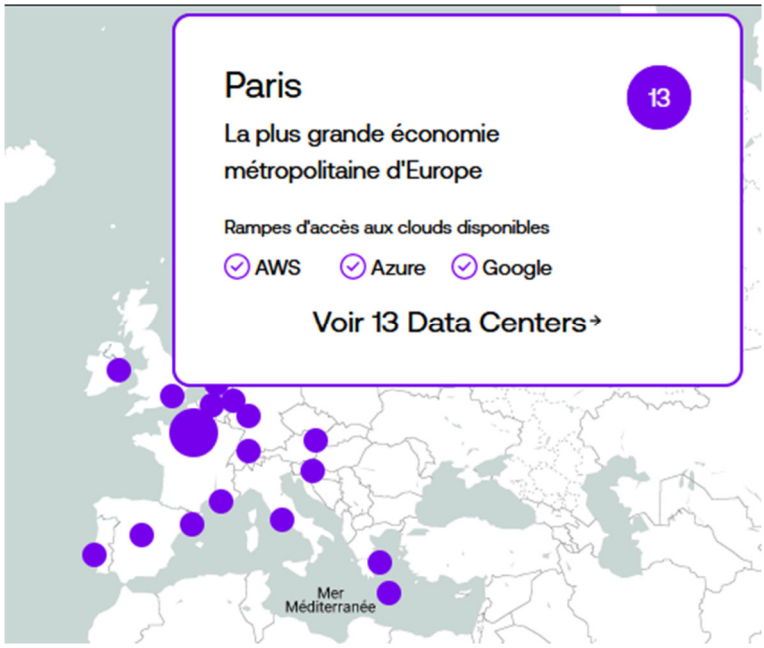
*Source : RTE.*

Au total, les acteurs du secteur (*hyperscalers* et développeurs et exploitants de data centers) représentent 39 % de la puissance contractualisée totale, avec 5,8 GW. Au sein de ces deux catégories, les acteurs états-uniens et français représentent respectivement 3,3 GW (22 %) et 1,3 GW (9 %).

Concernant les développeurs et exploitant des data centers, comme Digital Realty ou Data One, la nationalité de l'entreprise ne dit rien de l'utilisateur final de la capacité de calcul, comme cela a été démontré dans les auditions. Comme l'indiquait M. Coquio, à Marseille les infrastructures de Digital Realty à Marseille sont utilisées entre 60 % à 70 % par des clients extra-européens. Le site internet de Digital Realty illustre bien à quel point les hyperscalers sont structurants dans le portefeuille de l'opérateur [(1)]. La société réalise ainsi 60 % de son chiffre d'affaires en France avec des acteurs non-européens [(2)], dont 45 % avec des hyperscalers – elle classe toutefois en acteurs européens les sociétés Bleu et Tricolore.

*(1) https://www.digitalrealty.com/fr/data-centers/emea*

*(2) Réponses aux questionnaires de la rapporteure.*




*Source : Site internet Digital realty.*

En ce qui concerne DataOne, l'audition de cet acteur par la commission d'enquête a révélé un modèle qui présente peu d'intérêt en matière de souveraineté. Data One construit et entretient les bâtiments, gère les raccordements aux utilités et réseaux et assure l'aspect physique de l'accès aux données. En revanche, les racks informatiques et les GPU, c'est-à-dire la puissance de calcul, relèvent de ses clients. Dans son projet le plus avancé à Eybens, ce client est Core42, fonds d'investissement émirati. Data One agit donc comme un opérateur immobilier, spécialisé dans les data centers. Il n'a aucun contrôle sur les acteurs qui utiliseront la puissance de calcul et l'énergie qui sert à les faire fonctionner ([1]) : « *Je peux suggérer à notre client de privilégier ce type d'acteurs plutôt que d'imposer, une fois de plus, les Gafam. Mais le client reste maître de ses choix, puisque ce sont ses GPU et son matériel qu'il installe* ».

Plus de 9 GW sont portés par des acteurs non spécialisés, dans une logique d'investissement : développeurs immobiliers (prolongation de leur activité courante), énergéticiens (valorisation de leur foncier inutilisé et perspectives de vente couplée d'électricité) et investisseurs internationaux (recherche de placements financiers dans les infrastructures). Là encore, la nationalité du développeur ne détermine pas la nationalité de l'utilisateur final, son futur client. L'allocation des capacités d'accueil du data center ira à la meilleure offre. C'est pourquoi les *hyperscalers* sont en position de force pour capter l'essentiel des capacités. Grâce à

*(1) Audition conjointe, ouverte à la presse, de MM. Laurent Choukroun, président-directeur général d'Oreus et Julien Lescoulié, directeur technique, et M. Charles-Antoine Beyney, directeur général de DataOne, le 29 avril 2026.*

des bilans financiers solides, ils sont capables de signer des contrats de réservation de capacité de plusieurs dizaines de milliards d'euros.

Enfin, la rapporteure a étudié le modèle du Campus IA, un projet particulièrement soutenu par le gouvernement et qui s'inscrit dans le cadre du partenariat entre les Émirats arabes unis (EAU) et la France. La société Campus IA, dont l'entité contrôlante est MGX (fonds émirati) et dont BPIFrance, Nvidia et Mistral sont actionnaires minoritaires, a pour rôle d'assurer le développement du projet (identification de terrain, gestion des raccordements et des permis de construire). Les terrains seront ensuite vendus à des développeurs de data centers, dont l'identité n'est à ce jour pas connu. Cependant l'opérateur pressenti pour réaliser la première tranche du projet, est un opérateur émirati, Khazna.

Ce sont ensuite les développeurs et exploitants de data centers qui seront probablement propriétaires de la puissance de calcul, et choisiront leurs clients. L'identité du client final n'est pas connue actuellement.

À ce stade, à l'exception de la part réservée à Mistral AI et un partenariat avec l'École polytechnique, aucun élément contraignant ne permet d'assurer que ces infrastructures serviront à des opérateurs européens, et ce malgré le mandat donné à BPIFrance.

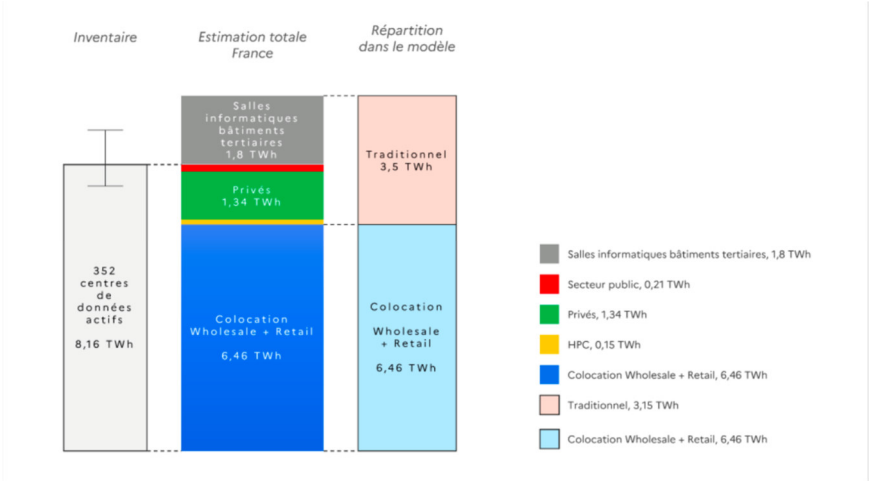
Suite à la lecture des réponses de BPIFrance au questionnaire qui leur avait été adressé, la rapporteure émet de sérieux doute sur le fait que le projet Campus IA permettra de renforcer la souveraineté de notre pays. En effet, dans les raisons données par BPIFrance pur justifier la joint-venture avec MGX, il est mentionné *« d'excellents accès aux hyperscalers (Google, Amazon, Microsoft, Meta) via son réseau et la plateforme AIP ».* La rapporteure précise également que MGX est actionnaire d'openIA, xAI et TikTok US.

### C. LA TRAJECTOIRE DE DÉVELOPPEMENT DES DATA CENTERS EST-ELLE SOUTENABLE POUR LE RÉSEAU ÉLECTRIQUE FRANÇAIS ?

La tendance actuelle des entreprises en France consiste à basculer leurs usages numériques de data centers propriétaires, hébergés dans leurs locaux, vers des infrastructures de cloud.

Le travail de l'Agence de la transition écologique (Ademe) a permis d'identifier en 2024, 352 data centers actifs pour un total de 8,16 térawattheures (TWh) d'électricité consommée [(1)].

*(1) ADEME,* ibid.




*Source : ADEME*

La consommation des data centers sur sites dédiés augmente régulièrement depuis 2019. Elle est de l'ordre de 4 TWh (1TWh en 2025 sur le réseau de transport d'électricité opéré par Réseau de transport d'électricité (RTE), 3 TWh sur le réseau Enedis), soit moins de 1 % de la consommation électrique française. En outre, une large partie des usages numériques français est aujourd'hui alimentée par data centers situés à l'étranger.

La forte croissance des projets aura des impacts structurels sur le système électrique français. Deux dimensions doivent être prises en compte : les volumes d'électricité disponibles (incluant les capacités de production nationales et les volumes échangés au sein du marché de l'électricité) et les capacités de connexion du réseau pour des projets de grande capacité.

### 1. Des volumes d'électricité disponibles suffisants

Selon RTE, le rythme de croissance de la production électrique bas-carbone en France ne pose pas de problème stratégique et peut alimenter simultanément, sans conflit d'usage, la décarbonation des secteurs des transports, de l'industrie et du bâtiment de manière prioritaire, ainsi que le développement du secteur du numérique. Les scénarios prospectifs de RTE sont fondés sur deux hypothèses : d'une part, tous les projets de data centers ayant réservé de la capacité ne se concrétiseront vraisemblablement pas, d'autre part, leur montée en charge s'étalera sur plusieurs années, de l'ordre de la décennie.

Les deux trajectoires étudiées par RTE au sein du bilan prévisionnel 2025 sont fondées sur l'hypothèse que le taux d'utilisation de la puissance à 2030 sera de l'ordre de 20 % de la capacité installée, en raison d'une montée en charge progressive :

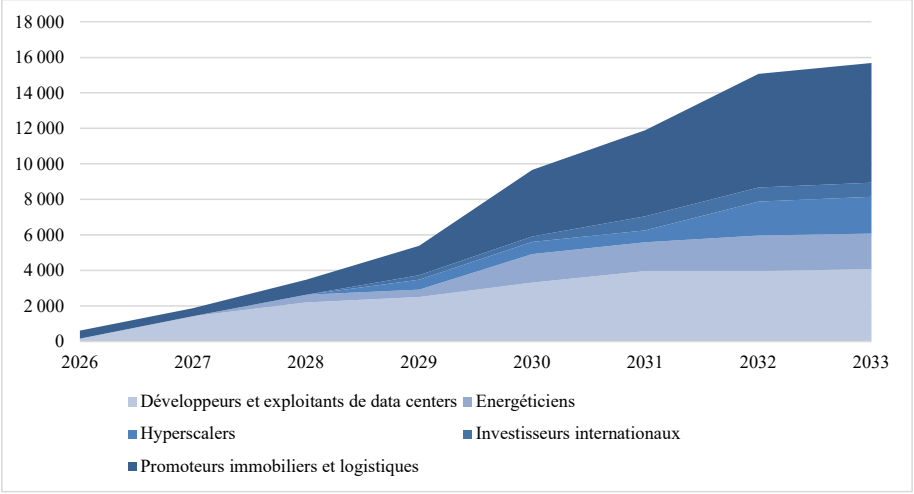
– la trajectoire de décarbonation rapide table sur une augmentation de la consommation de 10 TWh à l'horizon 2030, correspondant à un taux de

concrétisation d'environ 60 % (4,3 GW) pour les projets ayant sécurisé un raccordement au réseau de transport d'électricité avant 2030. Elle suppose en outre un développement des data centers raccordés au réseau de distribution dans la continuité de la tendance actuelle ;

– la trajectoire de décarbonation lente correspond quant à elle à une augmentation de 6 TWh à l'horizon 2030, et à un taux de concrétisation d'environ 30 % pour les projets ayant demandé un raccordement au réseau de transport.

Selon les mêmes hypothèses d'un taux d'utilisation moyen de 20 % et d'un taux de concrétisation de 60 %, les données les plus à jour issues des registres de demandes de raccordement font apparaître une consommation potentielle de 9,6 TWh en 2030 et 15,7 TWh en 2033.

**ÉVOLUTION DE LA CONSOMMATION PRÉVISIONNELLE PAR CATÉGORIE DE DÉVELOPPEURS DE PROJET (GWh)**




*Source : RTE.*

**Le niveau de demande des centres de données sur sites dédiés atteindrait finalement près de 32 TWh en 2035 dans la trajectoire de décarbonation rapide contre 21 TWh dans la trajectoire de décarbonation lente**. À titre de comparaison, l'électricité totale consommée en région Normandie était de 26,5 TWh en 2024.

Au regard des capacités de production électrique nationales, le risque de cannibalisation avec d'autres usages serait faible. La France exporte actuellement à des niveaux élevés (entre 80 et 100 TWh par an), et ces volumes exportés constituent autant de volumes disponibles pour permettre l'accueil de nouveaux usages sur le territoire national.

Dans les scénarios de plus long terme, les trajectoires de consommation du secteur des data centers pourraient atteindre autour de 50 TWh à l'horizon 2050 en

fonction de la concrétisation des projets. Elles sont soumises à des incertitudes importantes quant au futur de la technologie de l'IA générative et à la soutenabilité économique et environnementale des trajectoires de développement de chaque pays.

### 2. Des problèmes locaux liés à des congestions du réseau, entraînant des conflits avec d'autres usages de décarbonation

Selon RTE, la situation est *« plutôt bien maîtrisée »* concernant la demande de puissance installée. Les opérateurs de data centers ont tendance à éviter les zones industrielles – autre source importante de demande potentielle – et à privilégier les grandes zones urbaines. Les grands gestionnaires de foncier industriel comme les autorités portuaires veillent à assurer une allocation équilibrée du foncier et des capacités électriques. De plus, les grands sites « fast-track » (cf. *infra*) ont été définis également dans un souci d'éviter les conflits d'usage du réseau.

Cependant, dans certaines zones, les demandes de l'industrie et du numérique sont concurrentes. De telles tensions temporaires existent actuellement en Île-de-France, en Lorraine, dans la zone de Valenciennes-Maubeuge ou, dans une moindre mesure, en Auvergne-Rhône-Alpes et en Normandie. M. Fabrice Coquio cite également le cas de la zone industrielle de Fos-sur-Mer : « *Les besoins ne peuvent pas toujours être satisfaits par l'électricité immédiatement disponible sur le réseau, que ce soit en haute tension – pour RTE – ou en moyenne tension – pour Enedis –, ce qui peut causer des encombrements et poser des problèmes d'attribution (…). Cela renvoie à des enjeux de réindustrialisation et de décarbonation de certaines activités – je pense par exemple à la zone industrielle de Fos-sur-Mer –, mais aussi de mobilité, de transport et d'électrification des usages.* »

En vertu de la règle du « premier arrivé, premier servi », ce sont les projets ayant réalisé leur demande de raccordement le plus tôt qui bénéficient des capacités de raccordement existantes et évitent ainsi de devoir dépendre de la construction de nouveaux ouvrages. Outre des conséquences positives en termes de calendrier de mise à disposition de la connexion, les coûts de raccordement sont moindres, ainsi que les risques de non-réalisation des ouvrages.

L'article 29 de la loi du 10 mars 2023 relative à l'accélération de la production d'énergies renouvelables a créé un dispositif permettant à l'État de donner la priorité à des projets dérogeant ainsi à l'ordre de la file d'attente établi par RTE. Lorsque, dans une zone géographique donnée, l'ensemble des demandes de raccordement au réseau engendrent, pour au moins un des projets demandeurs, un délai de raccordement supérieur à cinq ans, RTE saisit le préfet de la région concernée, qui établit un nouvel ordre de priorité. Toutefois, ce dispositif est inopérant pour des data centers : s'il permet de hiérarchiser entre eux des projets industriels, il ne permet pas de modifier l'ordre entre des projets industriels et des projets de data center. En tout état de cause, ce dispositif s'éteindra au printemps 2027, conformément à la volonté du législateur.

En accord avec la Commission de régulation de l'énergie, RTE a organisé au premier trimestre 2026 une consultation publique proposant de faire évoluer la

logique actuelle de « premier arrivé, premier servi » vers une logique du « premier prêt, premier servi ». Des modalités concrètes de déclinaison de ce principe doivent maintenant être élaborées en concertation avec les acteurs. Or ce principe contribuera encore à renforcer la place des *hyperscalers*, dans la mesure où leur avantage concurrentiel les place dans de meilleures positions. Ainsi dans son étude sur les enjeux concurrentiels liés à l'impact énergétique et environnemental de l'IA [1], *« l'Autorité de la concurrence a analysé plusieurs comportements susceptibles de soulever des préoccupations au regard des règles de concurrence. Au-delà des risques de barrières à l'entrée ou à l'expansion pour des acteurs de taille modeste, l'Autorité sera particulièrement vigilante à ce que la position privilégiée des acteurs les plus importants du secteur ne leur permettent de sécuriser des approvisionnements d'énergie dans des conditions avantageuses* ».

### 3. Le mix bas carbone français : un mauvais argument pour justifier l'accueil des data centers sur notre territoire

#### *a. Ne pas servir d'excuse au développement inconsidéré de l'intelligence artificielle*

Avec l'intensification des usages et l'utilisation de data centers états-uniens et chinois alimentés par un mix énergétique fortement dépendant d'énergies fossiles, l'utilisation des outils numériques prend une part croissante dans l'empreinte carbone du numérique. Dans le cycle de vie, la fabrication, la distribution et la fin de vie continuent cependant de représenter la part la plus émettrice de $CO_2$.

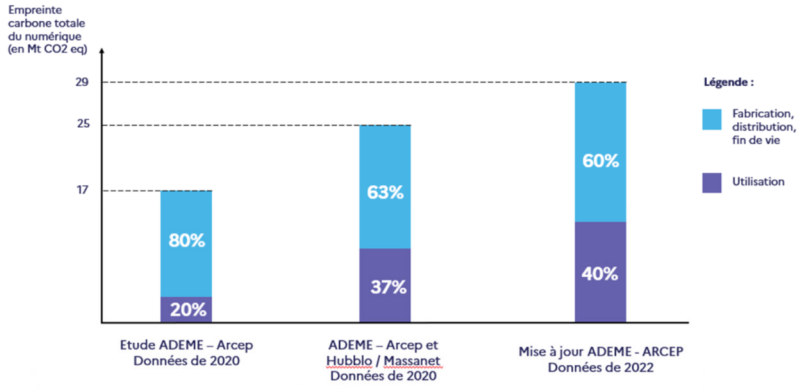



*Figure 5 – Comparaison des résultats avec les études précédentes – par phase du cycle de vie*

*Source : étude ARCEP-ADEME de 2025 sur l'empreinte carbone du numérique.*

L'impact environnemental principal des data centers, durant leur phase d'exploitation, est lié à leur consommation électrique massive. À ce titre, l'intensité carbone du mix électrique de leur pays d'implantation constitue l'indicateur principal à prendre en compte. La France se situe à la seconde place des pays

*(1) Autorité de la concurrence,* ibid.

d'Europe, derrière la Norvège, avec une intensité carbone de 22 grammes de $CO_2$ par kilowattheures, la moyenne des pays de l'Union européenne étant de 179.

Il est à noter cependant que dans son rapport sur la prospective d'évolution des consommations des centres de données en France de 2024 à 2060, l'Ademe note qu'« *une forte expansion tendancielle des consommations des centres de données entraînerait un accroissement important des émissions du secteur, incompatible avec l'Accord de Paris.* »

M. Lex Coors, président de l'association européenne des data centers, appelle d'ailleurs l'Europe à renoncer à ses objectifs climatiques et à « *ouvrir la conversation* » sur le recours à des énergies fossiles pour alimenter les data centers [(1)].

Les développeurs de projet recourent de façon croissante à des contrats d'achat d'électricité (*Power purchase agreements*, PPAs) directement auprès de producteurs d'énergie renouvelable, de façon à récupérer des « garanties d'origine ». L'utilisation de tels PPAs est une façon de justifier un bilan environnemental inattaquable, comme a pu le faire M. Coquio devant la commission d'enquête : *« Au sein du groupe Digital Realty, la France est pionnière en matière environnementale. Depuis 2014, nous nous y fournissons uniquement en énergie renouvelable – c'est également le cas de l'ensemble de nos data centers en Europe depuis 2021 ».* Pourtant, les garanties d'origine associées aux PPAs ne comptabilisent la production renouvelable qu'à la maille mensuelle, et non à la maille horaire, si bien que des consommateurs peuvent consommer de l'électricité carbonée venant du réseau durant certaines heures tout en étant couverts par des garanties d'origine. L'étude de l'impact environnemental des data centers devra donc s'appuyer sur des analyses fondées sur des méthodes validées, et tenant compte de l'intégralité des émissions, y compris celles pour l'entraînement des modèles.

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

Ce type d'obligation est d'ores et déjà en vigueur pour les installations de production d'hydrogène. Comme l'indique la Commission européenne à propos des actes délégués de l'Union européenne relatifs à l'hydrogène renouvelable [(2)], *« à moins que le système électrique ne soit déjà largement décarboné, il est essentiel de faire correspondre la demande d'électricité pour la production d'hydrogène à une production supplémentaire d'électricité d'origine renouvelable. Si la production d'hydrogène n'était pas accompagnée d'une production supplémentaire à partir de sources renouvelables, il se pourrait que la demande supplémentaire d'électricité des électrolyseurs risque d'entraîner une augmentation de la production d'électricité à partir de combustibles fossiles (…) À partir de janvier 2030, tous les producteurs d'hydrogène renouvelable, y compris ceux qui ont signé avec des centrales de production d'électricité renouvelable existantes, devront avoir une production correspondant à l'électricité qu'ils ont achetée, sur une base horaire. ».* Une telle obligation permettrait de faire du déploiement des data centers un atout dans la décarbonation européenne plutôt qu'une menace.

*(1) Mathilde Saliou, « Objectifs climatiques ou IA ? Pour le lobby des data centers, l'Europe doit choisir », Next, 22 juin 2026*

*(2) https://ec.europa.eu/commission/presscorner/detail/fr/qanda_23_595*

### *b. La permanence d'autres sujets environnementaux majeurs*

L'implantation des data centers en Europe s'accompagne d'obligations minimales en matière de publication des données environnementales, et bientôt de performances, s'agissant :

– de la récupération de chaleur fatale : depuis 2024, les centres de données d'une puissance de plus de 500 kW doivent remonter chaque année des indicateurs environnementaux auprès de la Commission européenne ;

– de la consommation d'eau : depuis 2022, l'Arcep collecte et publie annuellement les données relatives à la consommation en eau des centres de données dans son enquête « Pour un numérique soutenable ». Depuis 2025, ces obligations sont harmonisées avec le cadre européen issu de la directive2023/1791 sur l'efficacité énergétique, dans un souci de simplification administrative.

Toutefois, de tels projets sont loin d'être neutres pour l'environnement, comme le montre l'avis de mission régionale d'autorité environnementale (MRAE) d'Île-de-France sur le projet Campus IA, qui est un cas d'école pour les risques environnementaux nés d'un projet de data center atteignant le gigawatt de puissance installée [(1)] :

– la consommation de foncier, avec en particulier la destruction de terres agricoles dont les sols « *permettent d'obtenir de très bons rendements, des conditions pédoclimatiques très favorables à l'ensemble des cultures* ». Comme l'indiquait M. Arnaud Saint-Martin, député de la Seine-et-Marne, lors de l'audition de M. Arthur Mensch, « *ce projet est colossal (…) parce qu'il transformera ce territoire de Seine-et-Marne de façon importante. Il a déjà fait disparaître les champs de betteraves et de blé qu'on y trouvait auparavant – l'archéologie préventive effectue actuellement des fouilles* ».

– **la pollution atmosphérique liée au fonctionnement des générateurs de secours** ; il est prévu l'installation de 613 groupes électrogènes, ce qui représente 4,6 MWth de puissance installée, soit davantage que le parc thermique d'EDF sur l'ensemble de la France métropolitaine [(2)]. Dans un document de 2023, la MRAE réalise une synthèse des enjeux identifiés lors de ses différents avis sur des projets de data centers. S'agissant des groupes électrogènes, elle met en valeur les risques de pollution environnementale en cas d'incident sur un cluster de data centers, entraînant des effets cumulés : « *en cas de défaillance du réseau électrique, l'ensemble des groupes peut fonctionner simultanément en plein puissance. Leur impact apparaît comme déjà sensible compte tenu de ces tests réguliers, mais la question d'une panne systémique de plusieurs heures, voire de plusieurs jours, doit être examinée, notamment pour des centres de données implantés en milieu urbain ou dans un essaim (les sites des Ulis et de Marcoussis en Essonne sont susceptibles*

---

*1) Mission régionale d'autorité environnementale Île-de-France, Avis délibéré sur le projet de construction d'un campus de centres de données à Fouju (77), avril 2026*

*(2) 4 000 MW installés, composés de 4 cycles combinés au gaz et 13 turbines à combustion.*

*de concentrer dans un rayon de 5 km 16 centres de données de grande capacité) (...)* » [(1)]. La MRAE rappelle également que le data center des Ulis a fonctionné sur groupes électrogènes pendant 270 heures en novembre 2020.

– **l'utilisation de plus de 500 tonnes de fluide frigorigène de la catégorie des PFAS** pour le fonctionnement des 680 groupes froids crée de potentiels risques sanitaires liés aux fuites du fluide R-1234ze utilisé : « *Ces microfuites sont estimées à 3 % par an des 514,3 t présentes sur site, soit 15 t émises annuellement à l'atmosphère. S'agissant d'un PFAS, par ailleurs précurseur du TFA, ces rejets sont loin d'être négligeables et leurs effets doivent être précisés, avec une évaluation du risque sanitaire de ces pertes.* »

– **la création d'îlots de chaleur urbaine** ; dans un article sur linkedin à propos du projet [(2)], Mme Valérie Masson Delmotte indique ainsi qu'une première étude réalisée à partir de données satellitaires souligne un effet d'îlot de chaleur des data centers atteignant en moyenne + 2° C, avec un effet discernable sur un rayon de 10 kilomètres [(3)].

La commission n'a pas pu étudier, en raison du temps imparti, les impacts environnementaux du numérique et plus spécifiquement des data centers. Cependant l'exemple du projet Campus AI démontre la nécessité d'approfondir les recherches sur ce sujet et de suivre étroitement les émissions de polluants par les data centers. Les impacts environnementaux seront d'autant plus importants sur les territoires concernés par l'implantation de clusters, du fait du cumul potentiel des effets des installations. Ces éléments plaident pour un examen très resserré des demandes d'autorisation environnementale par les services instructeurs de l'État et la mise en place de contrôles par les directions régionales de l'environnement, de l'aménagement et du logement (Dreal).

### D. LES DATA CENTERS AU CŒUR DES ACTIONS DU GOUVERNEMENT : IA SUMMIT, FAST TRACK ET TASK FORCE

Pour soutenir le déploiement des data centers en France, l'État s'est mobilisé à travers trois grandes initiatives.

**La première est le soutien public marqué de la présidence de la République dans le cadre des sommets annuels que sont le Sommet de l'intelligence artificielle (*IA summit*) et *Choose France*.** En février 2025, à l'occasion du Sommet de l'intelligence artificielle, M. Emmanuel Macron annonçait 109 milliards d'euros d'investissements privés, dont 95 directement

---

*(1) Mission régionale d'autorité environnementale Île-de-France,* Les data centers (centres de stockage de données), *Éclairages 2023,*

*(2)*https://www.linkedin.com/pulse/les-enjeux-environnementaux-des-data-centers-val%C3%A9rie-masson-delmotte-zlxfe/

*(3)Andrea Marinoni, Erik Cambria, Weisi Lin, Mauro Dalla Mura, Jocelyn Chanussot, Edoardo Ragusa, Chi Yan Tso, Yihao Zhu, Benjamin Horton,* The data heat island effect: quantifying the impact of AI data centers in a warming world*, avril 202*

fléchés vers la construction de data centers. Ces investissements se répartissent de la façon suivante :

| Acteur | Pays d'origine | Montant de l'investissement annoncé (en Md €) |
|---|---|---|
| MGX | Émirats arabes unis | 50 |
| Data 4 / Brookfield | France et Canada | 15 |
| Fluidstack (projet abandonné en mars 2026) | Royaume-Uni | 10 |
| Amazon Web Services | États-Unis | 6 |
| Evroc | Suède | 4 |
| Prologis | États-Unis | 3,5 |
| Iliad | France | 2,5 |
| Digital Realty | États-Unis | 2,3 |
| Equinix | États-Unis | 0,6 |
| Sesterce | France | 0,4 |
| Telehouse | Japon | 0,4 |

*Source : réponse aux questionnaires de la rapporteure.*

Ainsi, les Émirats arabes unis comptent pour 50 milliards d'euros, le Canada pour 15 milliards, les États-Unis pour 12,4 milliards, le Royaume-Uni pour 10 milliards, la France (hors Data4) pour 2,9, la Suède pour 4 et le Japon pour 0,4.

Créé en 2024, MGX est capitalistiquement lié à Mubadala, fonds souverain émirati, et partenaire important de BPIFrance. Outre ces éléments, MGX a signé un accord avec Microsoft pour l'investissement de 100 milliards de dollars dans des infrastructures d'IA [(1)], a participé aux levées de fonds d'OpenAi [(2)] et d'Anthropic [(3)]. L'investissement de MGX s'inscrit dans le cadre du projet Campus AI, dans lequel sont aussi investisseurs BPIFrance et Mistral AI. Campus IA fait suite à un partenariat d'État entre la France et les Émirats arabes unis, formalisé en mai 2024 et matérialisé par un accord signé le 6 février 2025, qui vise à développer une capacité de 700 MW d'infrastructures IA sur le site de Fouju. À l'occasion de Choose France, en juin 2026, une extension du projet Campus IA à 3 GW a été annoncée.

Lors du même sommet de juin 2026, d'autres projets ont fait l'objet d'annonces additionnelles [(4)] :

– Brookfield (Canada) porte à 30 milliards d'euros ses investissements dans les infrastructures d'IA dans les Hauts-de-France, avec le développement de nouveaux data centers et d'un écosystème industriel associé ;

---

*(1) Communiqué de l'entreprise Microsoft, septembre 2024, https://news.microsoft.com/source/2024/09/17/blackrock-global-infrastructure-partners-microsoft-and-mgx-launch-new-ai-partnership-to-invest-in-data-centers-and-supporting-power-infrastructure/*

*(2) Communiqué de l'entreprise OpenAI, mars 2026, https://openai.com/fr-FR/index/accelerating-the-next-phase-ai/*

*(3) Communiqué de l'entreprise Anthropic, mai 2026, https://www.anthropic.com/news/series-h*

*(4) Communiqué de la Direction générale des entreprises, juin 2026, https://www.entreprises.gouv.fr/la-dge/actualites/choose-france-2026-un-nouveau-record-dinvestissements-en-faveur-de-lindustrie-de*

– Nebius (Pays-Bas) reconvertit l'ancienne friche Bridgestone de Béthune en site majeur de calcul et de cloud pour l'IA en Europe. En mars 2026, Nebius signait un accord avec Meta dans lequel cette dernière s'engage à contractualiser des capacités de calcul réparties sur plusieurs sites pour un montant cumulé de 27 milliards de dollars (1) ;

– Phoenix Group (Émirats arabes unis) développe des infrastructures numériques et des data centers de nouvelle génération, notamment dans la région lyonnaise ;

– SoftBank Group Corp. (Japon) annonce un vaste programme de centres de données dédiés à l'IA pouvant atteindre 75 milliards d'euros d'investissements. Le projet vise le déploiement en France d'infrastructures pouvant atteindre jusqu'à 5 GW de puissance électrique, correspondant à un investissement de 75 milliards d'euros, dont 3,1 GW dans les Hauts-de-France d'ici 2031 pour un investissement de 45 milliards ;

– Verne et Ardian (Royaume-Uni / France) développeront en Île-de-France un campus numérique bas carbone destiné aux capacités de calcul haute performance.

Le déploiement des actions annoncé au Sommet de l'IA est d'ailleurs suivi depuis l'Élysée, comme l'indiquait M. Laurent Choukroun lors de son audition « *Matthieu Landon, secrétaire adjoint du cabinet du président de la République, nous a reçus dans le cadre de nos échanges avec la DGE, afin de prendre la mesure de ce que nous étions en train de déployer, notamment sous l'aspect de nos relations avec notre partenaire émirati.* » (2)

**Le second dispositif de soutien au déploiement des data centers passe par la mise en place d'une procédure dite « fast track »,** permettant un raccordement au réseau de transport d'électricité en moins de quatre ans pour des sites d'une puissance électrique supérieure à 400 MW. À ce jour, cinq sites bénéficient de cette procédure :

– le site du Bosquel (Hauts-de-France), pour lequel le projet Softbank a été retenu ;

– le site du parc des Soufflantes à Escaudain (Hauts-de-France), où Data4 est en discussions avec la collectivité propriétaire du site ;

– le site du Grand port maritime de Dunkerque (Hauts-de-France), dont l'appel à manifestation d'intérêt (AMI) était ouvert jusqu'au 15 mai ;

– le site de Fouju (Île-de-France), attribué à MGX et dont une partie sera allouée à Mistral ;

---

*(1) Communiqué de l'entreprise Nebius, mars 2026, https://nebius.com/newsroom/nebius-signs-new-ai-infrastructure-agreement-with-meta*

*(2) Audition conjointe, ouverte à la presse, de MM. Laurent Choukroun, président-directeur général d'Oreus et Julien Lescoulié, directeur technique, et M. Charles-Antoine Beyney, directeur général de DataOne, le 29 avril 2026.*

– le site de l'ancienne centrale EDF à Montereau (Île-de-France), attribué à la filiale d'Iliad, OpCore.

**La troisième initiative est la mise en œuvre d'une *task force* data centers.** Sous le pilotage de la DGE, et comprenant en son sein Business France et RTE, celle-ci entend **faciliter et coordonner l'implantation de data centers sur le territoire français**, au travers de trois actions principales :

– aider les projets dans leur recherche foncière, avec l'identification de sites se prêtant à l'accueil de centres de données ;

– accompagner les projets dans leur réalisation : en dialogue régulier avec les porteurs de projets et les administrations compétentes, la *task force* intervient pour répondre aux éventuelles difficultés rencontrées (raccordement, autorisations) ;

– simplifier et réduire les délais d'implantation : la DGE a notamment travaillé à l'élargissement du statut de projet important d'intérêt national majeur (PINM) aux data centers, ainsi qu'à la création de la procédure « fast track ».

Au total, ce sont cinquante-sept entreprises qui sont accompagnées :

| Nationalité de l'entreprise | Nombre d'entreprises | Pourcentage des entreprises accompagnées |
|---|---|---|
| Union européenne | 25 | 44 % |
| *Dont Française* | *21* | *35 %* |
| Hors Union Européenne | 29 | 51 % |
| *Dont états-uniennes* | *14* | *25 %* |
| Indéterminée | 3 | 5 % |

*Source : Réponse aux questionnaires de la rapporteure.*

Soixante-cinq emplacements ont été identifiés par le gouvernement pour faciliter la recherche de foncier. Le tableau ci-dessous indique les régions dans lesquelles ces emplacements se situent. « *La task force datacenters, au travers de business France, propose aux porteurs de projets de présenter leurs cahiers des charges aux agences régionales de développement (ARD), pour qu'elles puissent par la suite prendre attache avec le porteur si un des sites répertoriés par l'ARD répond aux exigences du cahier des charges, et si l'ARD souhaite discuter avec le porteur* ».

| Régions | Nombre de sites identifiés |
|---|---|
| Hauts-de-France | 16 |
| Normandie | 8 |
| Grand Est | 7 |
| Bourgogne-Franche-Comté | 7 |
| Occitanie | 6 |
| Île-de-France | 6 |
| Centre-Val de Loire | 5 |
| Auvergne-Rhône Alpes | 4 |
| Nouvelle-Aquitaine | 3 |
| Bretagne | 3 |

*Source : Réponse aux questionnaires de la rapporteure*

La France bénéficie aujourd'hui d'un environnement attractif pour l'implantation de data centers, grâce à la qualité de son réseau électrique et à la présence d'emprises foncières bien connectées aux grands réseaux de télécommunications. Les atouts de la France pour l'implantation des data centers ont été mis en valeur dans une vaste opération de marketing territorial destinée aux investisseurs étrangers. S'ajoute à ces efforts une perméabilité au lobbying des grandes entreprises du numérique dans le cadre de l'examen des textes de loi. L'implantation de data centers en France sera facilitée grâce à l'article 35 de la loi de simplification de la vie économique. Suite à une campagne importante du lobby des Big Tech (1), le statut de projet national d'intérêt majeur ne sera pas réservé aux acteurs européens. Cette disposition, introduite par l'Assemblée nationale à l'initiative de Philippe Latombe, a été supprimée en commission mixte paritaire. L'objectif est donc de favoriser les investissements étrangers et non de renforcer la souveraineté européenne dans le domaine du numérique. Le soutien du gouvernement au déploiement des data centers ne répond pas à l'impératif de souveraineté, et ne poursuit aucun des objectifs de politique publique.

Les éléments recueillis par la rapporteure conduisent à formuler les trois conclusions suivantes :

– la France dispose effectivement d'une capacité de production électrique importante qui pourrait être utilisée pour fournir des services d'intelligence artificielle. Le risque est l'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 des capacités construites.** Pourtant, ainsi qu'il a été expliqué plus haut, il conviendrait de favoriser des projets visant à dédier des capacités de calcul à des opérateurs européens. Les *hyperscalers* ont eux-mêmes réservé près de 2 GW de capacité, d'autres projets visent explicitement à leur fournir des capacités additionnelles (projet Moebius) et les projets développés par des promoteurs immobiliers ou des promoteurs pourraient également être à leur bénéfice. Le fait de réguler les conditions d'implantation des data centers maximiserait la valeur réinjectée dans l'économie, réduirait fortement les risques liés à l'extra-territorialité et permettrait de servir une pluralité d'acteurs ;

– Une facilitation de l'implantation des data centers **au détriment des études relatives aux risques environnementaux et des objectifs climatiques**. Les dernières annonces, toutes portées par des investisseurs extra-européens, provenant des Émirats arabes unis (projet Campus IA), du Japon (projet Softbank) ou du Canada (Brookfield), témoignent d'un **véritable gigantisme, et font craindre des installations d'une taille démesurée.**

---

*(1) Séverin Lahaye, « Derrière la loi « simplification », l'offensive des Big Tech et du lobby des datacenters », Observatoire des multinationales, juin 2026* https://multinationales.org/fr/enquetes/profits-et-pertes-derriere-le-boom-des-datacenters-en-france/derriere-la-loi-simplification-l-offensive-des-big-tech-et-du-lobby-des

Ces éléments corroborent en tous points le constat effectué par Mme Ophélie Coelho devant la commission d'enquête : « *Sur la question de la valeur, ces centres de données en rapportent-ils ? Oui, ils créent de la valeur, mais pour qui ? Assez peu pour les pays européens qui les accueillent, car les grandes multinationales font tout pour ne pas payer d'impôts, un problème que nous n'avons pas réglé. En termes de valeur nette, nous sommes plutôt clients : nous leur donnons de l'argent tout en acceptant que leurs infrastructures puisent dans les ressources de nos territoires, que ce soit l'énergie ou l'eau. Même les gens du secteur admettent que les besoins en ressources vont augmenter, sans pouvoir dire de combien. C'est pour cela que les débats sont si vifs : nous n'avons pas les données. Nous ne savons pas comment les usages de ces infrastructures vont évoluer. Le retard est tel que Bruxelles a dû demander l'année dernière une remontée de données au niveau européen. Pourtant, les investissements sont déjà sur la table et les implantations en cours, sans aucun débat public digne de ce nom. La valeur ne va pas dans les poches de l'Europe, mais dans celles des grandes entreprises technologiques et de leurs investisseurs, qu'il s'agisse de BlackRock, Vanguard, Andreessen Horowitz, ou d'investisseurs émiratis ou chinois* ».

**Par sa politique de soutien effréné au développement des projets, le gouvernement ouvre grand la porte au verrouillage rapide du marché de l'intelligence artificielle par les plus grands acteurs américains.**

# QUATRIÈME PARTIE : POUR UN NOUVEAU MODÈLE NUMÉRIQUE EN FRANCE ET EN EUROPE

## CHAPITRE 13 – DES ALTERNATIVES ROBUSTES EXISTENT

Depuis des décennies, nous avons laissé s'installer la domination des Gafam sur le monde numérique européen. Le présent rapport dresse un constat des menaces et des dommages causés par le laisser-faire qui a prévalu.

La véritable force des Gafam est d'avoir également imposé l'idée qu'aucune alternative n'existerait, parce que les solutions techniques des autres acteurs ne seraient pas au niveau et parce que le numérique et ses effets de réseau exigeraient la constitution de giga-plateformes pour le bien du consommateur.

Or de telles alternatives existent bel et bien, et elles permettent d'envisager des modèles différents, synonymes de reconquête de notre propre souveraineté.

### A. LIBRE ET OPEN SOURCE : ALTERNATIVES À LA DOMINATION DES GAFAM

#### 1. L'open source : un outil puissant au service de la réduction des dépendances aux solutions imposées par les grandes entreprises de la tech

##### *a. Le logiciel libre : une définition à partir de quatre libertés fondamentales*

Le concept de logiciel libre a été défini pour la première fois dans les années 1980 par Richard Stallman, et la toute première licence libre publiée en février 1989 (1). Pour être qualifié de libre, un logiciel doit réunir quatre conditions : i) liberté d'utiliser le logiciel, c'est-à-dire d'exécuter le programme, pour tous les usages ; ii) liberté d'étudier le code et de l'adapter à ses besoins ; iii) liberté de copier le logiciel ; iv) liberté d'améliorer le programme et de publier ces améliorations.

Plusieurs types de licences peuvent être associées au logiciel libre. La licence « copyleft » (par opposition au « copyright ») impose qu'un logiciel dérivé conserve le statut de logiciel libre de l'original. En choisissant une licence copyleft, l'auteur pourra empêcher que toute évolution possible de son travail sorte du domaine du libre.

---

*(1)* https://culture-et-outils-libres.forge.apps.education.fr/logiciels-libres.html

Open source et logiciel libre sont des notions très semblables. Cependant, il est considéré que le terme de logiciel libre revêt une acception plus large, en désignant l'ensemble de l'approche, c'est-à-dire à la fois son approche communautaire et ses objectifs sociétaux. L'open source est une notion plus technique, qui désigne davantage une méthode de développement.

### *b. Les atouts décisifs du logiciel libre dans la lutte contre les vulnérabilités et dépendances*

Les caractéristiques du logiciel libre en font une solution incontournable pour lutter contre les dépendances et vulnérabilités induites par l'adoption de solutions propriétaires.

**Premier avantage, le logiciel libre est, par définition, exempt de tout risque de *vendor lock-in*,** puisque l'ensemble des éléments de code sont ouverts, que le code est utilisable sans restrictions, et qu'il peut être copié et adapté.

**Deuxième avantage, le logiciel libre n'est pas soumis à des redevances de licences.** Comme nous le verrons ci-après, cela ne signifie pas pour autant qu'il soit gratuit si l'on intègre les coûts de maintenance et de développement – d'ailleurs, la gratuité ne fait pas partie des quatre critères de définition du logiciel libre. Toutefois, l'utilisation de logiciels open source réduit grandement le coût global des solutions informatiques pour les utilisateurs.

Au-delà de l'absence de redevances de licence, M. Renaud Chaput, directeur technique de Mastodon, soulignait, à l'occasion de la table ronde sur le logiciel libre organisée par la commission d'enquête, que les conditions d'élaboration des logiciels libres les rendaient moins chers à produire, et donc plus compétitifs pour les utilisateurs [(1)] : « *le fait d'être un logiciel libre et de travailler de manière ouverte rend ce travail beaucoup moins coûteux. Nous avons une large base d'utilisateurs, nous travaillons sur des technologies qui fonctionnent, et nous n'avons pas d'intérêts contradictoires comme la gestion d'une régie publicitaire ou de données personnelles, ce qui simplifie nos logiciels. Ainsi, un budget qui paraîtrait ridicule dans une grande entreprise nous suffit pour employer une ou deux personnes au design, une ou deux autres sur l'interface, et obtenir des résultats très efficaces. Dès que nous disposons de ce minimum de moyens, nous sommes capables de créer des logiciels plus performants* ».

M. Nicolas Vivant, fondateur de France numérique libre, directeur de la stratégie et de la culture numériques de la commune d'Echirolles, qui a mené à bien une bascule vers les logiciels libres, a estimé que cela avait permis d'économiser plus de 2,5 millions d'euros de coûts de fonctionnement entre 2020 et 2026. Ne présentant plus aucune dépendance envers Google, Amazon, Microsoft, Oracle ou VMware, la commune n'a, en outre, pas été touchée par les hausses de tarification liées au passage à Windows 11 ou au rachat de VMware.

---

*(1) Table ronde sur le logiciel libre, le 6 mai 2026.*

**Troisième avantage, à rebours de la logique de construction de champions, le logiciel libre repose sur la construction de communautés actives autour de solutions partagées**. Comme l'indiquait M. Etienne Gonnu lors de cette même table ronde : « *Il faut aussi sortir de la quête d'un « champion », terme qui me semble revenir souvent dans vos auditions, et dépasser le strict enjeu de la nationalité, sans même parler de la problématique de l'application extraterritoriale de certaines lois. Ce qui est nécessaire, ce sont des logiciels libres dotés d'écosystèmes robustes, qui s'appuient sur des TPE-PME et une gouvernance claire et transparente. Mastodon ou PeerTube, (…) sont des exemples flagrants de projets libres qui fonctionnent avec des écosystèmes et une gouvernance clairs, sans nécessiter de champion particulier* ».

Les leaders internationaux mettent en avant leur capacité à offrir une solution sur l'ensemble de la planète. Le logiciel libre est une alternative à cette captation des infrastructures essentielles, comme en atteste l'exemple de Signal, dont sa présidente, Mme Meredith Whittaker, indiquait devant la commission d'enquête : « *Cela étant, cette perspective ne répond pas à la question de fond, qui est : comment se fait-il qu'un dispositif aussi vertueux et nécessaire que Signal ne constitue pas le modèle par défaut ? Une telle situation met en évidence un biais économique structurel et appelle d'autres interrogations, notamment sur les modalités permettant d'assurer la pérennité d'une infrastructure réellement indispensable (…).*

« *Dans les années 1990, les conditions ont été réunies pour permettre à un nombre restreint d'entreprises de s'imposer dans une logique de monopole et nous utilisons aujourd'hui leurs serveurs parce que cela est nécessaire pour assurer une couverture mondiale, sans disposer, pour notre part, des milliards de dollars annuels requis pour reproduire de telles infrastructures. Toutefois, nous mettons en œuvre un chiffrement rigoureux qui garantit que, même en recourant aux serveurs de ces entreprises, celles-ci ne peuvent accéder à vos données, puisque seul l'utilisateur détient les clés permettant d'accéder à ses communications sur Signal* ». (1)

**Quatrième avantage, le logiciel libre est plus résilient puisqu'il ne dépend pas de son propriétaire.** L'utilisation de logiciel propriétaire expose à deux risques importants : le *kill switch*, restriction volontaire de la part de son propriétaire, et l'arrêt du développement du produit pour des raisons économiques (faillite de l'entreprise, réorientation stratégique, etc.). Le fonctionnement de l'open source empêche de tels scénarios de se produire, ainsi que l'indique le directeur de la stratégie et de la culture numériques de la commune d'Echirolles (2) : « *une fois que Linux est installé sur mon serveur, il est à moi. Si demain la fondation coule, j'ai le temps de travailler tranquillement à une alternative. Pour GitHub, c'est pareil : si la plateforme venait à disparaître, nous avons des copies de nos codes en local sur nos machines. C'est le principe de GitHub : synchroniser des machines*

*(1) Audition, de Mme Meredith Whittaker, présidente de la fondation Signal, le 25 mars 2026.*

*(2) Table ronde sur le logiciel libre, le 6 mai 2026.*

*en local avec le dépôt. Effectivement, cela prendrait un peu de temps de créer un compte ailleurs, mais nous sommes capables de déplacer le code. Ce n'est pas du tout le même niveau de dépendance* ».

**Cinquième avantage, les solutions techniques sont souvent de grande qualité, et même meilleures que leurs alternatives propriétaires.** La preuve en est que les grands éditeurs de solutions se basent très largement sur des produits open source pour développer leurs propres plateformes. M. Renaud Chaput en donne ainsi un exemple : « *La plateforme Azure de Microsoft (…) repose en grande partie sur des logiciels libres ; ils y ont simplement apposé un logo et embauché des dizaines de milliers de personnes pour la présenter comme un produit. Google Cloud et les services d'Amazon sont entièrement construits sur du logiciel libre* » (1). À propos de la messagerie cryptée Signal, Mme Whittaker décrivait l'effet d'émulation créé par l'ouverture du code, qui incitait l'ensemble de la communauté à travailler à l'amélioration des solutions open source : « *Au cours des dix dernières années, nous avons acquis, au sein de la communauté technique, une réputation qui nous place véritablement comme un étalon de référence. Cela signifie qu'un écosystème complet s'est structuré autour de nous : nous ne nous limitons pas à publier du code dans une bibliothèque en ligne, mais nous avons développé une infrastructure entière qui fonde la confiance du public, non sur des opinions, mais sur des faits. Les hackers savent que, s'ils parviennent à compromettre notre système, ils trouveront un emploi chez nous* » (2).

La transition vers le libre peut ainsi être indolore pour les utilisateurs – « *il n'y a pas de résistance de la part des utilisateurs lorsque vous leur proposez un logiciel meilleur que celui qu'ils utilisent »,* relève Nicolas Vivant. « *Si vous interrogez les agents de la ville d'Échirolles, ils vous diront qu'ils n'ont pas noté de grands changements. Pourtant, ces changements ont été nombreux : réorganisation de l'équipe, préparation budgétaire*, reporting, monitoring, *documentation, tout a changé.* » (3).

Sixième avantage, le **code du logiciel libre est auditable** par toute personne qui souhaite l'examiner. Une telle propriété permet d'éviter l'insertion de fonctionnalités cachées. Tout utilisateur pourra ainsi vérifier les risques liés à l'utilisation du logiciel concerné. C'est le fondement même de la politique de Signal, dont le caractère open source des solutions est la meilleure garantie de résistance aux pressions politiques en vue de l'introduction de *« backdoors »* : « *Pour nous, la communication privée est un droit humain fondamental, sans lequel la démocratie et une vie pleine de sens ne sont pas possibles. Nous existons pour protéger ce droit et nous le faisons en fournissant un outil, un logiciel et des protocoles open source qui sont essentiels à la protection de la vie privée. (…) Pour autant, je peux avancer des arguments convaincants, mais cela demeure insuffisant lorsqu'il est question d'un élément aussi fondamental. La norme devrait être de*

*(1) Table ronde sur le logiciel libre le 6 mai 2026.*

*(2) Audition, de Mme Meredith Whittaker, présidente de la fondation Signal, le 25 mars 2026.*

*(3) Table ronde sur le logiciel libre le 6 mai 2026.*

*pouvoir vérifier et valider par soi-même, en accédant aux fondements techniques. (…) Ainsi, il n'est nul besoin de me croire sur parole, et tel n'est d'ailleurs pas mon objectif, car toutes les preuves sont accessibles* ».

Dans un contexte où la sortie des dépendances aux logiciels propriétaires doit constituer une priorité, le logiciel libre revêt de nombreux atouts qui en font une solution technique incontournable. Cet état de fait était d'ailleurs largement reconnu par l'ensemble de la filière. D'après une enquête réalisée auprès de 608 organisations publiques et privées de plus de vingt employés, commandée par le Conseil national du logiciel libre (CNLL), Numeum et Systematic Paris-Region [(1)], 90 % des structures interrogées considèrent l'open source comme *« un atout majeur pour la souveraineté numérique de la France et de l'Europe ».*

### 2. Un important potentiel économique

#### *a. Une filière française très dynamique et leader européenne*

Comment une économie peut-elle se baser sur quelque chose de gratuit ? Le modèle d'affaires repose sur la vente de services associés :

– les revenus des logiciels open source correspondent aux revenus générés par les fonctionnalités payantes et les contrats de support des logiciels libres ;

– les revenus issus des services open source correspondent aux revenus générés par les contrats de services s'appuyant sur des technologies open source ou les contrats d'hébergement et d'exploitation de solutions open ource.

Pour résumer, l'open source génère des revenus liés au développement de fonctionnalités adaptées aux particularités du client et au maintien en conditions opérationnelles de ces solutions dans son système informatique. À l'exception des clients les plus dotés en capacités de développement en interne, les utilisateurs ne seront pas capables de maîtriser l'ensemble des produits, et achèteront donc des prestations annexes de développement, de maintenance et d'exploitation.

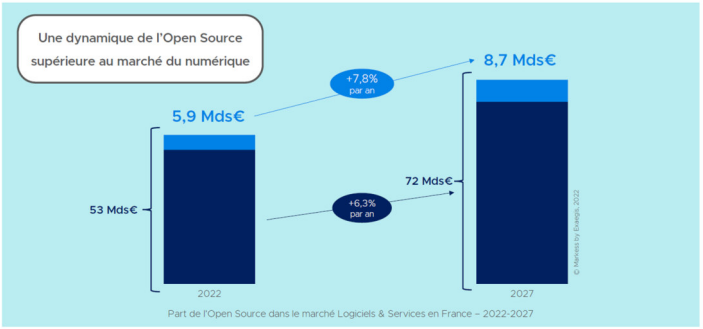
L'open source s'appuie sur une filière très dynamique en France. Ce sont les conclusions d'une étude de marché réalisée par le cabinet Markess en 2022 [(2)]. Cette étude apporte des éléments d'éclairage importants sur la taille du marché de l'open source français et sa comparaison avec la situation d'autres pays européens.

– Le marché de l'open source – rassemblant à la fois la vente de logiciels et de services – représentait 5,9 milliards d'euros en 2022, soit 11 % du marché total des logiciels et services numériques. Le marché est en croissance de 7,8 % par an, une tendance supérieure à celle du secteur (+ 6,3% par an). L'open source représentait 63 800 équivalents temps plein en 2022.

---

*(1) CNLL, Numeum, Systematic, Open source monitor France, Rapport 2023*

*(2) Markess,* Le marché de l'open source en France et en Europe, *novembre 2022* https://cnll.fr/news/etude-2022-le-march%C3%A9-de-lopen-source-en-france-et-europe/

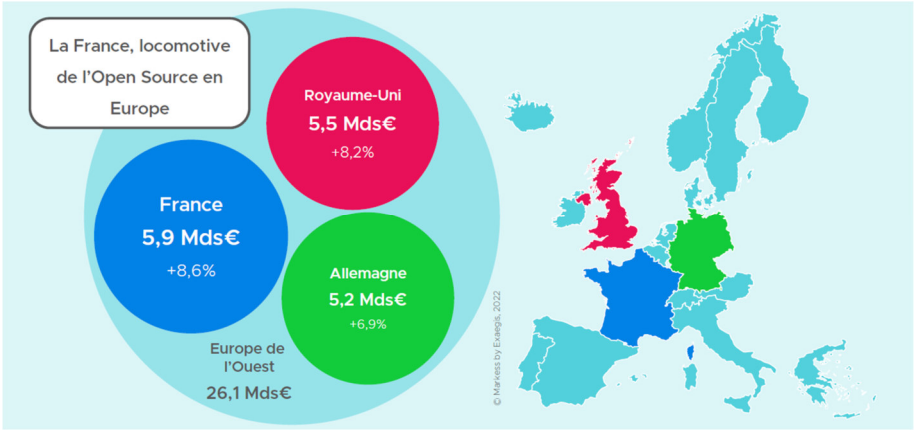



*Source : Markess.*

Fait intéressant, l'étude relève que les services de cloud open source IaaS et PaaS sont en croissance notable, et devraient représenter 21 % des services dans l'open source en 2027, soit un volume d'affaires de 1,7 milliard d'euros. Comme l'indique l'étude, « *les solutions technologiques open source sont à la base de nombreux services cloud vendu. Parmi elles, CloudStack, les containers Docker, Kubernetes, Prometheus pour le monitoring et les plateformes de gestion des services Cloud, Keycloak pour la gestion des accès et identités, PostreSQL, MongoDB et MariaDB pour les bases de données. Parse pour les solutions serverless promises à un bel avenir. L'ESN spécialiste de l'open source Alter way s'est ainsi centrée sur l'implémentation et la gestion des infrastructures cloud* ».

L'étude mentionne également que les solutions open source deviennent des références dans le domaine de la cybersécurité, et couvrent l'ensemble des besoins. Elle anticipe une très forte croissance de l'activité dans le domaine de l'intelligence artificielle et du big data.

Enfin, l'étude positionne la filière française de l'open source par rapport à ses homologues européennes. **Elle se situe à la première place**, devant le Royaume-Uni et l'Allemagne, et **représente 22 % du marché européen total**.




*Source : Markess.*

### *b. Un potentiel de contribution à la croissance très important*

En 2021, la Commission européenne commandait une étude pour mesurer le poids économique du secteur de l'open source, et sa contribution au PIB européen (1). Là encore, les conclusions montrent que cette filière est d'ores et déjà très dynamique et que le soutien à l'écosystème aurait des impacts économiques très positifs, en particulier pour les PME.

Le poids économique de l'open source dans l'économie européenne est estimé entre 65 et 95 milliards d'euros en 2018. Surtout, un soutien actif à la filière produirait des effets économiques en termes de croissance : *« une augmentation de 10 % [des contributions au logiciel libre] générerait chaque année entre 0,4 % et 0,6 % de PIB supplémentaire pour l'UE ».*

L'étude relève également que les développeurs européens de logiciels libres (développeurs indépendants, universitaires, fonctionnaires et salariés du privé) contribuent de manière significative à l'écosystème mondial des logiciels libres. « *Dans l'UE, ce sont les employés des petites et très petites entreprises qui sont le plus susceptibles de contribuer à la production de codes de logiciels libres (on parle de « commits »), tandis qu'aux États-Unis les commits sont principalement produits par les grandes entreprises du secteur des TIC, qui fondent avec succès leurs modèles commerciaux pertinents sur le vaste corpus de codes de logiciels libres disponibles gratuitement et en constante amélioration* ». Les contributions à la production de logiciel open source, dépassant les 30 millions par an en 2018, représentaient un investissement en personnel d'environ un milliard d'euros. Le nombre de contributeurs individuels se chiffrait à 260 000, soit 8 % des près de 3,1 millions d'employés européens travaillant dans le secteur de la programmation informatique. Cela témoigne donc d'une véritable culture de l'open source, à même de garantir sa solidité. Une augmentation de 10 % des contributions permettrait de créer environ 600 start-up supplémentaires par an.

## 3. La nécessité de renforcer l'écosystème de façon ciblée pour permettre un véritable passage à l'échelle

« *Le fait qu'un logiciel soit libre ne signifie pas qu'il soit protégé ; sa pérennité dépend de l'existence d'une communauté active de contributeurs, d'un investissement continu et de financements suffisants* », comme l'a rappelé M. Henri Verdier (2). Les atouts du logiciel libre vont de pair avec certaines fragilités, qui en sont le corollaire inévitable. Son développement exige que des conditions de faisabilité soient remplies.

---

*(1) European commission,* The impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy, *septembre 2021*

*(2) Audition de M. Henri Verdier le 10 mars 2026.*

### *a. Contribuer aux communs*

i. Le défi du financement

**Tout d'abord, le développement des briques et produits open source repose sur les contributions volontaires, ce qui peut constituer un risque pour la pérennité des produits**. Comme le relève M. Gosset, « *Nous sommes très conscients d'un problème dans le logiciel libre : le financement de la maintenance. C'est bien d'avoir un logiciel qui sort en 2026, mais comment faire pour qu'il soit toujours fonctionnel en 2027, en 2028 et au-delà ?* » Une rupture de continuité dans la maintenance, en cas d'arrêt d'un travail bénévole, ou un changement de gouvernance, peuvent constituer de graves vulnérabilités pour l'ensemble de l'écosystème. « *Un logiciel vit et évolue*, a expliqué M. Renaud Chaput. *Des failles de sécurité et des bugs apparaissent, nécessitant des corrections. Souvent, cela repose sur un réseau de volontaires qui maintiennent des logiciels libres très spécifiques mais omniprésents dans nos téléphones et ordinateurs. Récemment, une faille a été découverte dans une bibliothèque logicielle gérée par une seule personne sur son temps libre. Cette faille impactait des serveurs dans le monde entier. Cette personne a rappelé que, malgré l'utilisation massive de son travail, elle n'avait jamais reçu un euro de financement.* » (1)

Rendre le logiciel ergonomique et facile d'accès nécessite, en outre, un engagement significatif dont les acteurs du libre n'ont pas toujours les moyens. Pour M. Chaput, « *la vraie difficulté pour beaucoup de logiciels libres est que le terme est souvent associé au bénévolat. Énormément de logiciels libres ont été initiés par des passionnés, qui ont peut-être trouvé d'autres passionnés, mais qui développaient ces projets en plus de leur travail. Chez Mastodon, nous nous sommes rendu compte que pour créer un logiciel qui fonctionne bien, qui est simple au point que l'on oublie que c'en est un, qui n'est pas « moche » et qui marche mieux que les autres solutions, il est essentiel d'avoir quelques personnes qui y travaillent à temps plein. C'est un effort constant. Nous avons récemment lancé une nouvelle fonctionnalité qui paraît toute simple, mais qui a nécessité neuf mois de travail pour deux personnes afin d'atteindre cette simplicité. C'est un niveau de finition que beaucoup de logiciels libres ont du mal à atteindre, car ils sont souvent développés par des personnes qui y consacrent quelques heures par-ci par-là. Or, rendre un logiciel simple à utiliser est un vrai métier.* »

**Le troisième écueil à surmonter est celui du financement des investissements.** Les logiciels propriétaires sont financés par les éditeurs de logiciels, soit sur leurs fonds propres en avance de phase, soit pour répondre directement à des commandes des clients. La problématique pour l'open source est de pouvoir trouver des développeurs à même de répondre à des besoins clients, et surtout de les financer de façon vertueuse, sans que les premiers ne supportent un coût démesuré, ce qui suppose de mutualiser autant que possible les briques open source.

---

*(1) Table ronde sur le logiciel libre le 6 mai 2026.*

M. Chaput soulignait ainsi la difficulté à faire porter à des petites collectivités le coût du développement des fonctionnalités de la Suite territoriale. « *J'ajoute qu'au niveau des coûts, il y a une vraie question de mutualisation. Lorsqu'un syndicat se lance avec une suite nouvelle, s'il n'a que trois clients, ses coûts fixes sont probablement les mêmes à 90 % que s'il en avait deux cents. Nous le voyons côté Mastodon, et je pense que c'est vrai pour tous les logiciels libres : un des avantages des géants du numérique est justement leur taille. Ils ont développé une automatisation massive qui leur permet d'opérer pour des millions de clients avec un nombre très réduit d'intervenants humains. Mais cela est le fruit d'années d'investissements se chiffrant en centaines de millions ou en milliards de dollars, y compris de la part de la puissance publique américaine, qui ont amené ces géants à une taille telle que leurs coûts de revient deviennent marginaux. C'est une des magies de l'informatique : on peut automatiser beaucoup de choses, mais la mise en place de cette automatisation a des coûts fixes élevés. Demander aux très petites structures qui sont les premières à se lancer dans la suite territoriale de financer le déploiement de toutes ces automatisations, c'est un peu leur faire supporter le coût de rattrapage de dix, quinze ou vingt ans de retard sur la mutualisation. C'est un facteur de coût réel* ».

**L'objectif est donc de parvenir à un équilibre entre contributions individuelles et investissements des entreprises ou des administrations, de façon à maintenir le code dans la durée**. M. Pierre-Yves Gosset, coordinateur des services numériques de Framasoft, défend un tel engagement [(1)] : « *Si l'on considère le logiciel libre comme un produit sur étagère qui coûte zéro, cela ne peut pas fonctionner. La vraie difficulté est de passer d'une stratégie de consommation à une stratégie de contribution. Si vous ne faites que récupérer le logiciel sans travailler dessus, sans le maîtriser, cela ne fonctionnera pas (…) Il faut contribuer à ce commun numérique (…) Souvent, que ce soit dans les administrations ou les entreprises, on constate une grande difficulté à opérer cette bascule mentale, à se dire : « je ne paie pas, mais je ne vais pas contribuer en plus ». Si le discours était : « vous n'avez peut-être pas payé le logiciel, mais vous allez reverser du code et des améliorations pour le bien commun et l'intérêt général », je pense que nous aurions déjà franchi un pas* ».

ii. De premières initiatives de soutien public

Des initiatives ont vu le jour pour soutenir le financement des communs numériques.

**En la matière, le modèle allemand a été cité comme référence par de nombreux auditionnés.** L'Allemagne a mis en place, en 2022, un fonds, le ***Sovereign Tech Fund***, pour financer les briques open source de bas niveau essentielles à l'ensemble des infrastructures numériques mais difficiles à monétiser (bibliothèques de données, protocoles d'open source etc.). Doté d'un budget de 25 millions d'euros, il dépend d'une agence fédérale, la *Sovereign Tech Agency,*

*(1) Table ronde sur le logiciel libre, le 6 mai 2026.*

filiale de l'agence SPRIND et indépendante depuis 2024, sous tutelle du ministère de la numérisation et de la modernisation de l'État (BMDS) [(1)].

Le modèle, qui repose sur la contractualisation et non les subventions, est plébiscité par les acteurs du libre qui, comme Framasoft ou Mastodon, tiennent à préserver leur indépendance financière à l'égard des États. La *Sovereign Tech Agency* dispose de programmes pour salarier des développeurs à temps plein ou à temps partiel, les former, ou les aider à recruter afin d'assurer la maintenance de ces briques essentielles. Elle peut également signer des contrats avec des opérateurs du libre pour qu'ils développent certaines fonctionnalités, si elle estime qu'elles sont utiles à l'ensemble de la société – elle l'a notamment fait avec Mastodon, au motif qu'un réseau social est nécessaire à une démocratie fonctionnelle. Enfin, l'agence facilite l'accès des acteurs du libre aux institutions publiques en promouvant leurs services auprès de l'État allemand. « *Quiconque discute avec les acteurs quotidiens de l'open source vous confirmera que la Sovereign Tech Agency a un impact réel sur ce secteur et sur sa viabilité à grande échelle* » affirme M. Renaud Chaput.

Au niveau européen, la France, l'Allemagne, les Pays-Bas, l'Italie et le Luxembourg ont créé **l'Edic *Digital Commons*,** un consortium pour une infrastructure européenne dédiée aux communs numériques, avec l'objectif d'investir conjointement dans des briques numériques ouvertes, interopérables et réutilisables, pour soutenir l'autonomie stratégique de l'Europe. Les travaux de l'Edic se concentreront, en 2026, sur le système d'exploitation du poste de travail et la recherche sémantique entre différents outils collaboratifs. Comme l'a affirmé Mme Stéphanie Schaer, « *cette ambition européenne repose sur une conviction simple : seule la mutualisation de nos investissements, de nos talents et de nos capacités industrielles nous permettra d'apporter des réponses concrètes et de nous affranchir des dépendances imposées par des acteurs monopolistiques. Elle suscite d'ailleurs l'intérêt d'autres États : la Dinum a récemment signé avec son homologue québécois une déclaration d'intérêt fondée sur ces communs numériques. »* [(2)].

Tout en saluant l'initiative qu'il a contribué à porter, M. Henri Verdier a regretté que « *les moyens qui lui seront alloués restent modestes, de l'ordre de quelques millions d'euros* ». Pour Mme Ophélie Coelho, si ce type de projet favorise la coopération et la consolidation de standards communs, il pâtit du manque de coordination entre États membres et de la lenteur des procédures, qui reflète « *la fragmentation des acteurs et des intérêts au sein de l'Union* ». : « *Les projets sont toujours très intéressants sur le papier, mais je regrette qu'ils ne communiquent pas suffisamment entre eux. J'ai eu l'occasion de discuter avec certains responsables, et ils travaillent vraiment dans leur coin. C'est regrettable, car plusieurs Edic sont compatibles entre eux ou avec d'autres projets européens, et ils pourraient éviter de réinventer des couches technologiques déjà développées ailleurs. Je me demande parfois s'il ne faudrait pas créer une sorte de Centre européen de la recherche*

*(1) Réponses écrites de l'Ambassade de France en Allemagne au questionnaire de la rapporteure.*

*(2) Audition de Mme Stéphanie Schaer le 14 avril 2026.*

*nucléaire (Cern) du numérique, qui rassemblerait la recherche, les choix stratégiques de l'État, le secteur public et les entreprises. Nous avons un vrai problème de cohérence. La politique industrielle de l'Europe, si tant est qu'elle existe de manière clairement établie, manque de cohésion d'ensemble. »* (1)

Une généralisation de ce type de financement serait conforme au principe « *public money, public code* » selon lequel les investissements publics doivent bénéficier à l'ensemble de la communauté.

***b. Diffuser la culture des communs numériques dans la sphère professionnelle***

i. Le frein des compétences

**Le déploiement de logiciels libres peut également se heurter au manque de compétences dédiées dans les administrations**. Comme le souligne M. Renaud Chaput, il est essentiel que, « *lorsqu'une ville, une entreprise ou un ministère installe un logiciel libre, il y ait des personnes capables de « soulever le capot » et de comprendre comment il fonctionne* ».

Dans le cas d'Echirolles, les principales résistances se sont trouvées non du côté des utilisateurs, mais des services informatiques, comme l'a expliqué M. Nicolas Vivant : « *Un passage au logiciel libre ne consiste pas simplement à remplacer des logiciels propriétaires ; c'est un nouveau paradigme, un nouveau projet, une nouvelle façon de travailler, et donc un changement complet à opérer. Or, un service informatique est une équipe avec des compétences techniques, des équilibres et des habitudes de travail qui peuvent être fortement ancrées. Quand les compétences, parfois durement acquises, reposent sur des logiciels propriétaires, et que les agents qui les maîtrisent sont valorisés, un changement de cap induit forcément des bouleversements qu'il ne faut pas négliger. Tenter de convaincre tout le monde et de faire monter en compétences l'ensemble de l'équipe, c'est s'attaquer à l'Everest par la face nord en hiver*. »

Pour surmonter cet obstacle, il a revu la stratégie de recrutement, en utilisant le renouvellement naturel de l'équipe pour recruter des talents qui disposaient des compétences attendues et d'une appétence pour le logiciel libre, par une refonte des fiches de poste.

Le profil de compétences des personnels constitue bien un élément clé. Le directeur du numérique pour l'éducation, M. Audran Le Baron, a mis en avant cet atout : « *La culture du logiciel libre est intrinsèquement liée aux ressources internes en matière de numérique, un domaine dans lequel les ministères ne sont pas tous égaux. Il se trouve que nos trois ministères présentent un niveau assez homogène en la matière, car nous figurons parmi les quelques grands ministères à bénéficier de corps de fonctionnaires spécialisés dans le numérique. Au sein du ministère de l'éducation nationale, par exemple, nous nous appuyons sur le corps des ITRF*

*(1) Table ronde sur les infrastructures numériques le 2 avril 2026.*

*(ingénieurs et techniciens de recherche et de formation), dont une partie possède une expertise numérique. Nous disposons donc d'un grand corps de fonctionnaires particulièrement qualifiés, qui se maintiennent à niveau sur ces questions. Nombre d'entre eux ont été formés très tôt, dans leur métier de développeur, à l'utilisation de technologies libres. Par conséquent, cette culture du libre est profondément ancrée dans leur formation initiale et demeure très présente dans leurs pratiques* » (1).

ii. Pour une contribution des agents publics aux communs

Au-delà du soutien financier, les administrations peuvent contribuer directement aux communs numériques. C'est notamment le cas de la gendarmerie nationale, qui participe à la communauté du libre, et du ministère de l'éducation nationale qui promeut auprès des enseignants les outils pédagogiques reposant sur des logiciels libres, et met à leur disposition une forge logicielle pour en créer ou en développer en commun.

La politique en faveur des communs numériques éducatifs a été exposée par M. Audran Le Baron : « *Parmi les communs numériques que nous utilisons figure Moodle, une plateforme d'enseignement à distance qui est probablement le logiciel libre le plus utilisé au monde dans la sphère universitaire et de l'enseignement. Nous avons déployé à l'échelle nationale une plateforme Moodle nommée Éléa, que tout enseignant peut utiliser pour créer ses cours et faire faire des activités à ses élèves. Nous avons une autre plateforme, basée sur le notebook Jupyter, qui est aussi une technologie libre qui permet à des professeurs de partager des activités autour de l'enseignement de l'informatique, des sciences numériques et, plus globalement, des Stiam (sciences, technologies, ingénierie, arts et mathématiques). Nous avons également proposé la Forge des communs numériques éducatifs, c'est-à-dire un atelier au sein duquel les enseignants peuvent créer des ressources, des outils numériques libres, en open source. Cette forge est motorisée par un GitLab – c'est le même type de forge que celle que nous utilisons en interne pour le développement de systèmes d'information. Nous promouvons beaucoup cette culture, au-delà des frontières du numérique proprement dit, parce que je pense que nous avons beaucoup à y gagner*. » (2) Le commun MathALÉA, qui génère de façon aléatoire des exercices de mathématiques suivant les programmes scolaires officiels, a notamment été créé dans ce cadre.

À l'occasion de l'actualisation de la stratégie du numérique pour l'éducation 2023-2027, intervenue en 2025, le ministère a annoncé une feuille de route et un dispositif de soutien à l'innovation et au maintien durable des communs numériques éducatifs. La rapporteure appelle à déployer pleinement cette politique. Il est indispensable de proposer des formations dédiées à l'utilisation de ces ressources partagées, et de mieux structurer et valoriser les communs numériques existants afin de faciliter leur déploiement parmi les enseignants et auprès des élèves.

---

*(1) Table ronde réunissant des directeurs de systèmes d'information de ministères le 9 avril 2026.*

*(2)* Ibid.

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

Il s'agit en particulier de renforcer la formation des enseignants aux logiciels libres, d'investir dans la production, le développement et la maintenance des communs numériques éducatifs, et de mieux valoriser les outils partagés existants, notamment issus de la forge.

Cette dynamique gagnerait à être généralisée à l'ensemble des administrations de l'État, en permettant à tous les agents qui le souhaitent de contribuer aux communs numériques.

**Recommandation n° 15 : Permettre aux agents de l'État de contribuer, l'équivalent d'une journée par an, à des communs numériques de leur choix dans une logique d'intérêt général (exemple : Forge des communs numériques, Grist, Debian, Wikipedia, etc.).**

Une telle mesure permettra de renforcer la contribution des administrations aux communautés développant des projets open source, de diffuser les connaissances détenues par les agents publics, et de favoriser la connaissance des logiciels libres au sein des personnels de l'État.

### *c. Activer le levier de la commande publique*

Les acteurs du logiciel libre auditionnés ont tous souligné le rôle essentiel de la commande publique pour consolider l'écosystème. La loi pour une République numérique du 7 octobre 2016, en son article 16, prévoit que les administrations « *veillent à préserver la maîtrise, la pérennité et l'indépendance de leurs systèmes d'information. Elles encouragent l'utilisation des logiciels libres et des formats ouverts lors du développement, de l'achat ou de l'utilisation, de tout ou partie de ces systèmes d'information* ». Comme la première partie du rapport l'a montré, les logiciels libres demeurent néanmoins minoritaires, à l'exception de quelques administrations.

Pour M. Etienne Gonnu, le principe de priorité aux logiciels libres va de soi : « *Si l'on considère que les quatre libertés du logiciel libre – étudier, modifier ou faire modifier, et partager – répondent à des impératifs d'intérêt général (indépendance, mutualisation, maîtrise de l'équipement), alors une administration qui, dans son appel d'offres, choisit de se priver de l'une de ces capacités doit le justifier au regard d'autres intérêts contradictoires de même valeur, selon un principe de proportionnalité somme toute classique.* » (1)

L'orientation de la commande publique vers les logiciels libres est limitée par plusieurs freins, notamment : les difficultés que rencontrent les communes pour mutualiser leurs investissements dans le cadre actuel ; l'impossibilité d'imputer les dépenses d'aide à l'installation de logiciels libres sur le budget d'investissement, qui pourrait être amorti sur plusieurs années ; et le fait que la lourdeur de la procédure des marchés publics favorise souvent les gros groupes, au détriment des petits acteurs.

*(1) Table ronde sur le logiciel libre le 6 mai 2026.*

Sur ce dernier point, des instruments juridiques ont été créés pour favoriser le développement de produits innovants conçus par les petites entreprises, tels que le partenariat d'innovation prévu par l'article 31 de la directive 2014/24/UE sur la passation des marchés publics.

La Centrale d'achat de l'informatique hospitalière (CAIH), s'est emparée du dispositif. Elle a lancé, en février 2025, un appel d'offres pour un partenariat d'innovation visant à concevoir, expérimenter et industrialiser une suite logicielle souveraine open source qui pourrait être généralisée à l'ensemble des établissements hospitaliers en 2027.

M. Thomas Jan, directeur général adjoint en charge de l'innovation et de la stratégie numérique de l'Union des hôpitaux pour les achats (UniHa), a présenté le projet devant la commission d'enquête :

« *Le nouveau président de la CAIH, qui est le DSI de l'AP-HP (Assistance publique-Hôpitaux de Paris), ayant souhaité s'engager dans une démarche offensive en matière de souveraineté, nous avons conclu un partenariat d'innovation dédié aux technologies open source. Nous ne faisons pas de choix technologique en amont ; un industriel nous accompagne dans la conception du produit – c'est-à-dire l'assemblage de briques open source, qui doit tenir compte des spécificités du domaine de la santé, notamment la gestion des comptes HospiConnect –, son déploiement et le support. Nous avons également été accompagnés par un avocat expert des questions de souveraineté numérique qui nous aide à privilégier des industriels français, que ce soit pour les briques de résilience, le déploiement ou la maintenance.*

« *Au terme de ce travail interne de conception qui a duré six mois, nous avons lancé le partenariat d'innovation, qui doit à présent franchir différentes étapes. Après avoir reçu neuf candidatures, nous avons retenu les trois industriels prêts à répondre à l'offre technique. En juin, nous choisirons celui d'entre eux qui nous accompagnera. Celui-ci travaillera ensuite en hackathon, avec les douze établissements candidats, à la construction du produit. L'intérêt de ce type de marché est qu'au terme du processus, le produit sera disponible. Dans quatre ans, nous pourrons le renouveler en chargeant, le cas échéant, un autre industriel de déployer et d'assurer le support de cet outil créé pour la communauté hospitalière. Nous avons tout intérêt à ce que d'autres acteurs saisissent l'opportunité d'utiliser les mêmes briques technologiques que nous, de manière à produire un effet de levier et à faciliter la transformation*. » [(1)]

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

*(1) Table ronde des acheteurs publics le 9 avril 2026.*

### *d. Prévenir l'appropriation par les Big Tech*

Enfin, le dernier danger est celui de **l'entrisme des Big Tech**. C'est une façon pour eux de faire entrer par la fenêtre les logiques de propriété auxquelles le logiciel libre avait fermé la porte. Le meilleur exemple en est la forge Github, acquise par Microsoft en 2018. Comme l'explique M. Gosset, « *Microsoft a fait une excellente affaire, car aujourd'hui, une énorme partie des développements de code libre se fait sur cette plateforme. La raison pour laquelle les développeurs du monde du logiciel libre vont sur une plateforme opérée par Microsoft est simple : c'est l'effet de réseau. Plus il y a de monde sur une plateforme, plus il est simple d'entrer en contact (...) La deuxième bonne opération de Microsoft, au-delà de la quantité de code, a été d'y faire tourner ses modèles d'intelligence artificielle. GitHub est la plus grande bibliothèque de code au monde, ce qui leur permet de repérer des talents, des logiciels émergents, et d'entraîner leurs IA pour ensuite les revendre* ».

Les licences copyleft, qui garantissent qu'un projet logiciel construit avec ce type de licence conserve cette même licence libre dans le temps, constitue un « *outil puissant* », même si « *ce n'est pas une baguette magique contre les risques de réappropriation* » a déclaré M. Etienne Gonnu.

Une autre solution pour contourner ces stratégies d'entrisme est décrite par M. Pierre Yves Gosset : « *Comment s'en prémunir ? Il faut créer d'autres silos de données à côté de cet énorme silo qu'est GitHub. Chez Framasoft, nous avons une forge qui s'appelle FramaGit. Je peux aussi citer Codeberg, une forge opérée en Allemagne qui héberge des codes libres du monde entier, sans publicité ni exploitation des données personnelles. Le ministère de l'éducation nationale héberge également une forge des communs numériques. Il faut multiplier ces forges logicielles, qui sont encore trop peu nombreuses, et les interconnecter* ».

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

Le logiciel libre constitue la seule véritable alternative au modèle des Gafam. Parce qu'il présente toutes les qualités nous permettant de sortir de la dépendance à des solutions technologiques omniprésentes, il doit être au cœur de la stratégie numérique française. Cela nécessite pour cela de créer des instruments qui assureront sa solidité et sa pérennité dans le temps.

## B. LA NÉCESSAIRE GÉNÉRALISATION DES STANDARDS OUVERTS

Les logiciels open source se développent sur des standards ouverts, qui sont aujourd'hui peu interopérables avec les solutions de marché. Le renforcement des obligations d'interopérabilité constitue le second levier essentiel pour permettre la sortie des dépendances aux acteurs dominants et faire émerger un modèle différent.

### 1. Les atouts de l'interopérabilité

L'interopérabilité renvoie à la capacité de deux systèmes ou logiciels de pouvoir échanger des données. Elle implique que les informations soient renseignées selon des formats communs, à l'aide de protocoles partagés et des interfaces de programmation d'application (API) sur lesquelles il est possible de se connecter.

Les standards ouverts permettent de **lutter contre les positions monopolistiques des Big Tech**, en garantissant que d'autres acteurs puissent les concurrencer en proposant leurs produits. L'Autorité de la concurrence a souligné, dans ses réponses écrites, que « *la standardisation comme l'imposition d'obligations d'interopérabilité au titre de la régulation sectorielle sont pertinentes pour renforcer la transparence et la contestabilité des marchés du secteur numérique, protéger et promouvoir l'innovation mais également renforcer la capacité des utilisateurs à changer de fournisseurs de services et à se tourner vers les fournisseurs qui répondent le mieux à leurs demandes y compris sur des paramètres de concurrence non tarifaires comme peuvent l'être la soutenabilité ou la résilience* ».

En cassant les effets de réseaux, l'interopérabilité **rééquilibre le jeu en faveur des petites entreprises innovantes**. « *Si davantage de petits acteurs européens très compétents pouvaient se connecter et proposer leurs services, cela permettrait de mieux répartir le pouvoir et la capacité de contrôle,* observe Alexandra Lutz. *Il faut rappeler qu'au niveau européen, 99 % des entreprises sont des PME. C'est ce tissu qu'il faut soutenir, plutôt que de tout miser sur quelques géants ».* Comme le confirme Mme Francesca Musiani, « *avec les architectures fédérées, chacun peut contribuer selon ses capacités et ses disponibilités* ». L'interopérabilité permet aussi de surmonter la *fear of missing out* (Fomo), la peur de manquer quelque chose, qui pousse à rester sur les plateformes concentrant le plus grand nombre d'utilisateurs, « *puisqu'il serait possible, demain, de quitter Instagram pour rejoindre Mastodon tout en continuant à suivre des comptes restés sur Instagram* » [(1)].

De plus, **l'interopérabilité présente l'avantage de permettre l'intégration de solutions européennes diverses** répondant aux besoins des utilisateurs. Les standards ouverts proposent de fait une alternative à l'écosystème propriétaire intégré, celle d'une **architecture fédérée et décentralisée** qui préserverait la qualité de l'expérience utilisateur. Le directeur de recherche David Chavalarias en a montré tout le potentiel à travers l'exemple du réseau social Mastodon : « *Au lieu d'utiliser une grosse machine détenue par un seul acteur qui regroupe l'ensemble des utilisateurs et des données, vous pouvez avoir 10 000 machines détenues par autant d'acteurs différents. Mastodon fonctionne ainsi, par exemple. Comme les machines utilisent les mêmes protocoles, les utilisateurs peuvent discuter et créer un écosystème. Il faut sortir de cet ancien*

*(1) Table ronde sur les infrastructures numériques le 2 avril 2026.*

*monde, fondé sur des colonies numériques dans lesquelles un grand acteur refuse la portabilité pour rester propriétaire de ses utilisateurs, et changer de paradigme pour aller vers des écosystèmes numériques reposant sur des protocoles.* » (1)

Cette interopérabilité est vectrice de **résilience**, puisqu'en cas de défaillance ou d'indisponibilité d'un maillon, il est possible de reporter les usages sur les autres et d'assurer la continuité de l'activité, là où la monoculture et la dépendance généralisée à un acteur unique créent un risque systémique. M. Nicolas Vivant a salué la grande solidité de ces infrastructures ouvertes et décentralisées : « *Si demain notre serveur plante, cela ne plantera pas Mastodon. La messagerie utilisée par l'État, Tchap, sur laquelle nous travaillons pour un projet destiné aux collectivités, repose sur la même architecture distribuée. Si demain Tchap tombe, les collectivités pourront continuer à discuter entre elles. Seules les solutions libres et fédérées permettent ce niveau de résilience. Cette décentralisation est indispensable. Une étude du Ripe (réseau IP européen) sur la résilience de l'internet en Ukraine en situation de guerre a montré que le réseau n'est jamais tombé. Pourquoi ? Parce qu'en Ukraine, il n'y a pas quatre grands opérateurs, mais des dizaines de milliers de petits opérateurs locaux interconnectés. Il est impossible de détruire l'infrastructure internet globale du pays*. »

Enfin, une architecture décentralisée favorise un **modèle économique plus respectueux des droits fondamentaux et de la démocratie**, dans lequel les utilisateurs pourront exercer leur liberté de choix pour peser sur la gouvernance de l'infrastructure. Pour M. Bastien Le Querrec, juriste à La Quadrature du net, « *un tel cadre favoriserait l'émergence d'alternatives, notamment de start-up françaises et européennes, qui pourraient, au sein de cet écosystème de réseaux sociaux interopérables appelé Fediverse, proposer des algorithmes plus vertueux, voire s'en passer, ou encore développer des modèles économiques fondés sur l'abonnement et assortis d'engagements en matière de confidentialité. Les internautes disposeraient ainsi d'un véritable choix et pourraient participer à la définition des règles de modération. Aujourd'hui, dans le milieu des réseaux sociaux interopérables, les règles varient selon les instances : l'instance mamot.fr, gérée par La Quadrature du Net, applique par exemple des règles qui peuvent être moins strictes que celles d'instances se présentant comme des safe spaces pour la communauté LGBTQIA+. Il n'existe pas de modèle unique de modération et les règles sont déterminées par les internautes eux-mêmes au sein de chaque instance et, en cas d'insatisfaction, il leur est possible d'en changer sans perdre leurs contenus* » (2).

Comme l'a expliqué M. Renaud Chaput, ce modèle vise à limiter le pouvoir de la plateforme, et à empêcher toute forme d'ingérence :« *Concernant le contrôle de Mastodon, nous opérons une grosse instance, mastodon.social, sur laquelle s'appliquent nos règles de modération et la loi allemande. Mais nous n'avons aucun moyen de forcer les autres serveurs à faire quoi que ce soit, et nous ne le voulons pas. Nous poussons à la décentralisation car nous voyons bien les abus possibles.*

---

*(1) Table ronde réunissant M. David Chavalarias, M. Robin Berjon et Mme Maud Quessard le 10 mars 2026.*

*(2) Table ronde sur le thème de la protection des données personnelles le 25 mars 2026.*

*Même si Mastodon devenait un succès immense, nous ne voulons pas de cette responsabilité, ni qu'un gouvernement puisse nous forcer la main, comme on l'a vu avec Elon Musk utilisant son réseau social à des fins politiques. C'est l'antithèse de nos idées. Mastodon a commencé comme un projet technique, mais c'est aujourd'hui un projet politique. Le numérique est si important que les choix d'architecture, comme l'interopérabilité, sont devenus des enjeux clés pour la démocratie.* »

### 2. Une obligation qui monte en puissance

Pour M. David Chavalarias, « *l'État a un rôle important à jouer pour favoriser l'émergence de standards et la stabilisation de protocoles ouverts. Comme il l'a fait pour les télécommunications en adoptant une loi grâce à laquelle les utilisateurs conservent la propriété de leur numéro de téléphone, il doit imposer des règles permettant de casser les monopoles et de retrouver une libre concurrence, qui favorisera sans doute l'innovation. Certains acteurs chercheront à faire du profit tandis que d'autres privilégieront les biens communs numériques, mais leurs services seront interconnectables, ce qui permettra aux seconds de se développer*. » Les législateurs européens et nationaux ont, de fait, posé les prémices d'un cadre d'interopérabilité en imposant des obligations qui sont encore en phase d'implémentation.

En matière de cloud, le règlement européen sur les données du 22 décembre 2023 (Data Act) vise à lever les barrières au changement de fournisseur et à favoriser le recours au multi-cloud en imposant des obligations de portabilité, d'interopérabilité et d'ouverture d'API, applicables depuis le 12 septembre 2025. La Commission européenne est habilitée à adopter des normes harmonisées ou des spécifications d'interopérabilité.

Certaines mesures ont été introduites par anticipation en droit français par la loi Sren du 21 mai 2024. Celle-ci impose, en son article 28, que les fournisseurs de services cloud assurent leur interopérabilité avec les services d'autres fournisseurs, et la portabilité des actifs numériques entre les deux offres. Pour ce faire, ils sont tenus de mettre à disposition des API et des informations suffisamment détaillées pour permettre à des services tiers de communiquer avec leurs services. L'Arcep est chargée de vérifier le respect de ces exigences, et d'en préciser les modalités par l'édiction de spécifications d'interopérabilité et de portabilité. Dans ses recommandations d'octobre 2025, l'Autorité a ainsi recommandé des bonnes pratiques de transparence et de stabilité des API, tout en promouvant l'adoption de la spécification OpenAPI. Il est cependant encore trop tôt pour en dresser le bilan, compte tenu du calendrier d'application du Data Act et délais de mise en conformité des fournisseurs.

Des obligations de ce type ont également été instituées en droit de la concurrence. Conformément au DMA, les plateformes désignées comme contrôleurs d'accès doivent rendre leurs services interopérables avec ceux de leurs concurrents.

L'article 6, paragraphe 7, du règlement prévoit une interopérabilité verticale, permettant aux tiers d'échanger avec les fonctionnalités matérielles et logicielles contrôlées par le système d'exploitation. Le 19 mars 2025, la Commission européenne a adopté deux premières décisions visant à préciser les obligations d'Apple pour améliorer la connectivité des appareils et des applications de fabricant tiers avec certaines fonctionnalités de l'iPhone, et renforcer l'efficacité et la transparence du traitement des demandes d'interopérabilité avec iOS par Apple. La Commission a également ouvert, en janvier 2026, une procédure pour vérifier que Google ne favorisait pas son service Gemini en limitant l'accès des fournisseurs tiers de services d'intelligence artificielle aux fonctionnalités d'Android (1).

L'article 7 édicte une obligation d'interopérabilité horizontale spécifique pour leurs services de messagerie, en imposant aux contrôleurs d'accès de fournir sur demande et gratuitement les interfaces techniques nécessaires. Ils disposaient de six mois pour mettre en œuvre cette interopérabilité s'agissant des conversations individuelles, et de deux ans pour les conversations de groupe. À ce jour cependant, seulement deux fournisseurs de services de messagerie, BirdyChat et Haiket, ont annoncé, en novembre 2025, qu'ils deviendraient interopérables avec WhatsApp au cours de l'année 2026 (2).

M. Umberto Berkani a reconnu que le « *DMA constitue à cet égard un premier élément de solution. La Commission européenne relève d'ailleurs, dans ses rapports, des avancées concrètes en termes d'interopérabilité, de portabilité des données et de liberté de choix pour les clients. Il est toutefois prématuré d'en mesurer pleinement les effets puisque, comme tout texte nouveau, il fait l'objet de contestations par les entreprises visées, et il faudra attendre que cette pratique soit validée par les cours de justice, ce qui mobilise du temps et des ressources*. » (3)

Si l'article 53 du DMA prévoit que la Commission européenne doit évaluer à échéance régulière l'opportunité d'élargir l'obligation d'interopérabilité aux réseaux sociaux, ce n'est toujours pas le cas aujourd'hui. Le droit à la portabilité des données reconnu par l'article 20 du RGPD peut s'en trouver limité, faute d'interfaces techniques.

Dans certains cas, ces verrous techniques sont délibérément mis en place par les plateformes, comme l'a expliqué M. David Chavalarias s'agissant de X (4) : « *Certains volets du RGPD, concernant, notamment, la portabilité, sont en partie respectés, ce qui a permis aux utilisateurs de réclamer leurs archives sur X afin d'utiliser OpenPortability dans le cadre de l'opération HelloQuitteX. Néanmoins, nous n'en sommes pas encore à la portabilité effective des données. Dans le cas de X, cette possibilité a été volontairement supprimée. À l'époque de Twitter, des API*

---

*(1) Rapport annuel de la Commission européenne sur l'application du règlement sur les marchés numériques (DMA), présenté le 21 mai 2025 (COM[2026] 247 final).*

*(2)* Ibid.

*(3) Audition de M. Umberto Berkani le 5 mai 2026.*

*(4) Table ronde réunissant M. David Chavalarias, M. Robin Berjon et Mme Maud Quessard le 10 mars 2026.*

*(Application Programming Interfaces, interfaces de programmation d'application) gratuites et très efficaces permettaient de transférer les données d'une plateforme à une autre. Elles ont été délibérément fermées. Autrement dit, X a décidé d'empêcher la portabilité effective des données qui existait du temps de Twitter* ».

Pour permettre aux utilisateurs qui le souhaitaient de quitter X, le chercheur a conduit l'initiative HelloQuitteX en mettant à disposition un dispositif technique de portabilité des données. Le dispositif a été utilisé par plusieurs dizaines de milliers de personnes, témoignant du fait que « *la société civile est en attente d'une solution de ce type* ». Relatant les menaces dont il a fait l'objet par l'entreprise d'Elon Musk et l'écosystème Maga, sans aucun soutien des institutions, David Chavalarias a appelé à une réaction européenne : « *Si nous voulons assurer la souveraineté numérique de l'État, il faut protéger ce genre d'initiatives, les soutenir et leur permettre de se développer pour passer à l'échelle. Ce n'est pas un laboratoire isolé – nous n'étions que deux chercheurs – qui devrait mettre en place la portabilité. Le sujet devrait être traité au niveau européen et des moyens suffisants devraient lui être consacrés, d'autant que le problème ne concerne pas seulement les réseaux sociaux mais également d'autres infrastructures.* »

### 3. Le rôle clé de la puissance publique pour investir et définir des standards ouverts partagés

Au-delà de l'instauration d'obligations juridiques, il revient à l'État d'investir dans des infrastructures ouvertes communes et de contribuer à la consolidation des standards ouverts.

M. Henri Verdier a cité **l'exemple de l'Inde, où la construction par les pouvoirs publics de la plateforme ouverte, interopérable et gratuite UPI, en 2016, a permis de révolutionner le système de paiement** : « *J'observe, en Inde, une approche très intéressante fondée sur le développement des infrastructures publiques numériques, une mise en œuvre réussie de ce que j'appelais il y a quelques années l'État plateforme. Prenons l'exemple du paiement. L'État impose l'existence d'interfaces de programmation d'application (API) gratuites que toutes les banques sont obligées d'implémenter. Les entreprises privées sont ensuite libres de développer leurs propres services de paiement – plus de six cent sont ainsi en concurrence. Google garde une part de marché majoritaire, mais ne possède ni les données ni l'infrastructure et n'a donc pas la capacité d'exclure ou de déconnecter les autres acteurs. Les Indiens se sentent, à raison, en sécurité : le marché et la concurrence fonctionnent mais au sein d'infrastructures sous contrôle public. Ces dernières ne sont d'ailleurs pas coûteuses. Elles reposent sur un design d'API et une architecture logique, sans grands serveurs ni vastes data centers.* » (1) En 2024, le réseau UPI comptait plus de 500 millions d'utilisateurs et avait vu transiter 3 200 milliards de dollars, soit 82 % du PIB indien (2).

*(1) Audition de M. Henri Verdier le 10 mars 2026.*

*(2) Clément Perruche, « UPI, moteur de l'inclusion bancaire en Inde »,* Les Echos, *22 octobre 2025.*

Le succès indien a inspiré des initiatives similaires dans de nombreux autres pays. La banque centrale brésilienne a ainsi lancé, en 2020, le système de paiement numérique instantané PIX pour limiter la dépendance aux réseaux Visa et Mastercard pour les transactions numériques. Le professeur Luca Belli a présenté son fonctionnement et ses bénéfices lors de son audition : « *Cette infrastructure publique numérique, fondée sur des protocoles de standards ouverts et pilotée par la banque centrale, est désormais adoptée par l'ensemble du secteur bancaire national. Les bénéfices de cette politique sont multiples. Outre l'autonomie stratégique, elle permet de réinjecter dans l'économie les 3 à 5 % de commissions autrefois captés par les acteurs américains. Cette somme, qui représente plusieurs milliards, est désormais reversée dans les poches des consommateurs et des entreprises brésiliennes. Surtout, PIX brise le monopole de Visa et Mastercard sur la collecte et le traitement des données*. (…) *Ce succès repose sur la vision systémique de la Banque centrale, l'une des institutions les plus stables du pays. En 2020, elle a ainsi su identifier le risque posé par le lancement concomitant de WhatsApp Payment. Consciente que la position dominante de Meta aurait pu étouffer PIX, elle a imposé un délai au service de WhatsApp au nom de la protection de la concurrence et des données* » (1).

**L'État devrait également reprendre le contrôle sur la définition des standards techniques et des protocoles sur lesquels repose le fonctionnement d'internet**. Comme l'a expliqué Mme Francesca Musiani, « s*ur la couche des protocoles, la gouvernance est traditionnellement plus distribuée, avec des organisations comme l'Internet Corporation for Assigned Names and Numbers (ICANN) pour les noms de domaine ou l'Internet Engineering Task Force (IETF) qui élabore les standards techniques. Toutefois, des études montrent que même dans ces espaces, certains acteurs disposent de fait d'une capacité d'influence supérieure, liée à leurs importantes ressources techniques, humaines et économiques. (...) Les acteurs qui participent à l'élaboration des protocoles au sein de l'IETF ou d'autres organisations, ou qui imposent des standards de fait, comme Google avec le protocole QUIC, contribuent à définir les règles du jeu, des formats de données aux niveaux de sécurité.* »

**Il s'agirait pour l'État de favoriser la consolidation de standards interopérables** : « *Si l'on consolide des standards, par exemple pour la bureautique, et que l'on s'assure que les formats ouverts comme l'open document format devienne la norme d'usage, voire deviennent hégémoniques, on garantit que toute nouvelle solution devra se conformer à ce standard. C'est aussi une manière de s'assurer que les usages ne dépendent pas uniquement de logiques de profit, mais de quelque chose que l'on maîtrise collectivement* », illustre M. Etienne Gonnu.

La commande publique constitue à cet égard un levier majeur. **Le gouvernement allemand a annoncé, en mai 2025, la création du Deutschland-Stack, qui vise à fournir un socle technologique commun de briques open**

*(1) Audition de M. Luca Belli, professeur de gouvernance et régulation numériques à la fondation Getulio Vargas de Rio de Janeiro, le 7 mai 2026.*

**source et interopérables pour l'État, les Länder et les communes**. Elle couvre à la fois les infrastructures (centres de données, serveurs, réseaux), les plateformes (gestion des données, logiciels, modèles d'IA), et les applications. Pour y parvenir, l'IT-Planungsrat, le Conseil de planification informatique, a formalisé des normes strictes imposant des interfaces ouvertes et des formats harmonisés à l'ensemble des projets qui seront menés dans ce cadre. L'obligation faite aux acheteurs publics de recourir au format ouvert ODF pourrait notamment créer un effet d'entraînement sur tout l'écosystème, précise M. Etienne Gonnu : « S*i toute la puissance publique utilise et impose ce format, il devient beaucoup plus facile de quitter Microsoft, car n'importe qui d'autre peut proposer une alternative compatible. On réduit ainsi drastiquement l'adhérence. Cela ne résout pas tout d'un coup de baguette magique, mais cela crée de l'offre par la demande. Quand c'est fait à l'échelle d'un État comme l'Allemagne, on voit bien comment ce genre d'investissement peut soutenir et amplifier l'écosystème.* »

**Des standards partagés peuvent, enfin, favoriser la mutualisation des efforts entre le secteur public et le secteur privé**. C'est tout le sens de **l'initiative Open Interop** lancée par le comité stratégique de filière Logiciels et solutions numériques de confiance et présentée par le président du CSF M. Michel Paulin lors de son audition. Elle a pour ambition de spécifier, documenter et développer des composants open source pour établir un socle technologique commun, avec des API fédérées, et permettre aux utilisateurs publics et privés une meilleure interopérabilité. Cette approche, soutenue par l'État, doit permettre de mieux articuler les outils développés par la Dinum avec les offres du marché, en garantissant la liberté de choix des ministères. Mme Stéphanie Schaer a ainsi souligné « *toute l'importance de l'interopérabilité : les agents publics amenés à travailler avec ces différents outils doivent pouvoir bénéficier d'une ergonomie complète leur permettant de passer facilement de l'un à l'autre* ».

La rapporteure relève que la France dispose déjà d'un référentiel général d'interopérabilité qui impose aux administrations l'utilisation de répertoires de données, de normes et de standards, tel que le prévoit l'article 11 de l'ordonnance n° 2005-1516 du 8 décembre 2005 [(1)]. La dernière mise à jour du référentiel est intervenue en 2016. À cet égard, M. Loïc Dayot a appelé à ce que les normes existantes « *soient complétées et deviennent contraignantes* » : « *Actuellement, des commandes publiques qui ne respectent pas les référentiels généraux d'accessibilité, d'interopérabilité, de sécurité ou de sobriété peuvent encore être passées, ce qui n'est pas normal. Il serait vraiment intéressant de les renforcer. Pour les données personnelles, la Commission nationale de l'informatique et des libertés (Cnil) vérifie la conformité ; elle n'a sans doute pas assez de moyens, mais sa présence envoie un signal. Nous appelons par exemple à une « Cnil de l'interopérabilité », qui empêcherait que n'importe quelle solution puisse être achetée par la fonction publique*. »

*(1) Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives*

## C. RÉDUIRE LES IMPACTS NÉGATIFS DE L'IA

L'utilisation des modèles d'intelligence artificielle à grande échelle, dans tous les pans de l'économie, pose plusieurs problèmes dont : la consommation d'électricité et l'opacité sur l'utilisation des données et les conditions d'entraînement des modèles. Les stratégies de promotion de l'intelligence artificielle qui n'apporteraient pas de réponses structurelles à ces deux problèmes constituent donc une faute politique majeure puisqu'elles risquent d'aggraver le changement climatique et de contribuer au pillage de la connaissance à des fins mercantiles, voire à la diffusion d'informations attentatoires aux droits individuels et à la démocratie.

### 1. L'IA frugale

L'utilisation de modèles IA dits frugaux est aujourd'hui un enjeu fondamental pour le futur de cette technologie, eu égard aux investissements et coûts énergétiques massifs associés à l'élaboration des modèles et à l'inférence et de leur impact environnemental. Deux dimensions doivent ainsi être prises en compte : la consommation énergétique des modèles, mais également la nécessité même de recourir à l'IA pour remplir les tâches considérées.

L'Association française de normalisation (Afnor) a défini une première norme [(1)], la Spec 2314, qui définit des méthodologies de calcul et des bonnes pratiques pour mesurer et réduire l'impact de l'IA, de façon à permettre de « communiquer avec des allégations justes et vérifiables ». La définition retenue de la frugalité est la suivante : « *La frugalité d'un service d'IA vise à réduire globalement les besoins en ressources matérielles et énergétiques et les impacts environnementaux associés via une redéfinition des usages ou des exigences de performance (…) ou encore via une réorientation des besoins du producteur du système d'IA (amont) au fournisseur du service considéré. Un service frugal d'IA est donc un service pour lequel :*

« *– la nécessité de recourir à un système d'IA plutôt qu'à une autre solution moins consommatrice pour répondre au même objectif a été démontrée ;*

« *– de bonnes pratiques (…) sont adoptées par le producteur, le fournisseur et le client d'IA pour diminuer les impacts environnementaux du service utilisant un algorithme d'IA ;*

« *– les usages et les besoins visent à rester dans les limites planétaires et ont été préalablement questionnés* ».

Elle met l'accent sur la mesure de l'adéquation des outils d'IA aux besoins réels des utilisateurs.

---

*(1) AFNOR Spec 2314, juin 2024* https://www.afnor.org/actualites/intelligence-artificielle/referentiel-reduire-impact-environnemental-ia/

**L'AI Act ne contient aucune disposition contraignante sur le sujet de la performance énergétique des modèles.** Les seules obligations sont celles prévues par le point 2 d) de l'annexe XI relative à la documentation technique pour les fournisseurs de modèles d'IA à usage général, qui prévoit que ces derniers doivent communiquer des informations concernant « *la consommation d'énergie connue ou estimée du modèle* ». Dans le code de bonne pratique publié par le bureau de l'IA (1), et dont la vocation est d'aider les fournisseurs de modèles à se conformer à l'AI Act, le formulaire à remplir dans le cadre du chapitre relatif à la transparence comprend une section dédiée au calcul de la consommation d'énergie des modèles, reproduite ci-dessous :

| | Energy consumption (during training and inference) | AIO | NCAs | DPs |
|---|---|---|---|---|
| **Amount of energy used for training:** | Measured or estimated amount of energy used for training, reported in Megawatt-hours and recorded with at least two significant figures (e.g. $1.0 \times 10^2$ MWh). If the amount of energy used for training cannot be estimated due to the lack of critical information from a compute or hardware provider, enter 'N/A'. | ☒ | ☒ | ☐ |
| **Measurement methodology:** | In the absence of a delegated act adopted in accordance with Article 53(5) AI Act to detail measurement and calculation methodologies, describe the methodology used to measure or estimate the amount of energy used for training. Where the energy consumption of the model is unknown, the energy consumption may be estimated based on information about computational resources used. If the amount of energy used for training cannot be estimated due to a lack of critical information from a compute or hardware provider, the provider should disclose the type of information they lack. *[Recommended 100 words]* | ☒ | ☒ | ☐ |
| **Benchmarked amount of computation used for inference[1]:** | Benchmarked amount of computation used for inference, reported in floating point operations, recorded with at least two significant figures (e.g. $5.1 \times 10^{17}$ floating point operations). | ☒ | ☒ | ☐ |
| **Measurement methodology:** | In the absence of a delegated act adopted in accordance with Article 53(5) AI Act to detail measurement and calculation methodologies, provide a description of a computational task (e.g. generating 100000 tokens) and the hardware (e.g. 64 Nvidia A100s) used to measure or estimate the amount of computation used for inference. | ☒ | ☒ | ☐ |

[1] This item relates to energy consumption during inference, which makes up the "energy consumption of the model" (Annex XI, 2(e), AI Act) together with energy consumption during training. Since energy consumption during inference depends on more than just the model itself, the information required for this item is limited to relevant information depending only on the model, namely computational resources used for inference.

Les informations demandées sont particulièrement légères (taille de 100 mots recommandée), et une grande latitude est laissée aux fournisseurs concernant les méthodologies de calcul. Dans son avis sur les enjeux concurrentiels liés à l'impact énergétique et environnemental de l'IA, **l'Autorité de la concurrence mettait ainsi en valeur les risques d'information trompeuse pouvant être caractéristiques de pratiques anticoncurrentielles** (2) : « *des acteurs peuvent être tentés d'adopter des comportements trompeurs en termes de frugalité. Une telle situation pourrait notamment se produire lorsque la frugalité ou l'empreinte environnementale mise en avant ne repose pas sur une méthodologie robuste en termes scientifiques. Ainsi, un ou plusieurs acteurs pourraient, individuellement ou conjointement, mettre en avant la frugalité ou plus précisément encore l'impact environnemental faible ou mesuré de leurs solutions alors même que cette caractéristique serait erronée. Que le caractère trompeur de cette caractéristique soit volontaire ou non, elle pourrait s'apparenter à une forme de « green washing » (en français « verdissement »). Un tel comportement pourrait dès lors s'avérer problématique au regard du droit des*

*(1) https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai*

*(2) Autorité de la concurrence, ibid.*

*pratiques anticoncurrentielles (abus de domination ou entente) soit parce qu'il peut porter directement préjudice aux clients, soit parce qu'il peut permettre de bénéficier d'avantages concurrentiels, comme l'octroi de conditions avantageuses pour opérer sur un marché par exemple. À cet égard, l'Autorité appelle les pouvoirs publics à être particulièrement vigilants dans la fixation et la mise en œuvre des critères de sélection dans les appels d'offres comme dans l'octroi de soutiens financiers ».*

Cette situation perdurera tant que l'acte délégué prévu à l'article 53 (5) n'est pas publié. Une consultation publique sur le sujet a été ouverte en avril 2026 et est désormais clôturée (1). **À ce stade :**

**– les obligations ne portent que sur les informations à divulguer. La consultation envisage l'édiction d'« indicateurs de performance », sans que leur caractère obligatoire ne soit précisé.**

**– De plus, il est envisagé que ces indicateurs mesurent la consommation d'énergie par instance ou tâche, et non l'intérêt et l'adéquation de l'utilisation de l'IA pour réaliser cette tâche par rapport à une solution consommant moins d'énergie.**

Enfin, il est important de noter que la Dinum et le ministère chargé de la transition écologique ont fait paraître une fiche pratique pour l'achat responsable de solutions d'intelligence artificielle (2). Elle contient notamment des clauses types à destination des acheteurs publics.

### 2. L'IA open source

#### *a. La définition des modèles ouverts : OSAID 1.0, ou le débat sur la publication des données d'entraînement*

L'adaptation de la définition de l'open source aux modèles d'IA s'est rapidement posée comme une question essentielle. Contrairement aux logiciels traditionnels, ces modèles ne peuvent être définis par la seule ouverture de leur code source. D'autres paramètres devaient être pris en considération : le code, mais aussi l'architecture et surtout les conditions et données d'entraînement.

Open source initiative est l'association américaine responsable du maintien de la « définition de l'open source » (« *Open source definition* », OSD). Ses travaux ont donc été au cœur de ce processus d'adaptation. Comme l'explique le site de l'association (3), « *les systèmes d'IA modernes, tels que les grands modèles linguistiques, développent un comportement souvent imprévisible et inexplicable. Les processus d'apprentissage sont difficiles à reproduire de manière fiable, même par les créateurs du système. Ces particularités ont rendu nécessaire l'élaboration*

---

*(1)* https://digital-strategy.ec.europa.eu/en/consultations/targeted-consultation-measuring-energy-consumption-and-emissions-ai-models-and-systems

*(2)* https://ecoresponsable.numerique.gouv.fr/docs/2025/MINUMECO_fiche_IA_frugale_VF.pdf

*(3)* https://opensource.org/ai/faq#why-did-you-write-the-open-source-ai-definition

*d'une définition spécifique, allant au-delà de la « définition de l'open source » applicable aux logiciels* ».

Après deux ans d'échanges techniques, Open source initiative a publié en novembre 2024 une définition de l'open source applicable à l'intelligence artificielle, appelée « open source AI definition version 1.0 » (OSAID 1.0). Cette définition adapte les quatre libertés caractéristiques de la définition générale de l'open source au cas des modèles d'IA générative (1) : « *Une IA open source est un système d'IA mis à disposition selon des conditions et d'une manière qui garantissent les libertés :*

« *– d'utiliser le système pour tout but et sans autorisation requise ;*

« *– d'étudier le fonctionnement du système et d'en examiner les composants ;*

« *– de modifier le système pour tout but, y compris pour changer ses résultats ;*

« *– de partager le système afin que d'autres puissent l'utiliser, avec ou sans modifications, pour tout but.*

« *Ces libertés s'appliquent aussi bien à un système entièrement fonctionnel qu'à ses éléments distincts. Une condition préalable à l'exercice de ces libertés est d'avoir accès à la forme souhaitée pour apporter des modifications au système* ».

L'élaboration de l'OSAID 1.0 a donné lieu à d'âpres débats sur un point en particulier, l'exigence de publication des données nécessaires à l'entraînement des modèles. La définition retenue **n'exige pas la publication des données d'entraînement**. Comme l'explique l'OSI, « *Certaines personnes estiment qu'un accès total et sans restriction à toutes les données d'entraînement (sans distinction de nature) est primordial, arguant que toute restriction compromettrait la reproductibilité totale des systèmes d'IA, ainsi que leur transparence et leur sécurité. Cette approche reléguerait l'IA open source à une niche ne pouvant être entraînée que sur des données ouvertes. Cette niche serait minuscule, même par rapport à celle occupée par l'open source dans l'écosystème logiciel traditionnel. Les exigences d'information sur les données conservent la même approche que celle présente dans l'OSD ; elles n'imposent pas une reproductibilité et une transparence totales, mais les rendent possibles (approche de la reconstruction reproductible)* ». Exiger la publication de l'ensemble de données d'entraînement aurait écarté d'office les modèles entraînés sur la base de données privées, même acquises légalement, et de données sensibles ou confidentielles (par exemple, données personnelles de santé). C'est pourquoi le choix a été fait de ne pas exiger la publication intégrale. L'objectif que s'est fixée l'OSAID 1.0 est la **reconstruction reproductible**, c'est-à-dire la capacité pour quiconque à pouvoir parvenir au même résultat grâce à l'ensemble des informations données sur les méthodes et données d'entrée.

---

*(1) https://opensource.org/ai/open-source-ai-definition*

Parmi les institutions opposées aux choix réalisés par l'OSI, la *Free Software Foundation* et la *Software Freedom Conservancy*, dont le directeur, Bradley M. Kühn, a publié les commentaires suivants (1) : « *Le processus d'élaboration de l'OSAID a donné lieu à de vives polémiques, et cet article de blog ne résume pas l'ensemble des critiques formulées par la communauté à l'encontre de l'OSAID et de son processus d'élaboration. D'autres blogueurs et la presse se sont déjà penchés sur ces questions. En résumé, à mon avis, le problème est simple : l'OSAID n'exige pas que le public puisse reproduire le processus scientifique de développement de ces systèmes, car il n'impose pas d'exigences suffisantes en matière de licence et de divulgation publique des ensembles de données d'entraînement pour les systèmes dits « open source ». L'OSI a refusé d'ajouter cette exigence en raison d'une faille fondamentale dans son processus ; elle a décidé qu'« il était inutile de publier une définition à laquelle aucun système d'IA existant ne pouvait actuellement se conformer ». Ce compromis fondamental a sapé le processus communautaire et amplifié le rôle des parties prenantes qui tireraient un avantage financier de la déclaration rétroactive de l'OSI selon laquelle leurs systèmes sont « open source ». L'OSI aurait dû s'abstenir de publier une définition pour l'instant et, à la place, qualifier ce document de «recommandations » provisoires (…). OSI a également privé les utilisateurs et les créateurs de contenu de leur voix dans ce processus. Les militants du logiciel libre devraient s'engager dans des discussions plus larges avec les communautés concernées de créateurs de contenu pour savoir ce que signifie pour eux le terme « open source », et ce qu'ils pensent de l'intégration de leurs données dans les ensembles d'apprentissage de ces systèmes tiers. La frontière entre les données et le code est si facilement franchie avec ces systèmes que nous ne pouvons plus nous fier aux vieilles conclusions toutes faites selon lesquelles « les données sont distinctes et peuvent être propriétaires (voire indisponibles), tandis que le système reste "open source" ». Cet adage ne tient pas la route lorsqu'il s'agit d'analyser cette technologie, et nous devons avancer avec prudence — en nous affranchissant des intérêts commerciaux des entreprises emportées par l'engouement pour l'IA — pour déterminer comment nos philosophies bien établies s'appliquent à ces changements* ».

Ces débats montrent bien l'enjeu que revêt la publication des données pour l'entraînement des modèles. Or, cet enjeu a d'ores et déjà trouvé une traduction réglementaire dans l'AI Act.

### *b. La traduction réglementaire : le risque de l'open-washing*

L'AI Act introduit une définition réglementaire de l'IA ouverte, en prévoyant un régime spécifique pour la catégorie des modèles d'IA *:* « *publiés dans le cadre d'une licence libre et ouverte permettant de consulter, d'utiliser, de modifier et de distribuer le modèle, et dont les paramètres, y compris les poids, les informations sur l'architecture du modèle et les informations sur l'utilisation du modèle, sont rendus publics* ».

---

*(1) https://sfconservancy.org/blog/2024/oct/31/open-source-ai-definition-osaid-erodes-foss/*

L'article 53 de l'AI Act introduit notamment des exemptions d'obligations réglementaires pour les modèles respectant cette définition (hors modèles d'IA à usage général présentant un risque systémique). Ne s'appliquent pas à ces modèles les obligations d'élaborer et de tenir à jour la documentation technique du modèle et de mettre à disposition des fournisseurs en aval les catégories d'informations listées en annexe XII de l'AI Act.

En revanche, les obligations d'information sur l'origine des données d'entraînement sont les mêmes pour tous les modèles Les c) et d) de l'article 53 exigent ainsi que « *les fournisseurs de modèles d'IA à usage général (…)*

« *c) mettent en place une politique visant à se conformer au droit de l'Union en matière de droit d'auteur et droits voisins, et notamment à identifier et à respecter, y compris au moyen de technologies de pointe, une réservation de droits exprimée conformément à l'article 4, paragraphe 3, de la directive (UE) 2019/790;*

« *d) élaborent et mettent à la disposition du public un résumé suffisamment détaillé du contenu utilisé pour entraîner le modèle d'IA à usage général, conformément à un modèle fourni par le Bureau de l'IA* ».

Ainsi, aucune spécificité n'existe pour des modèles open source du point de vue de l'information relative aux données d'entraînement.

En décembre 2025, le bureau de l'IA a publié la notice explicative concernant le formulaire à remplir et le niveau de détail à donner par chaque fournisseur pour respecter l'exigence du 1. d) de l'article 53 [(1)]. Le bureau de l'IA explique ainsi que le niveau de détail requis a été adapté pour tenir compte de la protection du secret des affaires : « *Afin de protéger le secret des affaires des fournisseurs, le formulaire exige différents niveaux de détail en fonction de la source des données considérées. En particulier, la divulgation d'informations est limitée pour les données sous licence, étant donné que les titulaires de droits concernés sont parties aux accords de licence. En outre, les jeux de données privés qui ne font pas l'objet d'une licence commerciale accordée par les titulaires de droits et qui ont été obtenus auprès d'autres tiers ne doivent être répertoriés que s'ils sont de notoriété publique (ou si le fournisseur souhaite les rendre publics) ; dans le cas contraire, ils doivent être décrits de manière générale. Compte tenu du caractère public des informations contenues dans les ensembles de données accessibles au public, des précisions supplémentaires sont requises concernant ces ensembles de données, y compris la divulgation des « grands » ensembles de données (tels que définis dans le formulaire), conformément au considérant 107 de l'IA Act* ». Ainsi, il est symptomatique de constater que les obligations sont d'autant plus fortes que les jeux de données sont publics, alors que les fournisseurs ont la possibilité de révéler des informations très limitées sur les jeux de données privés utilisés.

(1) https://digital-strategy.ec.europa.eu/en/library/explanatory-notice-and-template-public-summary-training-content-general-purpose-ai-models

La notice explicative précise en outre : « *Les informations demandées dans le formulaire doivent être fournies sous une forme narrative, simple et efficace. Le modèle vise à garantir que les informations communiquées soient utiles et compréhensibles pour le public et pour les parties concernées, tout en évitant d'imposer un fardeau inutile aux fournisseurs de modèles d'IA à usage général, notamment les PME* ». Le bureau de l'IA invoque ici une exigence d'informer le grand public sur les modèles développés, alors que les vocations auraient vocation à être utilisées par les professionnels en mesure d'utiliser, analyser et reproduire les modèles d'IA générative. Le terme de fardeau (« burden ») est d'ailleurs extrêmement révélateur.

À titre de comparaison, l'OSAID 1.0, dont on a vu précédemment qu'elle avait été critiquée par les activistes de l'open source pour son approche permissive, précise que, pour être qualifiées de « suffisamment détaillées », les informations sur les données d'entraînement doivent contenir les critères suivants : « *(1) la description complète de toutes les données utilisées pour l'entraînement, y compris (le cas échéant) les données non partageables, précisant la provenance des données, leur périmètre et leurs caractéristiques, la manière dont elles ont été obtenues et sélectionnées, les procédures d'étiquetage, ainsi que les méthodologies de traitement et de filtrage des données ; (2) une liste de toutes les données d'entraînement accessibles au public et des sources où les obtenir ; et (3) une liste de toutes les données d'entraînement pouvant être obtenues auprès de tiers et des sources où les obtenir, y compris moyennant paiement* ».

**Il apparaît que l'industrie de l'intelligence artificielle a d'ores et déjà tourné le dos à la définition officielle de l'open source définie par l'OSI. Tous les modèles auto-labellisés « open source » ne le sont pas en réalité** (voir notamment [(1)] et [(2)]). **Nous sommes donc face à une situation comparable au green-washing, assimilable à des pratiques commerciales trompeuses.**

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

Cette recommandation devra faire l'objet d'actions au niveau français, vers les fournisseurs de modèles, mais également au niveau européen, à travers la promotion du niveau minimal d'exigence de l'OSAID 1.0 dans toutes les normes européennes.

La définition de l'open source de l'OSAID 1.0. est, en effet, la seule définition officielle de l'open source qui existe à ce jour. Elle est notamment endossée par le pôle open source de la Dinum, par le Conseil national du logiciel libre, et par Software Heritage. En parallèle, il convient de poursuivre le combat pour la transparence sur les données d'entraînement.

*(1)* https://letsdatascience.com/blog/open-source-vs-closed-llms-choosing-the-right-model-in-2026

*(2) Andreas Liesenfeld, Mark Dingemanse,* Rethinking open source generative AI: open-washing and the EU AI Act*, juin 2024*

# CHAPITRE 14 – PROPOSITIONS

## A. POUR UN MODÈLE DE NUMÉRIQUE OUVERT ET LIBÉRATEUR

### 1. Principes

#### *a. Le modèle que nous rejetons*

Depuis plusieurs décennies, nous sommes enfermés dans un modèle qui n'a jamais été remis en cause, malgré sa nocivité pour notre démocratie, notre économie, nos droits et notre santé.

En dix ans, les dépendances aux services numériques états-uniens se sont largement accrues. Les grandes plateformes numériques ont ainsi pu imposer leurs conditions économiques, techniques et commerciales.

En deux ans, depuis l'arrivée au pouvoir de Donald Trump, le contexte géopolitique a rendu crédibles des menaces qui semblaient théoriques jusqu'alors.

Quelles sont les conséquences pour nos concitoyens ? Voici ce que les travaux de la commission d'enquête ont montré :

**Violation de la vie privée de chaque citoyen par l'utilisation inconsidérée de leurs données.** Le modèle économique des plateformes repose sur l'exploitation de la donnée à des fins commerciales, que ce soit directement via le ciblage publicitaire, ou pour élaborer les futurs produits technologiques. C'est en accumulant de nombreuses données sur leurs utilisateurs que les Big Tech ont nourri et entraîné leurs modèles d'intelligence artificielle. Le RGPD, texte pilier de la régulation des données à l'échelle européenne, est régulièrement piétiné, en témoignent les nombreuses sanctions prononcées. Et l'existence d'une juridiction complice, l'Irlande, les protège. Grâce aux instruments que les Gafam ont mis en place, nous pouvons être pistés à chaque instant, fichés et catalogués, ce qui comporte un danger lorsque s'installe un gouvernement qui discrimine sur le fondement de la religion ou de l'opinion politique. L'écosystème qui s'est greffé sur ces géants n'est pas plus vertueux, puisque ces données circulent entre de nombreux acteurs qui en font une utilisation opaque, à des fins commerciales ou de renseignement, sans qu'aucun contrôle ne puisse être exercé en raison de la complexité des chaînes d'intermédiaires.

Nous aurions aussi pu aborder les pratiques de manipulation de l'information, les menaces sur nos démocraties liées aux ingérences étrangères, ou les ravages de l'économie de l'attention en matière de santé publique, autant de thèmes que nous n'avons pas pu traiter dans le temps limité qui nous était imparti.

**Vulnérabilités économiques des administrations et des entreprises, écrasement de la concurrence**. Profondément enracinés dans les systèmes

d'information de l'ensemble de nos organisations, les produits des entreprises états-uniennes ont étouffé ceux de leurs homologues européens. Sur le périmètre des cinquante fournisseurs de logiciels aux administrations les plus importants, les acteurs états-uniens représentent ainsi près 80 % des achats. Les dépenses publiques annuelles pour des solutions extra-européennes s'élèvent à 1,5 milliard d'euros, dont 1 milliard de coût de licences qui pourraient être économisés grâce à l'utilisation de solutions open source. Du fait de l'existence de nombreux verrous techniques et commerciaux, leurs propriétaires peuvent augmenter leurs prix de manière unilatérale, sans crainte de basculement vers la concurrence.

Cette domination passe par la conquête de l'ensemble de la stack technique, des infrastructures essentielles (câbles de fibre optique internationaux, data centers) aux terminaux et aux applications à destination des particuliers. La maîtrise de la chaîne rend possible la vente couplée de produits, ou encore la discrimination des offres concurrentes sur les plateformes gérées par les géants de la tech. Autant de pratiques répréhensibles, qui ont donné lieu à 17 milliards d'euros de sanctions au titre du droit de la concurrence, dont 12 milliards pour le seul Google.

**Danger géopolitique permanent**. Il y a d'abord la vulnérabilité des données qui sont stockées par des acteurs appartenant à des multinationales, y compris sur notre sol. Lorsqu'elles le peuvent, les entreprises dont le siège de la maison-mère est situé aux États-Unis répondront aux injonctions des juges américains. Et quand bien même des dispositifs techniques de chiffrement assureraient une protection suffisante – ce qui reste à démontrer –, les solutions hybrides, reposant sur des technologies américaines, seraient condamnées à l'horizon de quelques jours à quelques mois en cas de *kill switch*. Enfin, la dépendance aux outils numériques extra-européens permet de faire directement pression sur les décideurs politiques.

Ainsi que le résumait Henri Verdier, « *nous avons tout sous les yeux : l'affaire du juge Guillou, des preuves d'espionnage, des serveurs qui se font débrancher, des dominations sur des segments entiers de l'économie, des réseaux sociaux que nous n'arrivons pas à réguler. Et pourtant, les choses ne bougent pas beaucoup* ».

Avec l'intelligence artificielle, le modèle américain atteindra un nouveau palier. Certes, il existe encore de nombreuses inconnues à lever :

**L'ampleur de la transformation macro-économique**. Les précédentes révolutions technologiques ont prouvé que l'enthousiasme initial peut conduire à des effets de bulle spéculative – le FMI lui-même n'écarte pas de tels risques. Nul n'est capable aujourd'hui de prédire la pénétration réelle de l'IA dans notre économie et son impact sur le nombre et la qualité des emplois. De plus les modèles d'IA sont des outils d'essence probabiliste, dont on ne maîtrise pas la production.

Au cœur du problème, **le coût de l'utilisation de l'IA.** Dans une phase de course effrénée pour gagner des utilisateurs afin de maximiser leur valorisation

boursière, les nouveaux empereurs de l'IA diffuse à perte leurs services. Qu'adviendra-t-il du déploiement réel des outils d'intelligence artificielle lorsque le vrai coût des *tokens* sera intégralement reporté sur les consommateurs ?

**Les limites physiques à son développement.** Le développement de l'IA n'est pas dissociable de la capacité des économies à accroître significativement la taille de leur système énergétique. La construction des centrales de production et des réseaux prend plusieurs années. Elle dépend des capacités des fournisseurs d'équipement et des sociétés de construction à suivre le rythme. Sans même parler de l'extraction violente des minerais (coltan, nickel, étain ou or) indispensables à la fabrication des terminaux et des serveurs, ni des conséquences environnementales de l'utilisation massive de l'intelligence artificielle : émissions de gaz à effet de serre, consommation d'eau, contribution à l'artificialisation des sols, rejets de polluants.

**Malgré les incertitudes qui entourent encore la magnitude des transformations engendrées par l'IA, il est de la responsabilité de la puissance publique d'encadrer dès maintenant son développement au vu des dangers profonds qu'elle fait courir à notre société**.

**Une captation de valeur significative et des investissements massifs**. Quand bien même les valorisations des Big Tech seraient surévaluées, nous ne pouvons rester sans réaction face à l'accumulation et à la concentration de telles richesses et moyens aux mains de quelques personnes. Les phénomènes que nous avons connus en quelques années – la croissance des plateformes, la mise en place de l'ensembles des infrastructures – se sont encore accélérés. La pénétration des outils d'intelligence artificielle générative dans les foyers français est fulgurante, bien plus rapide que celle d'internet. Dans les entreprises, la peur de manquer la vague de l'IA conduit à la déployer sans considération des risques de dépendance à des fournisseurs ou de vulnérabilité des données.

**Des implications techniques profondes**. L'IA agentique – agissant en substitution de l'humain pour des séquences de tâches de plus en plus longues – conduit à affaiblir considérablement tout contrôle humain. La cybersécurité en est l'exemple le plus frappant.

Pour rendre le tableau encore plus sombre, ces transformations se produisent dans un contexte d'effondrement rapide de l'industrie européenne face aux deux géants que sont la Chine et les États-Unis.

Quelle place nous reste-t-il alors ? Sommes-nous condamnés à la vassalisation ?

### *b. Le modèle que nous voulons*

Pour nous convaincre de l'existence de solutions, nous reprendrons les mots d'une Américaine, Mme Meredith Whittaker, présidente de la fondation Signal, qui fait référence comme contre-modèle des Gafam.

*« À Bruxelles, à Paris, comme partout dans le monde, de nombreuses analyses sont avancées pour expliquer cette situation, qu'elles invoquent un déficit d'innovation ou une insuffisance de la réglementation, mais ces interprétations passent à côté de l'essentiel (…). Je le redis, si nous nous trouvons aujourd'hui dans cette situation, ce n'est ni en raison d'une réglementation excessive, ni parce que l'innovation ne ferait pas partie de la mentalité française, ni encore faute d'une union des marchés de capitaux, mais parce que le monopole et les décennies d'avance accumulées par les entreprises américaines nous ont conduits au point où nous sommes désormais. Telle est la situation que nous devons examiner ensemble. Cette réalité est certes difficile à admettre, mais il serait plus grave encore de la nier ou de s'y soustraire. Il nous appartient de l'affronter sans peur, car c'est ainsi que nous gagnons en clarté, que nous comprenons mieux le paysage et que, en ajustant notre regard, nous discernons des fissures dans cette forteresse prétendument impénétrable.* »

L'alternative ne reposera pas sur la reproduction du modèle américain, mais sur l'affirmation d'un nouveau modèle. « *Rappelons toutefois que remplacer un monopole américain, adversaire assumé de la démocratie, par son équivalent français, n'améliorerait ni la situation démocratique ni la liberté du marché. Autrement dit, si l'intégration nationale peut parfois représenter une solution adéquate, il est essentiel de maintenir des positions fermes en matière de régulation des monopoles.* ***Il ne suffit pas de changer la nationalité du tyran*** », souligne M. Henri Verdier.

**Un monde numérique ouvert**. La dépendance critique à des fournisseurs crée des vulnérabilités systémiques. L'alternative réside dans la création d'un écosystème technique et réglementaire qui permette à de nombreux acteurs de développer leurs solutions librement. Aucun d'entre eux ne doit maîtriser les conditions de développement des autres ni avoir un poids qui lui permette d'imposer ses produits. Dans la mise en œuvre technique, nous sommes confrontés à deux défis. Le premier est la conciliation entre la nécessité de disposer d'une multitude de solutions disponibles qui communiquent entre elles et le bénéfice des effets de réseau (plus les utilisateurs d'une solution sont nombreux, plus la valeur tirée des infrastructures numériques est importante). Le second est de créer les conditions économiques de la pérennité des logiciels libres, fondés sur des solutions open source gratuites.

**Le respect du droit comme principe fondamental et intangible.** L'application du droit européen par les Big Tech n'est plus une question de principe, mais un sujet transactionnel. Combien m'en coûtera-t-il de ne pas respecter la règle ? Combien de temps le régulateur mettra-t-il à sanctionner le déploiement de nouvelles technologies, qui reposent toujours sur les mêmes ingrédients non concurrentiels (ventes groupées, invisibilisation des concurrents, etc.) ? Quel droit vaut-il mieux que j'applique, le droit européen ou celui de mon siège social ?

Le droit est désormais perçu comme l'ennemi, responsable de la faiblesse du secteur numérique européen. Pourtant, au cours de l'ensemble des auditions de

la commission d'enquête, aucun interlocuteur n'a fourni d'exemple concret d'une dérégulation qui favoriserait le développement économique. Ce que nous avons montré, c'est plutôt que les modifications réglementaires en cours d'étude au niveau européen ont été insufflées par les Big Tech qui disposent d'énormes moyens de lobbying. Au regard de l'importance des enjeux, il convient de placer les sujets de la protection des citoyens européens et la structuration d'une industrie numérique européenne au cœur des discussions politiques sur la régulation du numérique.

**Le numérique au service de la connaissance et de l'intérêt public**. Nous avons été formatés pour accepter les produits tels qu'ils sont. L'un des enjeux fondamentaux est d'encourager, dans les entreprises comme dans les administrations et chez l'ensemble des citoyens, une réflexion critique sur les outils que nous acceptons d'utiliser, leurs conséquences sur nos vies privées, nos droits et notre économie. Pour en finir avec la dépendance aux solutions états-uniennes, il faudra proposer des outils et sortir d'une posture passive. Il faut tout d'abord revenir à l'ambition fondatrice d'internet : avoir accès à la connaissance sans limites, sans biais et sans que celle-ci ne fasse l'objet d'un pillage généralisé à des fins lucratives. Ensuite, il faut développer des usages bénéfiques pour la collectivité les citoyens. Dans un monde aux ressources énergétiques finies, comment faire en sorte que la priorité ne soit pas systématiquement donnée aux usages les plus rentables ? Et comment hiérarchiser les différents usages du numérique afin de respecter les objectifs climatiques définis lors des accords de Paris ?

### 2. Écueils et conditions de succès

#### *a. La difficulté d'agir seul dans un contexte européen*

Le cadre juridique est largement défini par le droit européen. C'est le cas des règles transverses applicables aux aides d'État et au droit de la concurrence, mais aussi de l'ensemble des textes sectoriels.

Les difficultés à trouver un consensus entre États membres pour adopter des réglementations ambitieuses ne sont plus à prouver. Chaque pays européen est tenu par son propre réseau d'alliances, dans le domaine de la défense ou du commerce international. Le contexte crée une opportunité, et les récentes décisions du gouvernement américain ont pu faire évoluer les consciences. Mais, comme l'a montré notre discussion avec des représentants de la Commission européenne, l'idée que les États-Unis sont un allié indéfectible de l'Union européenne perdure.

Quelle position adopter ? Selon les sujets et les circonstances, trois options sont possibles :

– adopter un modèle qui puisse entrer en résonnance avec les objectifs poursuivis par d'autres États membres, pour trouver des alliés de circonstance, voire impulser des changements par le bas, grâce à des collaborations techniques et financières sur des sujets définis ;

– assumer la défense de notre modèle lorsque cela le requiert, dans un affrontement direct avec la Commission européenne et les autres États membres à l'occasion des négociations sur les textes ;

– créer des leviers de pression, en travaillant sur nos forces : un écosystème attractif pour l'ensemble des acteurs numériques européens, un système énergétique robuste, une avance technologique dans certains domaines.

Il faut enfin se servir de l'Union européenne comme d'une force, lorsque notre volonté politique est alignée avec elle. L'open source est désormais au cœur de la stratégie de souveraineté politique européenne (1), ce qui est un gage d'accélération des dynamiques que nous souhaitons engager.

### *b. Le défi de créer une dynamique profonde, à même d'amorcer un véritable changement de modèle*

Alors même que nous ne maîtrisons qu'une partie de l'équation, retrouver notre destin numérique nécessite d'enclencher des changements radicaux. Cela ne pourra se réaliser qu'à trois conditions.

La première est de coordonner le déploiement des efforts de la sphère publique et des entreprises privées. L'État dispose d'un levier particulier avec les administrations, mais ces dernières ne représentent qu'une part minoritaire des dépenses en matière de numérique. L'objectif n'est pas de créer des solutions pour la sphère publique qui ne soient pas adoptées par les entreprises et les citoyens. Nous réunirions alors tous les ingrédients de l'échec industriel. Les propositions du rapport visent donc à mettre en cohérence les évolutions des systèmes d'information de l'État, le soutien public aux entreprises innovantes et la diffusion des progrès technologiques dans les entreprises, grâce à un cadre technique commun.

La deuxième est de définir un cap avec un horizon de temps long, le seul à même d'enclencher une véritable dynamique. Les résultats ne pourront être au rendez-vous qu'à la condition d'une constance dans la politique menée, donc d'une imperméabilité aux changements de majorité politique. Il convient donc de créer un véritable consensus sur les solutions à mettre en œuvre, au-delà des clivages partisans. Les arbitrages budgétaires de l'État devront également être constants pour produire des effets dans la durée. Enfin, pour accepter de réorienter leurs priorités, leurs pratiques et leurs activités, les acteurs économiques devront disposer d'une visibilité dans la durée.

La troisième condition de succès est de placer au premier rang des priorités l'intérêt général, dont l'État serait le garant. Les dix dernières années ont été celles d'un soutien sans conditions aux 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 :

---

*(1) https://digital-strf ategy.ec.europa.eu/en/policies/open-source-strategy*

reconquérir la maîtrise de nos outils, faire respecter le droit et soutenir le développement d'un écosystème économique pérenne et diversifié.

Plusieurs leviers devront être activés conjointement pour former une politique d'ensemble cohérente. La rapporteure a formulé un ensemble de propositions destinées à amorcer un véritable changement de modèle.

## B. LES LEVIERS

### LEVIER N°1 : LES COMMUNS NUMÉRIQUES

#### 1. Pour une France du Libre et de l'Open Source

- *Les enseignements de la commission d'enquête*

Il est possible de créer des alternatives aux logiciels propriétaires à partir de briques open source, comme l'ont montré les expériences réussies de la Dinum, de la DGFIP, de la gendarmerie nationale ou de la commune d'Echirolles. De nombreux outils d'ores et déjà utilisés au sein des administrations reposent sur des logiciels libres, qui ont fait la preuve de leur robustesse et de leur utilité.

Les logiciels libres pouvant être utilisés, étudiés, modifiés et partagés sans restriction, ils présentent plusieurs avantages : ils permettent de réduire les coûts ; assurent une plus grande maîtrise interne ; bénéficient des améliorations de l'ensemble de la communauté ; et s'adaptent aux besoins de l'organisation qui les déploie. Ils sont généralement développés et maintenus par des communautés de développeurs, bénévoles et professionnels, qui veillent à l'identification de failles et livrent régulièrement des mises à jour, ce qui favorise leur performance et un niveau élevé de sécurité. Ils apportent, enfin, une capacité accrue de mutualisation, puisque les briques *open source* peuvent également être utilisées par le secteur privé.

Pour que les logiciels libres puissent constituer un véritable levier d'indépendance, il est impératif de garantir leur pérennité et de porter une attention particulière à leur gouvernance, en contribuant activement à leur développement, à leur maintenance et à leur financement. Il convient notamment de veiller au maintien des solutions libres déjà utilisées au sein des administrations et à l'identification des briques *open source* essentielles de l'ensemble de la stack technologique.

- *Les modalités proposées*

La France devrait renforcer son soutien politique et financier à l'Edic Digital Commons, qui vise à structurer la coopération entre les États membres autour de la construction de communs numériques souverains. Créé à la fin de l'année 2025 à l'initiative de la France, de l'Allemagne, des Pays-Bas, de l'Italie et

du Luxembourg, l'Edic a suscité un fort effet d'entraînement, avec l'adhésion de sept membres observateurs – la Roumanie, la Pologne, la Hongrie, le Danemark, l'Autriche, la Finlande et la Flandre.

Il conviendra, en priorité, de contribuer financièrement à l'expérimentation d'un *Sovereign Tech Fund* européen, destiné à soutenir la production et la maintenance des briques ouvertes essentielles de bas niveau, sur le modèle du *Sovereign Tech Fund* allemand.

Le fonds pourra notamment contractualiser avec des acteurs privés, lucratifs ou non lucratifs, pour la réalisation de projets contribuant aux communs, salarier des développeurs pour assurer la maintenance de briques *open source*, à temps plein ou à temps partiel, ou soutenir la formation ou le recrutement dans le domaine du logiciel libre.

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

Dans ce cadre, contribuer à la mise en place d'un *Sovereign Tech Fund* européen qui financera la production et la maintenance des briques de bas niveau open source essentielles.

Au niveau national, la rapporteure préconise de créer une fondation France Libre Open Source (FLOS) qui assurera le développement et la maintenance des briques *open source* indispensables aux produits numériques déployés par l'État ou les collectivités locales (La Suite, data.gouv, La Suite territoriale, demarche.numérique.gouv.fr) afin de garantir leur pérennité. L'hébergement au sein d'une fondation préservera ainsi ces outils d'un éventuel changement de la politique numérique de l'État, ou de discontinuités dans la maintenance des solutions.

Le choix de la forme juridique d'une fondation se justifie par la volonté d'assurer une gouvernance collective et représentative de la diversité des parties prenantes – l'État, les collectivités, et le secteur privé lucratif et non lucratif – et d'élargir et animer la communauté des contributeurs. Elle favorisera leur coordination par l'identification partagée des solutions les plus critiques, tout en empêchant qu'un seul acteur prenne le contrôle sur un actif numérique essentiel.

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

La gouvernance sera représentative de la diversité des contributeurs aux briques hébergées, associant la sphère publique et la sphère privée.

La fondation se verra confier la gestion d'un fonds pour le libre, l'open source et la garantie de l'indépendance des communs (Logic). Elle travaillera en relation étroite avec le *Sovereign Tech Fund européen*, permettant à la France de

renforcer son engagement sur les segments ou les solutions qui constituent pour elles des priorités, tout en préservant l'ambition d'une mutualisation européenne.

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

Le fonds sera géré par la fondation France libre open source (Flos) et financé par la Caisse des dépôts et la Banque publique d'investissement.

- *Les effets attendus*

La France doit se positionner comme l'un des moteurs du logiciel libre en Europe. À cet égard, la fondation Flos constituera un point de convergence pour l'ensemble des acteurs utilisant des briques *open source* et créera de l'émulation au sein de la communauté grâce à une gouvernance transparente et collective. Le fait de disposer d'un organe de pilotage et de partage garantira la rationalisation des efforts et la qualité des contributions au code ouvert. L'Edic *Digital Commons* jouera le même rôle structurant au niveau européen.

La disponibilité des briques communes, avec de fortes garanties de sécurité et de pérennité, devrait catalyser la croissance de l'ensemble de l'écosystème numérique.

Les éditeurs de logiciels trouveront toute leur place dans cette dynamique. Ils pourront déployer leurs activités sur la base de ces infrastructures communes, en proposant les services d'intégration et d'implémentation de fonctionnalités supplémentaires attendues par leurs clients.

Enfin, le soutien public aux logiciels libres sera en pleine adéquation avec le principe selon lequel les capitaux publics doivent contribuer à financer du commun, accessible à tous.

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

À la suite de la recommandation du Conseil de l'intelligence artificielle et du numérique (CIANum), le gouvernement devra étudier la transposition des fiducies de données tant sur le plan juridique, qu'opérationnel, dans l'objectif d'inscrire dans la loi le statut de syndicat de données. Ces syndicats seront le support de la création d'outils de mutualisations des données d'intérêt général (données culturelles, environnementales, territoriales). Ils auront pour vocation de faire respecter les licences attachées à ces données et notamment de limiter leur usage dans un objectif privatif, en garantissant la réciprocité et la redistribution de la valeur auprès des communautés d'origine des données.

Les syndicats représenteront les titulaires de droits, producteurs de données et sujets de données. Ils pourront en leur nom engager des recours en justice relatifs au non-respect des licences libres ou des conditions de réutilisation des données.

Les syndicats des données seront encadrés par le Data Governance Act, dont le chapitre III est consacré intégralement aux « services d'intermédiation de données ». L'article 12 prévoit notamment les conditions d'indépendance et de neutralité qui leur sont applicables. Les syndicats de données, serviront de cadre au développement d'outils numériques respectant les règles du droit d'auteur ou encore la vie privée des personnes.

### 2. Le logiciel libre : pilier de l'éducation au numérique

#### *a. Généraliser l'usage des logiciels libres à l'école*

- *Les enseignements de la commission d'enquête*

Google et Microsoft ont mis en œuvre une stratégie de pénétration dans les établissements scolaires, en proposant aux enseignants, aux élèves et aux étudiants un accès gratuit, ou à moindre coût, à leurs outils bureautiques. Ces pratiques commerciales déloyales, qui visent à enfermer les citoyens dès le plus jeune âge dans leur écosystème propriétaire, constituent un frein au déploiement ultérieur de solutions souveraines.

La doctrine Cloud au centre conduit à interdire dans les établissements scolaires l'utilisation des suites bureautiques en ligne d'éditeurs non-européens en raison des risques en termes de protection des données, comme l'a rappelé le ministre de l'éducation nationale dans un courrier adressé aux recteurs le 28 février 2026.

En dehors de cet usage spécifique, les solutions américaines demeurent très utilisées en milieu scolaire. 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 [(1)], 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.

- *Les modalités proposées*

La rapporteure appelle à généraliser les logiciels libres à l'école, à travers deux leviers principaux : une bascule des équipements informatiques sur le libre ; et l'évolution des programmes scolaires.

---

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

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

Exiger que les collectivités locales équipent les établissements scolaires, les membres de la communauté éducative, et le cas échéant les élèves, exclusivement avec des postes de travail dotés de logiciels libres à l'horizon 2030. L'État accompagnera la transition et prendra en charge les éventuels surcoûts.

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

De façon générale, l'apprentissage du numérique à l'école doit permettre aux élèves de construire un rapport réflexif et responsable à l'égard du numérique par une compréhension fine du fonctionnement et des limites de ces différentes technologies. Les élèves apprendront à utiliser plusieurs outils libres et open source. L'enseignement devra également favoriser l'exercice de l'esprit critique et l'ouverture par l'utilisation des méthodes de l'informatique débranché, la présentation de l'impact environnemental du numérique, et l'apprentissage des limites de l'intelligence artificielle générative.

La communauté éducative devra être pleinement impliquée dans cette dynamique, grâce à la montée en puissance de la politique du ministère de l'éducation en faveur du développement des communs numériques éducatifs et de la formation à leur usage, comme on l'a vu dans le chapitre 13.

- *Les effets attendus*

Une utilisation précoce des logiciels libres et un enseignement de leur fonctionnement doivent permettre de cultiver un rapport plus actif à l'égard du numérique et d'enrayer les stratégies d'acculturation développées par les Gafam. Il s'agit d'un champ d'action prioritaire pour entraîner un changement d'usage global au sein de la société.

### *b. La préservation du patrimoine numérique et la diffusion de la culture sur l'informatique*

- *Les enseignements de la commission d'enquête*

En examinant nos dépendances et nos vulnérabilités, la commission a mis au jour la place centrale qu'occupe désormais le numérique dans l'ensemble de la société. Pourtant, il continue d'être considéré comme une infrastructure invisible par la très grande majorité des citoyens.

- *Les modalités proposées*

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

Le code fait aujourd'hui partie du patrimoine commun de l'humanité. Les codes sources sont le support de grandes avancées technologiques et scientifiques. Ils méritent à ce titre d'être conservés :

– pour pouvoir être étudiés et réutilisés, notamment dans un objectif de diffusion de la connaissance contenue dans les codes sources ; la préservation des codes sources permettrait notamment de conserver des codes qui ne sont plus mis à jour par leur créateur ;

– pour soutenir l'innovation grâce à l'accès égal pour tous et le droit de réutilisation par tous d'un code anciennement propriétaire qui n'est plus utilisé ;

– pour pouvoir être étudiés comme objets scientifiques en soi. Aux États-Unis est ainsi né un champ d'étude appelé « *Critical code studies* », destiné à replacer le code informatique dans son contexte socio-économique et culturel ; le développement de travaux universitaires sur le sujet sera d'autant plus important dans un contexte de développement de l'intelligence artificielle, qui rend absolument nécessaire la compréhension des biais et des valeurs induites par les modèles et leurs données d'entraînement.

L'État devrait renforcer son soutien à la Software Heritage Foundation, actuellement hébergée par l'Inria (Institut national de recherche en sciences et technologies du numérique), qui collecte et préserve le code source des logiciels afin de la rendre plus indépendante des financeurs privés.

**Proposition n° 8 : Créer un musée du numérique.**

Sur le modèle du Heinz Nixdorf MuseumsForum allemand, il est proposé de créer un musée de l'informatique et du code, qui aurait pour objectif de replacer les technologies informatiques actuelles dans l'histoire de leur développement et d'organiser des manifestations et expositions sur les enjeux du numérique.

### LEVIER N°2 : COMMANDE PUBLIQUE ET COMMANDE PRIVÉE AU SERVICE D'UNE FILIÈRE D'EXCELLENCE FRANÇAISE, L'OPEN SOURCE

Les auditions ont montré qu'un vecteur important pour soutenir l'écosystème français du cloud et du logiciel est l'achat public ou privé. Les propositions de la rapporteure visent à orienter commande publique et commande privée vers un même socle technique dans une logique de constitution d'une véritable filière d'excellence française, le logiciel libre.

Il est indispensable de rappeler que la monoculture dans le domaine du numérique constitue un des facteurs de risque. Loin de la représentation commune, le fait de ne pas utiliser seulement la solution standard peut être une manière de renforcer sa sécurité.

### 1. La commande publique

#### *a. Administrations d'État*

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

- *Les enseignements de la commission d'enquête*

La commission a mis en exergue des taux d'externalisation particulièrement inquiétants dans certaines administrations, en particulier 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.

La commission e constate également que les deux administrations les plus en pointe en matière de déploiement d'alternative aux Big Tech -– la gendarmerie nationale (de façon totale) et la DGFIP (de façon partielle) – ont la particularité d'être dotées de compétences et d'effectifs importants dans le domaine des systèmes d'information, permettant de maîtriser les développements et l'intégration de briques open source.

- *Les modalités proposées*

Il est proposé de doter les administrations d'effectifs supplémentaires dans les systèmes d'information, conformément aux recommandations du rapport de l'IGF et du CGE de janvier 2023 sur les ressources humaines de l'État dans le numérique. La mise en œuvre de solutions open source en substitution des solutions propriétaires comme les produits de Microsoft, Oracle et VM Ware, requiert des compétences supplémentaires, en termes d'architecture, d'intégration, de développement et de veille des technologies du marché.

Les ministères disposant actuellement du taux d'externalisation le plus élevé, au premier rang desquels le ministère de la justice, devront être tout particulièrement accompagnés par la Dinum sur leur feuille de route, la stratégie d'embauche et la formation des équipes.

- *Les effets attendus*

La réinternalisation aura trois avantages décisifs :

– la réalisation d'économies budgétaires très importantes. Le rapport a chiffré les coûts de licences évitables grâce à l'utilisation de solutions open source à 1 milliard d'euros par an. Ces économies s'ajouteront à celles liées à la réduction du recours aux prestataires externes, dont l'IGF a montré qu'elle entraînait un surcoût de 20 % par rapport au recrutement d'agents publics disposant des mêmes compétences ;

– pour les solutions demeurant externalisées, elle permettra à l'État de « mieux acheter », grâce à une meilleure maîtrise technique ;

– la réduction de la dépendance aux solutions propriétaires, qui entraîne des vulnérabilités stratégiques (risque de *kill switch*) et économiques (hausses brutales des tarifs) ;

– de manière générale, la sécurisation et la meilleure maîtrise globale du SI des administrations, dans un contexte d'évolution extrêmement rapide des technologies sous l'influence de la diffusion des modèles d'IA.

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

- *Les enseignements de la commission d'enquête*

Les travaux de la commission d'enquête ont montré que la majorité des logiciels supports utilisés par les administrations sont fournis par des acteurs extra-européens, sur la base de solutions propriétaires. Ces choix entraînent une dépendance, et de ce fait, une vulnérabilité à des hausses tarifaires, à l'occasion de la mise à jour des produits, etc.

Pourtant, les solutions techniques de substitution aux briques logicielles les plus répandues existent. Elles ont été mises en œuvre dans plusieurs administrations, en particulier la gendarmerie nationale (de façon totale) et la DGFIP (de façon partielle). Ces deux administrations présentent la particularité d'être dotées de compétences et d'effectifs importants, permettant de maîtriser les développements et l'intégration de briques open source.

Les conséquences en termes de finances publiques sont importantes. La commission d'enquête a montré ainsi que les dépenses de licences en logiciels substituables sont de 1 milliard d'euros sur le périmètre des administrations d'État sollicitées.

La commission d'enquête a également montré que le lien entre l'État acheteur et la filière n'était pas suffisant, ces derniers ne disposant pas de la feuille de route des besoins des administrations pour les prochaines années.

En somme, il s'agit de refonder le contrat de filière entre l'État et les acteurs français du logiciel. Les administrations devront désormais acheter du logiciel européen et s'engageront à travailler étroitement avec les acteurs français et européens pour leur expliciter leurs besoins en avance de phase. En contrepartie, le critère de l'open source devra s'imposer comme une règle, garantie de la maîtrise par l'État des solutions sur lesquelles il s'appuie.

- *Les modalités proposées*

Il est proposé de renforcer l'article 16 de la loi pour une République numérique en passant d'une logique d'encouragement à une logique contraignante. L'open source dans les marchés de logiciels pour les administrations et les entreprises publiques d'État doit être rendu obligatoire à partir du 1er janvier 2030.

L'entrée en application en 2030 de l'obligation permettra de préparer les administrations et l'écosystème à sa mise en œuvre.

Le périmètre des entités soumises à cette obligation devra également être défini pour répondre efficacement aux objectifs poursuivis. Seront visées prioritairement les administrations, opérateurs, entreprises publiques chargées d'une mission de service public critique, tout comme les entités privées chargées de l'exploitation d'un service public essentiel par le biais d'une concession. L'obligation pourra ensuite être étendue à l'ensemble des opérateurs de l'État.

Cette condition s'appliquera également aux outils d'intelligence artificielle, pour lesquels le recours aux solutions propriétaires sera interdit.

- *Les conditions de succès*

Le respect d'une telle obligation repose sur la mise en œuvre d'un plan ambitieux de la part du gouvernement pour :

– **identifier les dépendances actuelles aux logiciels propriétaires et les principales évolutions du SI dans les prochaines années**. Comme la commission d'enquête a pu le constater, le recensement des solutions informatiques utilisées par les administrations n'en est qu'à ses débuts, et les outils de pilotage sont encore lacunaires. L'élaboration d'un plan de basculement vers l'open source sera l'occasion d'une mise à jour complète de l'état des lieux initial ;

– **doter les administrations d'effectifs supplémentaires ;**

– enfin, il conviendra de **préparer l'écosystème au tournant de l'open source.** Avec un volume d'activité de 5,9 milliards d'euros, l'open source ne représentait que 11 % du marché du numérique français. Afin de disposer d'une

offre suffisante lorsque l'obligation entrera en vigueur, les fournisseurs de solution devront être informés suffisamment en amont des besoins des donneurs d'ordre publics.

- *Les effets attendus*

Les effets attendus d'une telle mesure sont de deux ordres :

– suppression des dépendances et vulnérabilités à des logiciels propriétaires. Alors que le sujet a été délaissé pendant de nombreuses années, le contexte géopolitique rend nécessaire la réalisation d'un effort massif dans un intervalle de temps très court. Il s'agit d'une obligation pour assurer l'indépendance de la France aux pressions internationales ;

– suppression des dépenses de licences : les travaux préparatoires permettront de disposer d'un chiffrage des économies attendues d'une généralisation de l'open source dans les administrations.

- *Deux mesures immédiates*

**Proposition n° 11 : Intégrer une clause d'entiercement (escrow) (1) lors de la contractualisation d'une structure publique avec un fournisseur afin de garantir la continuité de service.**

Cette mesure, déjà mise en place de façon courante dans le secteur privé, permet de garantir à une administration l'accès aux éléments indispensables à la continuité de service (logiciel, base de données, documentation technique, etc.) en cas de défaillance du fournisseur.

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

Les administrations disposent d'ores et déjà de référentiels pour l'achat de logiciels répondant aux standards d'interopérabilité et de solutions d'IA responsables. La rapporteure souhaite imposer le respect de ces prescriptions dans les marchés publics.

*(1) « L'entiercement est un concept anglo-saxon (escrow agreement) qui consiste, pour le fournisseur d'un produit ou d'un service, à confier à un tiers séquestre des éléments essentiels (logiciels, bases de données, documents, etc.) à l'usage de ce produit ou à la réalisation de ce service. L'objectif est d'assurer à un tiers (client, partenaire, etc.) la possibilité d'y accéder, selon les dispositions prévues entre les parties, et notamment en cas de défaillance du fournisseur ». Source : https://www.app.asso.fr/nos-solutions/escrow-agreement*

### *b. Collectivités territoriales*

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

- *Les enseignements de la commission d'enquête*

La commission d'enquête a choisi de ne pas traiter le sujet des dépendances des collectivités territoriales aux logiciels extra-européens.

Toutefois, les éléments collectés lors des auditions confirment que le problème se pose dans les mêmes termes pour les collectivités territoriales que pour les administrations d'État :

– les achats de logiciels américains sont très significatifs ;

– les mêmes dépendances techniques aux logiciels comme ceux de Microsoft, VMWare ou encore Oracle sont identifiées, et les mêmes solutions de substitution existent, basées sur des logiciels libres ;

– un levier important réside dans le développement des compétences pour basculer vers les produits open source, dont l'intégration au sein des systèmes d'information ;

– un frein identifié, spécifique aux collectivités territoriales, est celui des règles de la comptabilité publique. Les prestations d'aide à l'installation, de formation et d'accompagnement des utilisateurs sont aujourd'hui considérées comme une dépense de fonctionnement, ce qui ne constitue pas un cadre favorable pour les collectivités.

- *Les modalités proposées*

L'ensemble des dépenses d'exploitation visant à déployer du logiciel open source (y compris la formation des personnels) pourront être comptabilisées comme des dépenses d'investissement, de même que :

– l'ensemble des dépenses, y compris de formation, liées à l'hébergement souverain de données *on premise* ou d'IaaS ;

– les solutions d'IA répondant à la définition de l'OSAID 1.0.

- *Les effets attendus*

Les effets attendus sont du même ordre que pour les administrations d'État. L'extension aux collectivités territoriales a un double intérêt : améliorer la résilience et la robustesse des collectivités dans le domaine du numérique et accroître l'effet de levier de la commande publique sur le soutien à l'écosystème privé.

### *c. Une communication publique exemplaire*

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

- *Les enseignements de la commission d'enquête*

Des travaux précédents, comme la commission d'enquête sur les effets psychologiques de Tiktok, avaient étudié dans le détail les effets des réseaux sociaux sur la santé. Bien que cela n'ait pas constitué un axe prioritaire de la commission d'enquête, plusieurs auditions ont confirmé les analyses existantes sur la nocivité des réseaux sociaux de type X, qui biaisent la diffusion des publications en faveur des contenus toxiques et sont capables de changer l'issue d'une élection en influençant les décisions de vote.

La commission d'enquête a approfondi la problématique de l'interopérabilité, ou plutôt de son absence chez les grandes plateformes numériques. En gardant la « propriété » de leurs abonnés, ces dernières maximisent la commercialisation des données personnelles et s'assurent qu'aucune alternative n'émerge. Le DSA a pour objet d'introduire des mécanismes de régulation des *gate keepers*, les plateformes qui touchent tous les Européens. Mais dans l'attente de la confirmation de son apport réel, pourquoi l'État continue-t-il à communiquer sur des plateformes dont l'effet nocif est avéré et qui ne jouent pas le jeu de la modération et de l'interopérabilité ? Comment convaincre des utilisateurs de choisir les acteurs respectant les règles alors que tous les ministères font de X leur premier canal de communication ?

- *Les modalités proposées*

Toutes les institutions publiques, à commencer par le gouvernement et la présidence de la République, doivent quitter le réseau X et s'astreindre à communiquer uniquement sur des réseaux sociaux interopérables et décentralisés.

C'est ce mouvement que sont en train de réaliser des administrations homologues dans d'autres pays voisins :

– la Commission européenne a créé une instance Mastodon [(1)] ;

– en Allemagne, les ministères de la défense et des affaires étrangères ont décidé de quitter X en janvier 2025 ; le ministère des affaires étrangères a fait le choix de la plateforme Blue sky [(2)].

– aux Pays Bas, le conseil rassemblant les directeurs de communication des douze ministères a transmis un mémo au cabinet du Premier ministre hollandais, recommandant de fermer les vingt-huit comptes des ministères et secrétariats d'État,

(1) https://ec.social-network.europa.eu/about

(2) https://www.reuters.com/world/europe/german-defence-foreign-ministries-depart-elon-musks-x-2025-01-15/

ainsi que ceux des administrations et de ne conserver des comptes que pour la gestion de crise et le maintien de contacts diplomatiques [1]. Une décision doit être prise après l'été.

- *Les effets attendus*

Grâce à leur position de leaders d'opinion, les institutions publiques pourront inciter les utilisateurs des réseaux sociaux néfastes à les quitter et valoriser des plateformes conformes à nos valeurs.

Pour les administrations, le fait de passer par des réseaux sociaux interopérables est une garantie de mieux maîtriser leur communication et de limiter les risques sur la souveraineté informationnelle que peuvent faire peser des décisions unilatérales des plateformes (fermetures de comptes brutales, usurpations d'identité).

***d. Au niveau européen***

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

- *Les enseignements de la commission d'enquête*

Le marché européen du numérique demeure très ouvert et libre-échangiste, quand la plupart des partenaires de l'Union ont restreint l'accès à leur territoire pour les biens et services étrangers. Le droit de la concurrence et la directive sur les marchés publics limitent la capacité des acheteurs publics à favoriser les acteurs européens, *a fortiori* français, au détriment des entreprises de pays tiers.

La multiplication des coups de boutoir états-uniens contre le droit international, les menaces répétées visant ses alliés, et la coupure brutale de la fourniture du modèle d'intelligence artificielle d'Anthropic, démontrent la nécessité d'une préférence européenne.

- *Les modalités proposées*

Dans le cadre des négociations qui s'ouvrent sur le paquet « souveraineté numérique » présenté le 3 juin 2026 par la Commission européenne, la rapporteure appelle à :

– soutenir l'instauration d'un référentiel européen de souveraineté pour le cloud qui permette un niveau d'exigence d'immunité au droit extra-européen équivalent au référentiel SecNumCloud ; et imposer aux administrations d'y recourir pour leurs usages sensibles, dans le cadre des négociations sur le Cloud and AI Development Act (CADA) [2] ;

---

*(1) https://nltimes.nl/2026/05/26/top-civil-servants-urge-dutch-govt-abandon-social-media-platform-x*

*(2) https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada*

– défendre l'extension de la préférence européenne au segment des logiciels, dans un objectif de réduction des dépendances et de sécurisation des approvisionnements, notamment à l'occasion de la révision de la directive sur les marchés publics et de la discussion du prochain cadre financier pluriannuel.

- *Conditions de succès*

Pour que la préférence européenne soit mise en œuvre, elle doit s'appuyer sur des critères clairs. Le sommet franco-allemand qui s'est tenu en novembre 2025 a permis de lancer des travaux pour parvenir à une définition commune de service numérique européen. Face aux tentatives de *sovereignty washing* qui ne manqueront pas, la rapporteure appelle à défendre une approche exigeante, en veillant à ce que la localisation du siège et la structure de l'actionnariat soient bien européens, qu'il y ait un nombre important de salariés en Europe et que l'essentiel de la valeur ajoutée soit réalisée sur le sol continental.

### 2. La commande privée

La commande publique ne représentant qu'une part minoritaire des achats dans le domaine du numérique en France, la commande privée est un levier indispensable du changement et doit donc être actionnée pour favoriser le développement d'une offre française de logiciel et de cloud.

La rapporteure souligne la nécessité pour toutes les entreprises, et notamment les plus grandes d'entre elles, de mettre en place un dispositif d'évaluation des risques, comme l'indice de résilience numérique. Elle souhaite également rappeler l'importance de la commande des grandes entreprises dans la consolidation de la filière numérique.

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

- *Les enseignements de la commission d'enquête*

La commission d'enquête a montré que la vulnérabilité aux solutions étrangères est un sujet d'inquiétude croissante au sein des entreprises.

La rapporteure propose d'accompagner les PME, dont les systèmes d'information sont de taille plus réduite et les services dédiés au système d'information moins dotés en expertise que les ETI ou les grandes entreprises.

- *Les modalités proposées*

Il est proposé d'instaurer un dispositif de soutien Open source, destiné aux entreprises de moins de 250 salariés [(1)]. Sur le modèle du crédit d'impôt innovation, il permettrait à ces dernières de déduire de leur impôt sur les sociétés les dépenses de digitalisation.

Les dépenses éligibles couvriraient les dépenses d'intégration de solutions open source et les dépenses de formation et d'accompagnement des utilisateurs, ainsi que les dépenses relatives à l'auto-hébergement des serveurs ou à la contractualisation avec un opérateur européen, garant de l'immunité aux lois extraterritoriales, pour les cinq premières années. Pourraient également être intégrées les dépenses de déploiement d'outils IA respectant la définition de l'OSAID 1.0 hébergées sur des clouds souverains.

- *Les effets attendus*

L'objectif est de contribuer au soutien de la filière française du numérique via un soutien fort à l'open source. Le crédit d'impôt, s'il est maintenu durant une période assez longue, permettra de donner une visibilité à la filière suffisante pour amorcer un véritable tournant vers les solutions libres et pour recruter les ressources nécessaires.

L'étude de la Commission européenne sur l'impact économique de l'open source a démontré que le soutien de cette filière pourrait avoir des effets importants sur la croissance et la création d'entreprises.

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

- *Les enseignements de la commission d'enquête*

Les travaux de la commission d'enquête ont fait ressortir trois problèmes liés à l'utilisation des solutions de cloud fournies par les *hyperscalers* :

– la vulnérabilité des données aux lois extraterritoriales ;

– la dépendance aux technologies fournies, qui rendent un client des solutions hybrides comme Bleu ou Sens vulnérable au *kill switch*, c'est-à-dire à l'absence de mise à jour du fournisseur principal de technologies ;

– les pratiques commerciales tendant à enfermer les clients dans des architectures propriétaires, qui rendent difficiles la portabilité et le multi-cloud, et à favoriser des pratiques de vente couplée.

*(1) Une PME est une entreprise employant moins de 250 salariés, réalisant soit un chiffre d'affaires annuel inférieur à 50 millions d'euros, soit un total de bilan inférieur à 43 millions d'euros. Un dépassement de seuil n'a d'effet qu'après 2 exercices consécutifs.*

Le référentiel SecNumCloud constitue une solution, mais n'est pas adapté à toutes les situations.

La commission a également pu constater la sensibilité particulière des données de santé et l'attachement des Français à ce que ces données soient protégées.

- *Les modalités proposées*

Face à ce constat, la rapporteure appelle à l'intégration d'une clause de souveraineté dans la certification Hébergeur de données de santé. Ainsi cette certification ne pourrait être attribuée qu'à un acteur dont la majorité du capital serait détenue par des acteurs européens, hébergeant et traitant ces données sur le sol européen.

- *Les effets attendus*

Cette mesure vise à protéger des données particulièrement sensibles, et à éviter que le stockage de ces dernières soit effectué par des acteurs soumis à un droit extraterritorial. Elle doit également permettre de se prémunir contre le risque de *kill switch*, dont les conséquences seraient particulièrement critiques dans le domaine de la santé.

S'agissant des domaines autres que la santé, la rapporteure considère qu'il n'est pas nécessaire d'édicter un référentiel spécifique, compte tenu des discussions actuelles sur la mise en œuvre d'un référentiel européen qui prenne en compte les exigences de souveraineté dans la proposition de règlement CADA.

### LEVIER N° 3 : L'ARSENAL DE SOUVERAINETÉ

Les mesures proposées précédemment ont pour but d'impulser une véritable dynamique dans la filière du logiciel et du cloud en France. Un tel soutien doit s'accompagner de conditionnalités fortes pour s'assurer de la bonne utilisation du crédit d'impôt et du maintien durable en France des PME soutenues.

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

- *Les enseignements de la commission d'enquête*

Le financement des entreprises innovantes par l'amorçage est salué de façon unanime par l'ensemble des acteurs. S'agissant des subventions, BPIFrance indiquait ainsi que les aides à l'innovation relatives au numérique avaient représenté 1,1 milliard d'euros en 2025.

Les subventions et avances remboursables sont un levier de développement important pour les entreprises naissantes car elles leur permettent de disposer de

financements gratuits, sans procéder à des levées de fonds qui peuvent avoir pour effet de diluer la détention du capital par les fondateurs.

Pourtant, au terme du processus, rien n'oblige les entreprises qui réussissent à conserver leurs activités et leur siège social en France.

- *Les modalités proposées*

Comme l'a proposé le président Philippe Latombe, lors de l'examen du projet de loi de finances pour 2026, une entreprise du secteur du numérique financée par le biais de subventions et ayant bénéficié du crédit impôt recherche, devra rembourser les sommes perçues en cas de vente à un acteur extra-européen.

- *Les effets attendus*

L'État accepte une part de risque dans le financement des entreprises innovantes. Du fait de son rôle d'amorçage, très en amont, il subventionne nécessairement un nombre important d'entreprises et de projets qui ne parviennent pas à la viabilité commerciale. En revanche, lorsque des entreprises se développent, cela ne doit pas se faire au détriment de l'intérêt public.

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

- *Les enseignements de la commission d'enquête*

Le Premier ministre a annoncé, le 16 juin 2026, le remplacement du logiciel d'analyse de données de Palantir utilisé par la DGSI depuis 2015 par l'offre de la société française Chapsvision. En parallèle, le ministre de l'action et des comptes publics prévoit la généralisation pour un million d'agents de la fonction publique d'un assistant conversationnel fondé sur les modèles de Mistral AI. Ces systèmes sont également déployés par le ministère des armées et des entreprises stratégiques telles que CMA CGM ou Airbus.

Il n'existe cependant aucune garantie que ces entreprises demeurent françaises à moyen terme. Des fonds américains sont déjà présents au capital de Mistral AI, et le directeur général de ChapsVision a cédé une précédente société au fonds américain BlackRock [(1)].

Le devenir d'actifs devenus stratégiques en quelques mois, parce que l'État leur a concédé des contrats stratégiques, est entre les mains des investisseurs dont les intérêts ne sont pas alignés avec ceux de la puissance publique. Ces investisseurs n'ont, par nature, qu'un seul objectif : la performance de leur portefeuille boursier à l'occasion d'une future levée de fonds.

*(1) Olivier Pinaud, « ChapsVision, société française, remplace Palantir à la DGSI, un choix de souveraineté au long cours et complexe », Le Monde, 17 juin 2026*

- *Les modalités proposées*

L'État doit renforcer son pouvoir de contrôle. Il est proposé que l'État ait recours à des actions spécifiques, ou *golden shares*, au sein de ChapsVision ou de Mistral.

Ces actions spécifiques, prévues par l'article 31-1 de l'ordonnance du 20 août 2014, confèrent à l'État des droits préférentiels indépendamment de la quotité de capital qu'il détient : un droit d'agrément sur les franchissements de seuils de détention du capital ou des droits de vote ; un droit d'opposition sur les décisions de cession, d'apport ou de transmission d'actifs stratégiques de la société, ou la modification de leurs conditions d'exploitation, si elles sont de nature à porter atteinte aux intérêts essentiels du pays ; un droit d'information renforcé sur les opérations affectant les actifs stratégiques ; et la nomination au conseil d'administration d'un représentant de l'État sans voix délibérative.

- *Les conditions de faisabilité*

Des actions spécifiques peuvent être mises en œuvre par décret en Conseil d'État. L'application du dispositif à Mistral AI et ChapsVision nécessiterait cependant d'actualiser l'ordonnance du 20 août 2014, qui fige le champ des sociétés éligibles à la date du 1er janvier 2018, donc avant la date de création de ces deux entreprises – respectivement en 2023 et 2019.

Ce ne sera pas la première fois que le périmètre des actions spécifiques évolue. En 2019 déjà, le législateur avait considéré que la limitation aux cas de cession de parts d'entreprises publiques au secteur privé conduisait à « *restrein[dre] la capacité de l'État à protéger ses actifs stratégiques, sans pour autant répondre à une contrainte valable* » (1). La loi Pacte (2) a ainsi étendu le dispositif aux sociétés dont l'une des activités est considérée comme stratégique, au sens de l'article L. 151-3 du code monétaire et financier, à la condition qu'elles entrent dans le périmètre de l'Agence des participations de l'État, ou qu'elles soient cotées et que BPIFrance ou ses filiales détienne une participation d'au moins 5 % du capital à la date du 1er janvier 2018.

L'argument avancé pour justifier le gel du périmètre tenait à la nécessité d'assurer la sécurité juridique, notamment à l'égard des investisseurs (3). Ce champ apparaît, à nouveau, en profond décalage avec la réalité stratégique à laquelle la France est confrontée. Ignorant les bouleversements liés à la généralisation des cyberattaques et à l'émergence de l'intelligence artificielle, il empêche de protéger des actifs désormais essentiels pour l'État et dont la compromission présenterait un risque avéré pour l'ordre public et la sécurité nationale.

---

*(1) Exposé des motifs du projet de loi relatif à la croissance et la transformation des entreprises, n° 1088, déposé le mardi 19 juin 2018.*

*(2) Loi du 22 mai 2019 relative à la croissance et la transformation des entreprises.*

*(3) Avis du Conseil d'État du 19 juin 2018 sur le projet de loi relatif à la croissance et la transformation des entreprises.*

Aussi la rapporteure souligne-t-elle l'urgence de mettre à jour le texte, par voie législative. Deux conditions devraient ainsi être supprimées : l'obligation de cotation, l'existence de la société à la date du 1er janvier 2018. Il est, en revanche, proposé de laisser le seuil de 5 % inchangé.

- *Les effets attendus*

La détention de *golden shares* au capital de Mistral AI et de ChapsVision permettra à l'État de disposer d'un droit de veto ciblé à l'encontre des décisions susceptibles de compromettre la souveraineté de la France, notamment dans le cas de l'entrée au capital d'investisseurs étrangers, tout en laissant une large autonomie aux dirigeants dans la définition de la stratégie de l'entreprise.

Elle complétera ainsi utilement le dispositif de contrôle des investissements étrangers en France (IEF). Outre que celui-ci demeure opaque, sans contrôle parlementaire et difficile à appliquer, sa portée est limitée : il n'autorise l'État à bloquer qu'un rachat par des acteurs étrangers, mais pas les autres décisions de l'entreprise sur l'exploitation de ses actifs stratégiques qui risqueraient de porter atteinte aux intérêts essentiels de la Nation. Surtout, dans la réalité, le contrôle de son application par les services de l'État est difficile à réaliser. Une fois l'opération réalisée, la perte de tout levier est définitive.

Les *golden shares* obéissent à une autre logique, en ce qu'elles permettent d'autoriser des prises de participation étrangères tout en garantissant qu'elles ne se traduiront pas par une perte de contrôle. Elles constituent ainsi un outil particulièrement précieux compte tenu des besoins d'investissements importants dans l'IA et du manque de fonds atteignant la taille critique en Europe.

Ce contrôle renforcé pourra être atteint **pour un coût maîtrisé**. Aucune acquisition supplémentaire ne sera nécessaire pour ChapsVision, dont BPIFrance détient déjà une part de capital supérieure à 5 %. S'agissant de Mistral AI, de prochaines levées de fonds pourraient permettre à BPIFrance de porter sa participation actuelle de 2 % aux 5 % requis.

Le risque que l'intervention de l'État entraîne une décote sur la valorisation doit également être relativisé s'agissant d'entreprises dont la croissance repose en grande partie sur la commande publique et dont la visibilité internationale a grandement été accrue par la diplomatie économique française. La confiance de l'État constituera un levier de crédibilité supplémentaire dont elles pourront se prévaloir pour obtenir des marchés dans des secteurs d'activité critiques. Enfin, le dispositif des *golden shares* est encadré par le droit européen en vertu duquel un contrôle de nécessité et de proportionnalité est réalisé. C'est le meilleur gage du respect de l'équilibre entre les droits des actionnaires et l'intérêt général. D'autres mesures, comme des clauses spécifiques du pacte d'actionnaires, ne sont pas aussi transparentes, et dépendent ainsi de négociations *intuitu personae* entre les différents actionnaires.

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

- *Les enseignements de la commission d'enquête*

Le bon fonctionnement de l'État et des services publics est de plus en plus conditionné au bon fonctionnement de services et d'infrastructures numériques. Il est indispensable que l'État puisse garantir la continuité de service, sa sécurité et la souveraineté française.

- *Les modalités proposées*

Il est proposé la création d'une clause de souveraineté devant être intégrée lors de la signature de marchés publics ou de contrats de financement portant sur un service dont le bon fonctionnement est nécessaire à la continuité de l'État et au bon fonctionnement des services publics.

Cette clause de souveraineté finale vise à garantir que des services numériques structurants restent dans un périmètre européen.

Elle stipulerait qu'en cas de changement de contrôle au profit d'une entité dont la direction se situe hors de l'Union européenne, un mécanisme s'appliquerait automatiquement pour préserver le contrôle européen sur les fonctions critiques, sous la forme d'une licence perpétuelle, irrévocable et gratuite au bénéfice de l'État français ou toute autorité qu'il désigne.

Cette mesure organise la mise à disposition des codes développés à l'ensemble des utilisateurs potentiels (open source) ou bien à une tierce partie dans un cadre défini (clause de souveraineté finale). Toute exploitation commerciale concurrente serait exclue et l'activation de la mesure serait motivée par des enjeux de continuité de l'État et des services publics essentiels ainsi que par des enjeux de sécurité.

- *Les effets attendus*

L'État peut financer de manière importante des services ou le fonctionnement d'infrastructures numériques par subvention ou marché public, car ils sont essentiels pour la société ou son activité. Il est alors indispensable que puisse être garantie leur permanence sur le long terme, et ce d'autant plus qu'ils sont largement déployés au sein d'administrations ou d'organisations publiques.

Une vente à un acteur extra-européen pourrait nécessiter de redévelopper ou de faire redévelopper intégralement une solution alternative.

La clause de souveraineté finale est donc une clause de dernier recours, qui permet de garantir la protection de l'intérêt général.

## LEVIER N° 4 : LES INFRASTRUCTURES

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

- *Les enseignements de la commission d'enquête*

Sur la base des demandes de connexion au réseau de transport effectuées auprès de RTE, la commission d'enquête a démontré l'existence de trois phénomènes :

– la spéculation dans le déploiement des data centers en France : plus de 60 % des capacités en développement sont le fait des acteurs du secteur de l'immobilier et des fonds d'investissement ;

– la captation en cours des capacités par les acteurs extra-européens : sur les 39 % restants, représentant un total de 5,8 GW, les acteurs américains représentent plus de la moitié des capacités en développement (3,3 GW, dont 2 GW pour les *hyperscalers*) ;

– l'activité de cloud n'étant pas soumise à la taxe sur les services numériques, les retombées fiscales d'une telle activité ne sont pas assurées.

Les chiffres mentionnés plus haut ne prennent pas en compte les projets supplémentaires annoncés lors du sommet Choose France du mois de juin 2026.

Les tendances actuelles ne répondent à aucun objectif de politique publique :

– les retombées économiques des data centers développés par des investisseurs et industriels étrangers seront limitées ;

– aucune garantie n'est donnée sur le fait que l'utilisation de la capacité de calcul ne soit pas au bénéfice exclusif d'acteurs extra-européens ;

– dans le même temps, les data centers auront des impacts environnementaux importants sur le territoire en termes de pollution et d'artificialisation des sols.

Il apparaît finalement que les autorités nationales et européennes se sont engagées dans un processus d'accélération du déploiement des data centers sans même que les fondements d'une telle politique aient été réellement examinés.

- *Les modalités proposées*

Compte tenu de l'ensemble de ces éléments, il est nécessaire d'instaurer un moratoire sur les projets de data centers développés par des acteurs extra-européens, des fonds d'investissement ou des acteurs immobiliers, ou dont l'utilisation

envisagée n'est pas destinée à des acteurs européens. C'est pourquoi la rapporteure demande à l'État d'examiner l'ensemble des voies et moyens permettant de mettre en œuvre un moratoire dans un laps de temps resserré.

- *Les effets attendus*

Une telle décision sera nécessairement critiquée pour le signal négatif qu'elle enverrait aux investisseurs internationaux et le coup d'arrêt mis au développement de l'intelligence artificielle.

L'examen des conditions dans lesquelles les projets bénéficieraient effectivement à la collectivité, et non aux seuls investisseurs n'a pas été réalisé, témoignant ainsi d'une précipitation irresponsable.

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

- *Les enseignements de la commission d'enquête*

La commission d'enquête a montré que les data centers répondant aux impératifs de souveraineté sont une infrastructure stratégique. Dès lors, le développement des data centers a-t-il vocation à être confié au secteur privé, sans aucune régulation par la puissance publique ?

Aujourd'hui, le déploiement des data centers avec une haute capacité de calcul s'effectue de façon anarchique, sans que la capacité développée ne soit mise en regard des besoins réels. Surtout, les *hyperscalers* sont en position de force pour capter l'essentiel des capacités, y compris celles qui sont développées par des investisseurs généralistes et des fonds d'investissement. En effet, grâce des bilans les plus solides, ces derniers sont capables de signer des contrats de réservation de plusieurs dizaines de milliards d'euros.

- *Les modalités proposées*

La rapporteure demande la mise en place d'un modèle permettant de garantir un contrôle public des investissements dans les data centers pour l'intelligence artificielle.

Le contrôle public aura vocation à garantir que les capacités de calcul sont bien utilisées au service de la collectivité – les entreprises françaises du numérique ou les utilisateurs.

Plusieurs dispositifs peuvent être envisagés :

– un régime d'autorisation permettant de vérifier que le porteur de projet respecte les conditions qualitatives et cumulatives suivantes : immunité aux droits extra-européens, impact environnemental (performance énergétique, faible

consommation d'eau, etc.), obligation d'accès à une diversité de modèles (open source, propriétaire…) et de vocations (recherche, utilité sociale, lucratif…)

– un régime de concession, permettant à l'État de dégager des recettes fiscales par l'intermédiaire de redevances sur l'activité d'inférence ou bien de garantir que les capacités de calcul sont mises à disposition des utilisateurs au meilleur prix pour le consommateur ;

– enfin, la création d'une société d'investissement à capital majoritairement public. Une telle option permettrait d'assurer un contrôle efficace sur le secteur dans la durée. De plus, elle pourrait constituer un investissement profitable pour les citoyens. Enfin, elle contribuerait à diminuer le coût global des investissements en réduisant le coût d'accès au capital, en raison d'une exigence de coût moyen pondéré du capital (*weighted average cost* of capital, WACC) inférieure (accès à une dette proche du risque souverain, possibilité de garantie publique, etc.).

- *Les effets attendus*

Les effets positifs attendus sont nombreux :

– **protection des données vis-à-vis de législations extraterritoriales** ;

**– réservation des capacités pour certains usages**, en particulier la recherche et développement et des activités d'utilité sociale ;

– **limitation des risques de monopole.** Les leaders mondiaux de l'IA ont d'ores et déjà pris une avance en matière de déploiement chez les usagers et de maîtrise des infrastructures. L'existence d'un nombre limité d'acteurs est susceptible d'engendrer des situations dominantes, qui se traduiront ensuite par les pratiques anti-concurrentielles régulièrement constatées.

### LEVIER N° 5 : UTILISER L'ENSEMBLE DES LEVIERS CONFORMES AU DROIT EUROPEEN POUR RENFORCER LE CONTRÔLE DES GRANDES PLATEFORMES SUR NOTRE TERRITOIRE NATIONAL

#### 1. Au niveau européen

- *Les enseignements de la commission d'enquête*

Les États-Unis instrumentalisent la puissance de leurs entreprises numériques et l'hégémonie du dollar pour exercer des pressions ciblées sur des personnalités à des fins politiques et idéologiques. Plusieurs magistrats de la Cour pénale internationale ont ainsi été inscrits sur la liste de sanctions américaines et se sont trouvés privés d'accès à l'ensemble des services numériques et aux moyens de paiement, y compris au sein de l'Union européenne. Certaines sociétés européennes, notamment des établissements bancaires et des compagnies d'assurance, ont également appliqué les sanctions et interrompu la fourniture de leurs services aux

personnes visées, en raison d'une interprétation extensive de la portée des lois extraterritoriales et de la crainte de procédures sur le marché américain.

L'Union européenne a jusqu'ici échoué à protéger ses ressortissants face à ces sanctions pourtant sans fondement en droit européen, en refusant d'activer le règlement de blocage. Ce dernier vise pourtant précisément à lutter contre les pratiques de surconformité en interdisant aux entreprises soumises au droit de l'Union européenne d'appliquer des sanctions illégales de pays tiers.

Au-delà des pressions exercées à l'encontre des individus, l'administration américaine menace l'ensemble de la communauté européenne de représailles pour faire échec à l'application des règles numériques que l'Union européenne a pourtant souverainement adoptées.

- *Les modalités proposées*

Face à ces remises en cause répétées de la souveraineté de l'Union sur son propre territoire, et le risque que de telles sanctions soient demain utilisées pour faire pression sur des magistrats, des défenseurs de droits, et des responsables politiques, la rapporteure propose de mobiliser l'ensemble de l'arsenal juridique mis en place pour lutter contre les tentatives de coercition de pays tiers.

Elle appelle la Commission européenne à activer le règlement de blocage contre les sanctions extraterritoriales ciblant des citoyens européens sans fondement dans le droit européen, à commencer par celles qui visent les magistrats de la Cour pénale internationale. Cela aurait pour conséquence d'annuler les effets des sanctions étrangères sur le territoire européen et d'interdire à toute entreprise européenne de les mettre en œuvre.

À moyen terme, il serait nécessaire de réviser le règlement de blocage pour le rendre véritablement dissuasif en renforçant les sanctions prévues contre les entreprises européennes qui appliqueraient les législations extraterritoriales malgré l'interdiction. En l'état actuel du droit, les États membres sont libres de déterminer les sanctions à imposer. La France pourrait appliquer des sanctions pénales, prévues aux articles L. 542-1 et suivants du code des douanes ; d'autres États n'ont pas prévu de sanctions dissuasives, ce qui affaiblit la portée du règlement au sein de l'Union.

En dernier recours, la rapporteure appelle l'Union européenne à utiliser l'instrument anticoercition. Cet instrument, instauré par le règlement 2023/2675 du 22 novembre 2023 relatif à la protection des intérêts de l'Union européenne et de ses États membres contre la coercition économique exercée par des pays tiers, permet à l'Union européenne de réagir aux tentatives ou menaces de coercition économique de pays tiers qui viseraient à influencer les choix politiques souverains de l'Union ou d'un État membre. Si la coercition est avérée et si la médiation échoue, la Commission européenne peut adopter un éventail de contre-mesures incluant, entre autres, l'augmentation des droits de douane, des restrictions à l'importation ou à l'exportation des marchandises, l'exclusion des marchés publics,

ou la limitation des investissements directs étrangers. La nécessité d'obtenir une majorité qualifiée de 55 % au Conseil limite cependant la capacité de cet instrument à constituer un moyen de dissuasion crédible.

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

Il est, par ailleurs, nécessaire de protéger les citoyens européens placés sans fondement sous sanctions américaines, en garantissant leur accès à des services de paiement. Pour ce faire, la rapporteure appelle à mettre en place une entité bancaire immune publique qui offrirait des services de base en matière de banque et d'assurance. Elle ne devrait pas recourir au dollar et être totalement indépendante du marché américain, de façon à éviter tout lien de rattachement pouvant justifier une inculpation devant les tribunaux américains.

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

- *Les effets attendus*

Dans un premier temps, l'activation du règlement de blocage permettra aux opérateurs européens de faire valoir devant les juridictions américaines leur obligation, au titre du droit européen, à poursuivre une activité contraire à des sanctions américaines.

L'entité bancaire immune au droit extraterritorial offrirait aux personnes sous sanctions américaines une alternative pour la tenue de compte, les moyens de paiement et les services d'assurance.

Enfin, si l'instrument anticoercition devient un moyen de dissuasion crédible, il permettra de rééquilibrer le rapport de force avec les États-Unis en utilisant pleinement le levier que constitue l'accès au marché unique.

### 2. Au niveau national

En parallèle des mesures européennes, des actions au niveau national sont également possibles, dans le respect du droit européen.

- *Les enseignements de la commission d'enquête*

Le transfert de la régulation des services numériques à l'Union européenne, avec l'adoption du RGPD, du DSA, du DMA et du Data Governance Act, restreint les marges de manœuvre dont disposent les États membres.

Les associations de protection des données ont notamment témoigné de la difficulté à défendre les droits des personnes sur leurs données personnelles dans le cadre actuel, en raison de la longueur des procédures, de leur coût financier important, et de l'impossibilité d'accéder au dossier ou d'être entendu. Le DSA a également été fréquemment contourné par des plateformes comme X, TikTok ou Shein, par la diffusion de contenus haineux, violents ou pédopornographiques, sans réaction européenne appropriée.

Les défaillances de l'application du droit européen obligent ainsi à envisager des solutions de repli nationales.

- *Les modalités proposées*

La rapporteure a identifié quatre instruments qui pourraient être activés par la France, en cas d'inaction de l'Union européenne, pour protéger ses ressortissants contre les abus des grandes plateformes. Ils visent à favoriser le dépôt de réclamations, mieux identifier les manquements, les sanctionner, et les faire cesser, en conjuguant le recours au droit européen, au droit administratif et au droit pénal.

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

L'introduction d'un recours collectif, comme le permet l'article 80, paragraphe 2 du règlement, permettrait aux associations de présenter des réclamations contre les manquements au RGPD et de renforcer la protection des droits des personnes. En étant la première à s'engager dans cette voie, la France pourrait exercer un effet d'entraînement sur le reste de l'Union européenne.

L'article 80, alinéa 2, du RGPD autorise les États membres à prévoir que tout organisme, organisation ou association puisse introduire, indépendamment de tout mandat, une réclamation auprès de l'autorité de protection des données s'il considère que les droits d'une personne prévus par le règlement ont été violés. Aucun État membre ne s'est cependant saisi de cette possibilité jusqu'à maintenant.

Comme l'a fait valoir M. Max Schrems lors de son audition, une telle procédure de recours collectif renforcerait le pouvoir d'action des ONG : « *Cette clause nous aurait permis de porter devant la justice de nombreuses affaires que nous ne parvenons pas à faire aboutir. À titre d'exemple, nous recevons de nombreuses plaintes de parents qui nous demandent d'agir contre les atteintes à la vie privée subies par leur enfant, mais aucun d'eux n'accepte que celui-ci soit identifié comme plaignant dans une procédure officielle – contre l'école ou une autre institution –, précisément par crainte de nuire à sa vie privée. L'alinéa 2 de l'article 80 nous permettrait de traiter des situations de ce type*. »

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

Le droit pénal demeurant de la pleine compétence des États membres, l'application de la réglementation européenne sur les services numériques n'interfère pas avec les procédures judiciaires qui pourraient être lancées au niveau national.

Aussi la rapporteure appelle-t-elle à ouvrir des informations judiciaires à l'encontre des grandes entreprises du numérique et de leurs dirigeants en cas de signalement d'atteintes aux droits des personnes résultant de traitements informatiques. Il est indispensable d'envoyer un message très clair : ce qui est interdit hors ligne est interdit en ligne. Des moyens adaptés doivent être mobilisés pour ce type de procédure.

Le parquet de Paris a lancé une telle procédure, le 6 mai 2026, à l'encontre des sociétés du réseau social X, d'Elon Musk et Linda Yaccarino pour les chefs de collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite, administration d'une plateforme en ligne pour permettre des transactions illicites, la violation du secret des correspondances, et extraction frauduleuse de données d'un système de traitement automatisé de données.

**Proposition n° 27 : Suspendre les plateformes dangereuses.**

En cas de violation grave et répétée de leurs obligations par les grandes plateformes, demander au président du tribunal judiciaire compétent d'ordonner la suspension de leurs services, sur la base de l'article 6-3 de la loi pour la confiance dans l'économie numérique.

Si le DSA prévoit, en son article 51, paragraphe 3, la possibilité que l'autorité judiciaire d'un État membre suspende temporairement l'accès à une plateforme, cet outil ne peut être activé qu'en dernier recours, sous des conditions très strictes : tous les autres pouvoirs doivent avoir été épuisés sans permettre de faire cesser l'infraction, et celle-ci doit entraîner un préjudice grave, constituer une infraction pénale impliquant une menace pour la vie ou la sécurité des personnes, et ne pas pouvoir être évitée par l'exercice d'autres moyens prévus par le droit de l'Union ou le droit national.

D'autres pays dans le monde ont pourtant réussi à imposer un tel rapport de force saux grandes plateformes américaines qui ne respectaient pas leur droit, comme l'a montré la suspension du réseau social X par le tribunal suprême du Brésil pendant plus d'un mois en 2024. Le professeur Luca Belli a souligné les différences entre les modèles de régulation européen et brésilien : « *Alors que le STF brésilien intervient directement par voie judiciaire pour protéger l'ordre démocratique, le modèle européen privilégie une régulation administrative centralisée autour de la Commission. Le DSA instaure un cadre graduel et rigoureusement encadré, loin de l'assertivité créative du juge brésilien. En vertu des principes de proportionnalité et de subsidiarité, la suspension d'une plateforme demeure une ultima ratio. Un tel dénouement exigerait des années de procédures, incluant injonctions de conformité, audits, sanctions financières et mesures de mitigation des risques*. »

**La suspension du réseau social X au Brésil**

Comme l'a expliqué le professeur Luca Belli, les réseaux sociaux états-uniens jouent un rôle central dans la vie économique, sociale et politique du Brésil, notamment X, WhatsApp et Instagram. La pratique du *zero-rating*, qui permet à ces entreprises de subventionner l'accès à leurs applications, quand l'accès au reste d'internet demeure onéreux, conduit à ce que l'information de la population passe exclusivement par ces plateformes.

Après l'attaque du 8 janvier 2023 de la place des Trois pouvoirs par des militants d'extrême-droite, marquée par la diffusion massive d'appels à la haine et de fausses informations sur les réseaux sociaux, le Tribunal suprême fédéral a ouvert une enquête à l'encontre de la plateforme X. Celle-ci a été mise en demeure de transmettre des informations sur les milices numériques et de bloquer les comptes de plusieurs émeutiers soupçonnés de disséminer de fausses informations. L'entreprise a refusé de s'y soumettre et a fermé, le 17 août 2024, ses bureaux au Brésil, en violation de la loi sur la protection des données qui exige la présence d'un représentant légal.

Le 30 août 2024, le juge Alexandre de Moraes a ordonné le blocage immédiat des activités de X sur le territoire brésilien, comme le permet l'article 12 du Marco civil da Internet, jusqu'à ce que le réseau social se conforme aux décisions de justice, désigne un représentant légal et s'acquitte des amendes prononcées. Les fournisseurs d'accès à internet ont dû bloquer techniquement les adresses IP du réseau social, sous la supervision de l'Agence nationale des télécommunications (Anatel). Les utilisateurs brésiliens qui contournaient l'interdiction, notamment par l'utilisation de VPN, s'exposaient à une amende de 50 000 reals, soit environ 8 000 euros. La suspension a entraîné une migration des utilisateurs sur d'autres réseaux sociaux, tels que LinkedIn ou Bluesky.

Cette mesure a été particulièrement efficace, puisqu'elle à conduit X à obtempérer et à s'acquitter des amendes de 28,6 millions de réals, soit 4,8 millions d'euros, permettant la levée de la sanction le 8 octobre 2024. Par le passé, cet outil avait déjà démontré son effet dissuasif, en poussant WhatsApp à adopter une posture constructive à l'égard des autorités brésiliennes, après des suspensions similaires intervenues en 2016 et 2017.

Le modèle brésilien n'est cependant pas exempt de paradoxes. Le processus d'examen du projet de loi n° 2630 de lutte contre la désinformation, dit *Fake News Bill*, déposé en 2020, n'a ainsi toujours pas abouti, entravé par l'intense campagne de lobbying menée par les Big Tech contre ce qu'ils appellent une « législation de censure », et par les pressions états-uniennes, notamment la hausse des droits de douane de 50 % justifiée par de prétendues préoccupations sur la liberté d'expression.

« *Au Brésil, la vigueur de la régulation a été rendue possible par l'intervention du pouvoir judiciaire, là où des autorités administratives se montrent souvent plus prudentes, voire léthargiques, malgré leur mission originelle* », a expliqué Luca Belli. C'est cette inaction qui conduit l'autorité judiciaire à adopter un rôle moteur. Par une décision du 26 juin 2025,le Tribunal suprême a ainsi prononcé l'inconstitutionnalité de l'article 19 du Marco Civil Da Internet de 2014, qui reconnaissait l'irresponsabilité des grandes plateformes sur les contenus qu'elles hébergent, et demandé au Congrès national d'adopter un modèle de régulation qui consacre des obligations de vigilance et de retrait immédiat des contenus manifestement illégaux.

Dès lors, la rapporteure souligne l'importance de préserver une capacité d'action nationale, s'appuyant sur l'autorité judiciaire. L'article 6-3 de la loi pour la confiance dans l'économie numérique du 21 juin 2024 dispose que le président du tribunal judiciaire peut prescrire toutes les mesures propres à prévenir ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne.

Sur ce fondement, le gouvernement a demandé à la justice, en décembre 2025, d'ordonner la suspension totale du site Shein après avoir constaté la vente de poupées pédopornographiques. La demande a été rejetée par le tribunal judiciaire qui a considéré qu'elle était disproportionnée au regard du retrait des produits illicites par Shein. Ce jugement a été confirmé par la Cour d'appel le 19 mars 2026. La rapporteure relève néanmoins que cette décision ne préjuge pas du succès de futures procédures en cas de dommage avéré, grave et persistant. Elle appelle ainsi le gouvernement à mobiliser pleinement cet instrument.

- *Les effets attendus*

La rapporteure souligne qu'il est indispensable d'établir un rapport de forces avec les Big Tech dès lors qu'ils enfreignent et contournent nos lois de façon répétée. L'objectif est de renforcer les outils pouvant être mobilisés au niveau national afin de faire appliquer nos règles et de redonner du poids à la France dans les discussions au niveau européen.

### LEVIER N° 6 : LA GOUVERNANCE

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

- *Les enseignements de la commission d'enquête*

En dépit d'une volonté réaffirmée par le gouvernement de faire de la souveraineté numérique une priorité, la mise en œuvre d'une stratégie ambitieuse de réduction des dépendances pour les systèmes d'information de l'État est entravée par la faiblesse de la gouvernance et une approche éclatée entre les différents ministères.

La commission d'enquête n'a pu que constater une grande asymétrie de moyens, techniques, humains et financiers, entre les administrations, qui place certaines d'entre elles dans une situation de grande vulnérabilité et compromet leur capacité à assurer leur mission régalienne ou de service public. La mutualisation des produits numériques et des clouds interministériels est insuffisante, limitant les économies d'échelle et l'effet d'entraînement. Si l'État a posé, par voie de décret ou de circulaire, un certain nombre d'exigences de souveraineté – notamment une incitation à privilégier les logiciels libres, un seuil limite d'externalisation des compétences et l'obligation de recourir à un cloud de confiance pour l'hébergement

des données d'une sensibilité particulière, désormais consacrée par la loi –, la commission d'enquête a constaté qu'elles n'étaient pas systématiquement respectées.

La procédure d'avis conforme de la Dinum sur les grands projets numériques de l'État peut être délibérément contournée par les administrations et ne permet pas de faire cesser les initiatives contraires à la souveraineté, comme l'ont montré les précédents de la Plateforme des données de santé ou du projet Virtuo du ministère de l'éducation nationale. Le récent renforcement de la procédure d'audit à l'égard des achats de logiciels à la demande restera lettre morte si l'impact des décisions de la direction n'est pas conforté.

Les instruments de pilotage font défaut. Si un travail a été lancé par la Dinum, la direction des achats de l'État et l'Ugap pour mesurer les dépendances numériques de l'État, il n'existe pas d'outils de suivi centralisé des dépenses de logiciels, de cloud et de prestations informatiques, et pas davantage de cartographie des données sensibles des administrations.

À cela s'ajoute un défaut d'articulation entre la transformation numérique de l'État et sa politique industrielle dans le secteur du numérique. Le soutien à travers des subventions ou des prises de participation n'est pas mis en cohérence avec les besoins futurs des administrations.

- *Les modalités proposées*

La gouvernance de la stratégie de souveraineté numérique de l'État devrait être portée au plus haut niveau, par la création d'un ministère du numérique de plein exercice, au rang de ministère d'État. Son périmètre devrait couvrir à la fois le développement de la filière numérique française, la transformation numérique de l'État et le portage des positions françaises au niveau européen, afin d'assurer leur pleine cohérence.

Ce ministère serait chargé de l'élaboration d'une feuille de route susceptible d'engager l'ensemble de l'écosystème dans une trajectoire de réduction des dépendances, avec des objectifs chiffrés à moyen et long terme.

Sous son autorité, la Dinum ou la future autorité interministérielle que le gouvernement vient d'annoncer devra bénéficier d'un réel droit de veto sur les grands projets numériques, pour éviter la création de nouvelles dépendances ou vulnérabilités. L'impossibilité de recourir à une solution souveraine devrait être démontrée par une étude de marché approfondie, évitant ainsi à la racine la constitution de nouvelles dépendances.

- *Les effets attendus*

Le renforcement du pilotage gouvernemental de la politique numérique permettra d'enclencher et de piloter la trajectoire d'adoption des logiciels libres dans l'ensemble de l'économie, en en suivant toutes les dimensions : état de la

filière numérique, complétude de la stack technologique, réorientation de la commande publique et de la commande privée.

La feuille de route chiffrée permettra aux entreprises du numérique de disposer d'une visibilité sur les besoins de l'État et des entreprises, afin de développer leur offre en conséquence. Elle garantira également aux ministères la continuité nécessaire sur le temps long pour engager des transformations profondes de leurs systèmes d'information.

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

- *Les enseignements de la commission d'enquête*

La rapporteure a constaté la faible transparence de l'État sur le niveau de ses dépendances numériques, en particulier sur les segments des logiciels et des prestations de services numériques. L'information budgétaire et technique délivrée au Parlement en la matière demeure parcellaire, ce qui ne lui permet pas d'exercer pleinement son rôle de contrôle.

En outre, les enjeux numériques se trouvent morcelés entre les différentes commissions permanentes de l'Assemblée nationale, empêchant les députés de les aborder conjointement. Sont ainsi compétentes :

– la commission des lois s'agissant de la protection des données personnelles et des atteintes aux droits fondamentaux ou au bon fonctionnement de la démocratie ;

– la commission des affaires économiques pour le développement de la filière numérique, le soutien à l'innovation, la sécurité économique, ou les enjeux énergétiques sous-jacents ;

– la commission de la défense et des forces armées sur les menaces informationnelles et la lutte cyber ;

– la commission du développement durable sur l'impact environnemental des infrastructures de télécommunication ;

– la commission des affaires culturelles et de l'éducation quant au développement des compétences numériques, la formation au libre, ou l'impact de l'IA sur la création.

– la commission des affaires sociales quant à l'impact du développement de l'IA sur l'emploi.

À titre d'exemple, l'examen du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité a nécessité la création d'une commission spéciale dédiée du fait de sa nature transversale. De

même, traiter séparément les enjeux d'innovation et de protection des droits fondamentaux conduit trop souvent à les opposer, comme l'ont illustré les débats sur l'intelligence artificielle et le droit d'auteur.

- *Les modalités proposées*

La rapporteure appelle la Conférence des présidents à créer une délégation au numérique au sein de l'Assemblée nationale afin de reconnaître sa dimension transversale et structurante.

- *Les effets attendus*

La délégation au numérique permettra à l'Assemblée nationale d'articuler les différents enjeux que soulève le numérique et de renforcer la cohérence de son approche des politiques menées en la matière, en exerçant un contrôle accru sur la réduction des dépendances.

Elle est également susceptible d'encourager le travail transpartisan et de favoriser des initiatives législatives ambitieuses. Les travaux de la délégation aux droits des femmes ont ainsi conduit à l'adoption de la loi du 6 novembre 2025 modifiant la définition pénale du viol et des agressions sexuelles.

Il demeure cependant essentiel que les commissions permanentes ne se dessaisissent pas du sujet, structurant pour l'ensemble de leurs thématiques.

## LISTE DES RECOMMANDATIONS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## LISTE DES PROPOSITIONS

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

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

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

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

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

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

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

**Proposition n° 30 :** Prévoir que le code source des logiciels développés par une entreprise entrera dans le domaine public en cas de cessation définitive d'activité.

**Proposition n° 8 :** Créer un musée du numérique.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**Proposition n° 27 :** Suspendre les plateformes dangereuses.

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

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

## EXAMEN EN COMMISSION

*Au cours de sa réunion du mercredi 8 juillet, à 15 heures, la commission a procédé, à huis clos, à l'examen du projet de rapport suivi d'un vote.*

**M. le président Philippe Latombe.** Nous arrivons au terme des travaux de notre commission d'enquête, après 45 auditions, au cours desquelles nous avons entendu 112 personnes – chercheurs, représentants d'associations, d'entreprises et d'administrations – et un déplacement à Bruxelles.

Ces travaux ont permis d'établir une cartographie inédite et très précise des dépendances et vulnérabilités de notre pays et de l'Union européenne dans le domaine du numérique, ainsi que des dangers qui y sont associés.

Ils s'inscrivent dans la continuité de mon rapport d'information, publié il y a cinq ans, qui appelait à bâtir une souveraineté numérique française et européenne. Depuis, la nouvelle donne internationale, l'affaiblissement de la régulation européenne et l'omniprésence de l'intelligence artificielle (IA) nous obligent à redoubler de vigilance et à renouveler nos solutions.

L'actualité récente l'a montré – le blocage de l'accès aux derniers modèles d'intelligence artificielle d'Anthropic à la demande du gouvernement américain –, le *kill switch* n'est plus seulement une hypothèse mais une réalité.

Je remercie la rapporteure et salue son travail riche et exigeant, dont témoigne le volume du document qui est soumis à votre vote. Je crois pouvoir dire que nous avons travaillé de manière assez consensuelle.

Je remercie également les membres de la commission d'enquête qui ont pris part aux travaux et j'invite ceux qui le souhaitent à faire parvenir une contribution au secrétariat avant vendredi, douze heures. Ces contributions seront annexées au rapport lors de sa publication.

À l'issue de notre discussion, je mettrai aux voix l'adoption du rapport.

**Mme Cyrielle Chatelain, rapporteure.** Je voudrais remercier le président pour la qualité de notre collaboration et le travail que nous avons effectué, ainsi que les équipes, qui ont consacré beaucoup de temps à l'analyse des informations que nous avons demandées.

En six mois, il ne nous était pas possible d'examiner de manière approfondie des questions comme les cyberattaques et les ingérences, qui constituent des sujets d'étude à part entière, ni de nous pencher en détail sur l'aspect matériel des dépendances. Un certain nombre d'éléments sont donc absents du rapport. Il est à noter que le gouvernement mène un travail à ce sujet et que plusieurs Livres blancs

y ont été consacrés. Nous devrions débattre en septembre du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité – d'après la dernière rumeur, le texte pourrait être inscrit à partir du 21 septembre.

Chacun est conscient du contexte géopolitique, rappelé par le président, dans lequel le groupe Écologiste et social a fait usage de son droit de tirage tendant à la création de cette commission d'enquête.

Je voudrais revenir sur les enseignements que nous avons tirés de nos travaux.

Le premier d'entre eux est la mise en évidence d'une forte dépendance, depuis de nombreuses années, dans le domaine des logiciels, qui est source d'effets nocifs. Nos administrations font face à une dépendance quasi généralisée à trois fournisseurs : Microsoft, VMware et Oracle. Parmi les cinquante plus gros fournisseurs de logiciels aux administrations, les acteurs états-uniens représentent près de 80 % des achats selon l'Ugap (Union des groupements d'achats publics). Cette dépendance s'accompagne d'un système de verrouillage qui entraîne une augmentation des prix. La dépendance est donc non seulement technologique mais aussi économique, comme plusieurs acteurs nous l'ont confié lors des auditions.

Les dépenses des administrations publiques, collectivités comprises, à destination des acteurs extra-européens sont estimées à 1,5 milliard d'euros. Je voudrais revenir très rapidement sur la méthodologie employée pour parvenir à ce chiffre. Le rapport comporte plusieurs chiffres. Le premier est consolidé à partir des réponses que les administrations centrales ont apportées aux questionnaires que nous leur avons adressés. Le deuxième résulte du travail accompli par la Dinum (direction interministérielle du numérique) sur ce même périmètre. Une estimation plus globale de l'Ugap comprend les administrations d'État et les collectivités locales. Sur le milliard et demi que j'évoquais, on peut estimer que 1 milliard est aujourd'hui directement substituable. Des solutions existent, dans le domaine des logiciels, pour remédier aux dépendances.

J'apporterai une note d'optimisme en relevant que les dépendances sont moins prononcées s'agissant des logiciels critiques car plusieurs acteurs français et européens sont positionnés sur ce marché. Nous n'avons toutefois pas pu examiner les logiciels utilisés par les opérateurs français et européens – cela devrait faire l'objet d'un travail plus approfondi.

S'agissant du cloud, nous avons souligné l'efficacité de la labellisation SecNumCloud, qui permet de contenir les risques liés à l'utilisation du cloud dans les administrations d'État. À côté des outils SecNumCloud, on trouve également des clouds publics comme Pi ou Nubo, qui offrent un niveau de sécurité élevé. On constate malheureusement une inégalité entre les administrations. Certains ministères, notamment les ministères sociaux, ceux de la justice et de la culture, continuent de recourir à des clouds qui ne correspondent pas à la doctrine Cloud au centre. Par ailleurs, les opérateurs d'importance vitale recourent dans une large

mesure à des clouds extra-européens. On peut dresser les mêmes constats pour les entreprises privées. Les entreprises européennes achètent des logiciels et des services cloud aux entreprises américaines pour un montant de 264 milliards d'euros.

L'utilisation par les administrations et les entreprises privées de services numériques extra-européens et, en ce qui concerne les logiciels, d'outils essentiellement américains se traduit par une perte directe de valeur ajoutée pour la France et l'Europe. Le taux de valeur ajoutée des entreprises qui restent sur le territoire n'excède pas, dans le meilleur des cas, 28 %, alors que la moyenne, dans le secteur des plateformes et du cloud, avoisine 42 % – le taux est même supérieur pour les opérateurs français ou européens.

L'impôt sur les sociétés (IS) engendre de très faibles recettes. En revanche, la taxe sur les services numériques joue son rôle ; si les acteurs extra-européens ne s'en acquittaient pas, leur contribution fiscale serait très limitée. Les opérateurs cloud extra-européens, tel Digital Realty, ne sont toutefois pas soumis à cette taxe.

Le rapport traite également de la violation de la vie privée par les Big Tech. Le modèle économique de ces entreprises repose sur l'exploitation des données à des fins commerciales. Ces données transitent par de nombreux acteurs, dont certains sont très opaques, comme les *data brokers*. Cela entraîne un risque systémique de fichage de la population et constitue aussi un danger géopolitique comme économique, qui peut se matérialiser, par exemple, par le *kill switch* ou l'espionnage industriel.

Le fait d'être dépendant d'opérateurs qui obéissent à des lois étrangères nous rend vulnérables, tant sur le plan de la protection des données que dans le domaine technologique, comme l'illustrent le cas du juge Guillou et le blocage d'Anthropic. Pour mesurer l'ampleur du phénomène, il faut savoir que le gouvernement américain a adressé à Microsoft plus de 5 500 demandes de divulgation de données au second semestre 2025 et plus de 60 000 à Google, qui les a satisfaites dans 89 % des cas. La question de la protection des données se pose donc, tant vis-à-vis des acteurs états-uniens qu'à l'égard des entreprises chinoises.

J'en viens aux raisons de cette dépendance très enracinée. Il faut d'abord tordre le cou à l'idée souvent exprimée – qui est un outil de lobbying – selon laquelle il n'y aurait pas d'alternative possible. Les auditions ont montré qu'il existe des solutions technologiques, que nous avons des produits solides, à l'image de la plateforme des données de santé. Cela étant, les centrales d'achat ne savent pas toujours distinguer les produits américains des autres. Les chiffres donnés par l'Ugap ont dû être retravaillés parce qu'elle considère comme européens des groupes dont la maison mère est installée en Irlande, mais qui sont clairement des opérateurs américains, tel Amazon. Il faut savoir opérer cette distinction.

L'idée selon laquelle il n'y aurait pas de solution alternative est véhiculée par les passeurs de technologie, qui sont des entreprises de conseil ou de service qui

réalisent une grande partie de leur chiffre d'affaires par le biais, notamment, de Microsoft ou d'autres Big Tech, en vendant des logiciels extra-européens considérés comme standards et en opérant sur ceux-ci.

L'éducation contribue à l'enracinement de la dépendance, qui commence très tôt. Microsoft s'est rendu incontournable dans le domaine scolaire et crée des habitudes d'usage dès le plus jeune âge.

La deuxième raison fondamentale de la dépendance tient au fait que le soutien financier substantiel qui a été apporté à la filière du numérique s'est concentré sur l'émergence de licornes et de start-up sans être systématiquement assorti de conditions liées à la souveraineté et aux infrastructures. Cette absence de conditionnalité des aides et des prises de participation est de nature à fragiliser les opérateurs lors de la revente, alors que le passage à l'échelle est complexe sur le marché européen et qu'il n'y a aucune garantie que ces start-up fonctionnent sur des infrastructures ou avec des logiciels européens.

La vision de l'État sur la politique numérique est balbutiante puisque, longtemps, le numérique a été considéré comme un support neutre et non comme une politique en tant que telle. Nous sommes confrontés à plusieurs enjeux en matière scolaire et dans le domaine des compétences ministérielles. Les ministères les plus dépendants au cloud extra-européen et aux solutions propriétaires américaines sont ceux qui détiennent le moins de compétences numériques propres. Les taux d'externalisation peuvent dépasser 60 % ; ils ont parfois même atteint 90 %, ce qui signifie que le chef de projet lui-même était externalisé. Dans ce cas de figure, on perd totalement le contrôle sur le système déployé. En outre, l'État peine à coordonner les choix de ses ministères ; il conviendrait qu'ils adoptent des solutions techniques identiques.

Nous nous heurtons à des difficultés en matière d'application de la réglementation. Les sanctions prises à l'encontre des géants du numérique, les Gafam, s'élèvent à près de 17 milliards d'euros, dont 12 milliards contre le seul Google. Toutefois, ces montants restent faibles au regard de leurs capacités financières. En outre, les procédures sont très longues, les sanctions sont souvent prononcées trop tard et les amendes ne sont pas toujours recouvrées.

L'Irlande est dépendante économiquement des grandes entreprises de la tech, qui y ont installé leurs sièges sociaux, mais est aussi le pays où sont jugés les contentieux relatifs au RGPD (règlement général sur la protection des données). Il en résulte un conflit d'intérêts qui rend la situation intenable. Le Luxembourg abrite également des maisons mères, mais à un niveau bien moindre. Pour ce qui concerne le DMA (règlement sur les marchés numériques) et le DSA (règlement sur les services numériques), nous avons moins de recul car ce sont des réglementations récentes.

Nous aurions intérêt à nous protéger du lobbying. À l'échelle européenne, les Gafam y ont consacré 35 millions d'euros en 2025 ; 210 lobbyistes sont

déclarés ; 265 rendez-vous ont été pris avec la Commission européenne, soit quasiment un par jour ouvré. On assiste à un lobbying intensif auprès des instances européennes alors que se tiennent les discussions sur l'omnibus numérique.

La dernière partie du rapport est consacrée à l'intelligence artificielle et aux data centers. Nous nous sommes fondés sur plusieurs travaux, publiés très récemment, émanant notamment de la direction du Trésor et de l'Insee, mais aussi sur des études précédentes, comme le rapport de la Commission de l'intelligence artificielle. La réflexion n'en est qu'à ses débuts. Nous avons peu de recul sur l'IA, qui soulève plusieurs questions.

S'agissant du modèle économique, on peut se demander si l'on assiste à la formation d'une bulle. Le FMI (Fonds monétaire international) l'évoque sans trancher la question. En tout état de cause, le montant des investissements est bien supérieur aux revenus obtenus comme aux revenus potentiels, même dans une vision maximaliste.

Nous nous interrogeons aussi sur le coût de l'utilisation de l'IA et son apport pour les entreprises. Comme les personnes auditionnées l'ont reconnu, aucune étude ne montre que l'IA entraîne une hausse du retour sur investissement des entreprises. En outre, l'intelligence artificielle a un impact considérable sur l'environnement.

Le rapport consacre un développement aux liens entre l'IA et l'emploi. Nous essayons de dresser un état des lieux des informations et réflexions existantes à ce sujet, sachant que de nombreux facteurs d'incertitude demeurent. Nous ne savons pas quelle sera la vitesse de pénétration de l'IA, quel type de tâches elle affectera ni quelles améliorations ou, en tout cas, quelles évolutions elle connaîtra. Le débat public s'est emparé de ces questions, notamment à la suite d'un certain nombre de licenciements qui ont été annoncés comme étant imputables à l'intelligence artificielle, même si la direction du Trésor nuance ce lien de causalité. Ces annonces peuvent parfois être justifiées par d'autres motifs mais le lien entre le développement de l'IA dans les entreprises et l'évolution de l'emploi n'en constitue pas moins une réelle préoccupation.

La protection des données, dans le cadre du déploiement de l'IA, est peu régulée. La définition de l'open source fait débat mais demeure inappliquée. Le travail sur l'intelligence artificielle ne fait que commencer.

L'intelligence artificielle repose sur les data centers dont les besoins ont fortement progressé ces deux dernières années, notamment depuis le Sommet pour l'action sur l'intelligence artificielle.

Le rapport revient sur la question des capacités électriques. Nous nous sommes d'abord penchés sur l'implantation de ces centres. Nous ne divulguons ni les terrains identifiés ni les emplacements exacts mais fournissons des indications géographiques pour donner une idée de leur répartition. Les projets se concentrent dans deux régions : sans surprise, l'Ile-de-France, et, dans une moindre mesure, les Hauts-de-France.

RTE a réservé 15 gigawatts (GW) de capacité de raccordement aux projets de data centers, soit 24 % de la puissance électrique du parc nucléaire français, une proportion très élevée. Au-delà de la question de la soutenabilité, il s'agit de savoir à quels opérateurs cela profite. Après analyse approfondie, nous avons pu établir la décomposition suivante : 2 GW sont destinés aux *hyperscalers*, autrement dit des opérateurs américains ; 2,5 GW à des acteurs extra-européens autres que ces opérateurs ; 9 GW à des acteurs non spécialisés poursuivant une logique d'investissement, ce qui ne nous permet pas de savoir qui seront les utilisateurs finaux – des auditions, on peut déduire qu'il s'agira d'*hyperscalers*, qui ont la capacité de payer ; enfin, 1,4 GW seulement à des acteurs européens. La puissance électrique réservée étant dans une très large proportion captée par des acteurs extra-européens, nous devons nous mobiliser si nous voulons éviter de créer de nouvelles dépendances.

J'ajoute que parmi les opérateurs accompagnés par la task force, 35 % sont français et plus de 50 % sont extra-européens.

Le rapport comporte à la fois des recommandations et des propositions. Les recommandations portent sur des actions plutôt consensuelles, à mettre en œuvre assez rapidement, je pense à la publication des décrets de la loi visant à sécuriser et à réguler l'espace numérique, dite loi Sren,

Les propositions quant à elles concernent des enjeux plus structurants, comme l'open source. Nous suggérons notamment de créer une fondation dédiée à l'open source. Elle encouragerait divers acteurs – État, opérateurs privés, activités à but lucratif ou pas – à développer ensemble des briques pour ensuite les utiliser selon leurs besoins propres. Nous suggérons que cette fondation gère un fonds similaire au Sovereign Tech Fund allemand pour financer la maintenance des outils open source. À côté du Consortium pour une infrastructure numérique européenne (Edic), il importe de soutenir une structure française œuvrant en ce sens.

Nous préconisons, par ailleurs, de viser pour 2030 l'objectif de réserver une part des commandes publiques aux acteurs de l'open source français et européens, lesquels sont très en avance. Il importe également de réorienter la commande privée, ce qui suppose d'instaurer un crédit d'impôt destiné à inciter financièrement les PME à rechercher l'appui d'acteurs de l'open source.

D'ici à 2030, il convient également de s'assurer que les outils externalisés peuvent continuer à fonctionner. Nous suggérons de généraliser le mécanisme de l'*escrow* dans les contrats signés par une structure publique avec un fournisseur : en cas de défaillance de ce dernier, ladite structure a accès aux éléments indispensables au fonctionnement du logiciel. Pour assurer la continuité des services, l'État devrait se tourner vers ce dispositif auquel les entreprises privées ont déjà recours.

Il faut par ailleurs réaffirmer la nécessité de sortir Microsoft de l'école si nous voulons mettre fin à l'une des dépendances les plus profondément enracinées.

Nous proposons, en outre, de renforcer de manière graduelle les contreparties qui s'imposent aux entreprises soutenues par l'État. Seraient visées en priorité les entreprises qui, après avoir bénéficié d'aides publiques, sont revendues dans un délai court à des opérateurs américains : prévoyons, en cas de vente, un remboursement de ces aides, qu'il s'agisse des aides à l'amorçage ou du crédit d'impôt recherche.

Nous envisageons la possibilité pour l'État de détenir une *golden share* dans Mistral AI et ChapsVision qui deviennent pour lui des partenaires essentiels. Cela permettrait d'instaurer un droit de blocage de certaines décisions, notamment celles concernant le capital, et éviterait que des atteintes soient portées à la souveraineté de la France.

Enfin, solution de dernier ressort, une clause de souveraineté finale pourrait être proposée aux fournisseurs de logiciels jouant un rôle structurant au sein de l'État. En cas de revente, les éléments indispensables pour les faire fonctionner seraient rétrocédés à l'État. Autrement dit, c'est une manière d'empêcher la revente car aucun acheteur ne voudrait d'une entreprise ayant perdu de tels avantages.

Je reviens aux data centers pour préciser que le rapport préconise d'instaurer un moratoire sur les projets profitant aux acteurs extra-européens et de définir un nouveau cadre de régulation pour orienter les projets au service de l'intérêt public national.

Sur le plan juridique, il importe à la fois de renforcer les règles et leur application. Au niveau européen, il ne faut pas céder aux lobbies. Défendons-nous, notamment en recourant à des outils jusqu'à présent peu utilisés comme l'instrument anticoercition de l'Union européenne, si les comportements de Donald Trump l'imposaient. Au niveau national, il convient de réfléchir à la manière de mobiliser des outils nous permettant d'agir, tout en respectant le droit européen. Pensons aux procédures de recours collectif pour la bonne application du RGPD ou à la création d'un syndicat de données. Il s'agirait de favoriser la mutualisation des données publiques en faisant respecter les licences qui s'y rattachent.

Je conclurai avec la gouvernance. Considérant que le numérique appelle une politique publique à part entière, nous vous proposons la création d'un ministère du numérique de plein exercice. Par ailleurs, nous suggérons la mise en place au sein de notre assemblée d'une délégation consacrée au numérique, enjeu qui concerne de nombreuses commissions – lois, affaires sociales, affaires économiques, affaires culturelles, défense. Cela nous permettrait de suivre de plus près ce sujet, dont on débat finalement assez peu alors qu'il est devenu structurant, et de lui donner de la visibilité.

Après cette présentation longue mais synthétique, je vous soumettrai trois modifications du rapport mais je laisse d'abord au président le soin d'ouvrir une phase d'échanges.

**M. Vincent Thiébaut (HOR).** Vous avez mené un nombre considérable d'auditions et je vous en félicite. Un bel été de lecture m'attend avec votre rapport, au sujet duquel je formulerai deux réserves principales.

Premièrement, il faut être clair sur ce que l'on entend par open source et avoir en tête les implications juridiques inhérentes aux quatre-vingts licences existantes. L'open source n'est nullement une garantie de souveraineté et d'autonomie, je le sais pour avoir travaillé avec ces outils dans le cadre de mon activité professionnelle. Il implique des contraintes en termes de distribution et de propriété. Sur le plan financier et économique, les utilisateurs sont, en outre, fortement liés, soit à un prestataire, soit à des équipes internes, auxquels ils doivent notamment avoir recours pour toute modification de code ou mise à jour. Certes, pour les PME, le coût d'acquisition du logiciel est moindre mais le coût de maintenance reste très élevé.

Ma deuxième remarque concerne l'aspect financier. Pour ce qui est du domaine bancaire, vous avez bien cerné une partie des enjeux. Nous avons bien vu quelles avaient été les répercussions des sanctions américaines qu'a subies Nicolas Guillou, juge à la Cour pénale internationale. Il ne peut plus utiliser de systèmes de paiement américains comme Visa.

Je regrette toutefois que vous n'ayez pas intégré les prestations de services de paiement, ce qu'on appelle les Fin Tech. Cet important enjeu européen a jusqu'à présent été un peu négligé. Lors du débat sur le projet de loi-cadre sur les transports, a été évoqué le problème de souveraineté que posait le recours à des *wallets* comme Apple Pay ou Google Pay pour l'achat de billets. C'est une préoccupation qu'il faut aussi avoir à l'esprit pour les transactions bancaires concernant l'e-commerce, qui ne reposent pas non plus sur des solutions souveraines.

**Mme Virginie Duby-Muller (DR).** Je vous félicite pour cet important travail, dont l'actualité récente a révélé toute la pertinence. Le récent recours au *kill switch* par l'administration américaine montre en effet que les questionnements sur la dépendance, la vulnérabilité, la souveraineté sont loin de relever de la fiction.

La proposition n° 18 porte sur le remboursement des aides à l'amorçage. Je comprends la logique qui la sous-tend mais votre démarche me semble trop répressive. Ne serait-il pas plus vertueux de faire en sorte de préserver l'implantation de ces entreprises en France ? Souvent, ce n'est pas par choix qu'elles quittent notre pays. Veillons à accompagner leur croissance, de scale-up à licornes.

J'appuie la proposition n° 28 visant à créer un ministère dédié au numérique. Ces dernières années, le portefeuille du numérique a connu plusieurs rattachements administratifs, successifs : le Premier ministre, sans disposer d'administration, Bercy, la recherche, à nouveau Bercy. Le ministère que vous envisagez serait-il placé sous la tutelle du premier ministre ? C'est à voir car l'ensemble des politiques publiques menées en ce domaine suppose un pilotage

politique. Autre question : aurait-il la Dinum (direction interministérielle du numérique) dans son périmètre ?

**M. Nicolas Bonnet (EcoS).** Je me joins à mes collègues pour vous féliciter du travail accompli. Je suis globalement d'accord avec les conclusions que vient de nous présenter Mme la rapporteure.

Je reviendrai sur la question de l'open source. La valeur d'un logiciel en accès libre, tient au nombre de ses utilisateurs. Plus la communauté est fournie, plus il y a de moyens pour le développer, plus il est simple à mettre à jour et moins la correction des bugs est coûteuse, ce qui contribue à diminuer la facture à long terme. L'open source n'est certes pas synonyme de souveraineté mais il peut nous aider à réduire notre dépendance. Nous avons tout intérêt à massifier le recours à ces logiciels qui offrent des possibilités auxquelles les logiciels propriétaires détenus par les Big Tech ne nous donneront jamais accès. Prenons le cas de Microsoft : personne ne peut corriger les bugs de Windows 10 puisque le code source n'est pas ouvert ; dès lors que le support n'est plus assuré, la migration vers Windows 11 devient incontournable.

À cet égard, la proposition consistant à favoriser le recours à l'open source dans les PME me paraît intéressante.

Je vous soumets une autre piste : fournir un package de logiciels en open source aux collectivités ayant les mêmes besoins, typiquement les petites communes. Cela leur ferait faire des économies extraordinaires. Compte tenu de l'effet d'échelle, cela ne coûterait à terme pas plus cher que les logiciels sous licence, qui sont en grande majorité américains.

Madame Duby-Muller, vous déplorez une approche trop répressive à l'égard des PME, évoquant le cas d'entreprises « obligées » de quitter la France. Vous estimez que nous devrions nous montrer sympathiques à leur égard ? Il faudrait donc leur dire : puisque vous n'avez vraiment pas le choix, partez sans rendre l'argent. C'est cela ? J'aimerais vraiment que vous m'expliquiez.

**M. le président Philippe Latombe.** Je confirme que l'open source est une question très vaste. Certaines solutions sont sous licence, d'autres non. Des communautés sont composées de seulement deux personnes quand d'autres en comptent plusieurs milliers, voire centaines de milliers. Certaines solutions, comme Mozilla, dépendent d'une fondation quand d'autres, comme Red Hat, sont à but commercial. C'est d'ailleurs pour cette raison que le rapport plaide en faveur d'une définition commune de l'open source au sein de l'Union européenne. En tout état de cause, nous aurions pu consacrer six mois supplémentaires de travail à cette seule question.

Par ailleurs, j'appelle votre attention sur le fait que l'actualité est particulièrement brûlante. À son arrivée au sommet de l'Otan, tout à l'heure, le président américain a affirmé qu'il ne voulait plus travailler avec trois pays européens, parmi lesquels l'Espagne et l'Allemagne. J'espère que cela réveillera les

consciences, car quand nous nous sommes rendus à Bruxelles, nous avons constaté une différence de traitement entre les entreprises américaines et les autres sociétés étrangères.

Il faut donc développer une vision européenne et j'espère que ce rapport aidera le gouvernement à défendre certains sujets auprès de la Commission européenne, surtout eu égard au contexte qui s'envenime fortement depuis quelques heures.

Enfin, comme la rapporteure l'a dit, certaines entreprises souhaitent capter une énergie abondante, décarbonée et bon marché pour faire fonctionner les data centers. À cet égard, j'espère que le travail transpartisan que nous avons mené nous permettra de réfléchir, avec nos collègues sénateurs, à une véritable politique industrielle dépassant les seules questions des investissements directs à l'étranger et de l'énergie.

Quant aux entreprises elles-mêmes, les auditions ont montré que certaines bénéficient d'avantages fiscaux et d'aides publiques, mais sans en rembourser le montant en cas de rachat ; le débat revient lors de chaque acquisition. Une manière de le trancher une bonne fois pour toutes – toujours de manière transpartisane – serait de dire que des aides comme le crédit d'impôt recherche sont amortissables sur trois ou cinq ans et qu'en cas de cession au cours de cette période, la part non amortie doit être remboursée. Il ne s'agirait pas d'une mesure coercitive : le plan de financement du rachat inclurait cette obligation.

Notons que le financement européen pose question de manière générale. Je fais ici référence au 28e régime et au projet d'union des marchés des capitaux, dont le rapport Draghi faisait déjà état. Nous n'avons pas pu aller au bout de cette discussion lors de notre déplacement à Bruxelles, mais, là encore, il s'agit d'une très vaste question.

Vous l'avez compris, je suis très heureux que nous ayons travaillé de manière transpartisane et abouti à des propositions. Il peut bien sûr y avoir des désaccords, c'est le propre de l'Assemblée nationale, mais au moins partageons-nous certains constats pouvant nous faire avancer vers des solutions consensuelles.

**M. Vincent Thiébaut (HOR).** Au fond, Nicolas Bonnet et moi sommes d'accord.

Quand on parle de l'open source, on pense spontanément à Microsoft ou à Google, mais la majorité des PME utilisent des logiciels de gestion français, ou du moins développés en France. L'éditeur le plus utilisé par les TPE-PME, Sage, est certes anglais, mais sa solution est entièrement développée en France, à Metz notamment. Beaucoup de solutions sont donc souveraines et répondent à nos règles sociales et fiscales.

Par ailleurs, n'oublions pas que les mises à jour font partie du contrat de maintenance des entreprises et qu'elles ne leur coûtent que quelques centaines

d'euros. Mais pour les sociétés qui fonctionnent en open source, il faut compter au moins 600 euros par jour, hors frais de déplacement.

Dans la mesure où nous disposons d'un écosystème purement national, notamment en ce qui concerne les logiciels de gestion, peut-être devrions-nous donc défendre à la fois l'open source et les solutions souveraines. Je suis entièrement d'accord avec vous s'agissant de la bureautique et de la place de Microsoft, mais l'écosystème numérique français ne se résume pas à cela. L'open source n'est pas la panacée, à moins de nous entendre sur une définition très précise.

Quant aux questions énergétiques, je suis également d'accord : nous devrions en débattre. Je viens de rencontrer les représentants de la société Stellaria, qui conçoit des SMR, c'est-à-dire des petits réacteurs modulaires, qui présentent d'intéressantes perspectives en matière d'énergie décarbonée.

**Mme Cyrielle Chatelain, rapporteure.** Je suis d'accord avec ce qui vient d'être dit au sujet de l'open source. Au-delà de sa définition, qui doit effectivement être précise, l'interopérabilité est également très importante. À cet égard, l'idée n'est pas d'imposer l'open source aux PME, mais de les inciter financièrement à opter pour les opérateurs qui l'utilisent, car ils représentent un moindre degré de dépendance. Nous avons rencontré certains éditeurs français dont l'offre se fonde sur l'open source : ils cherchent un marché. Peut-être que l'argent public que nous consacrons à juste titre au développement numérique des entreprises est insuffisamment orienté en leur faveur. C'est d'ailleurs tout l'objet du Buy European Act, que nous appelons de nos vœux dans le rapport, mais qui n'existe pas encore. Le recours aux acteurs européens est insuffisant ; nous sommes d'accord.

Je suis également d'accord avec vous concernant les questions bancaires. Une partie du rapport est consacrée au développement de Wero et de l'euro numérique, mais comme ce sont des projets en cours, nous n'en avons pas fait des recommandations à proprement parler.

S'agissant du remboursement des aides publiques, nous aurons certainement des visions différentes, mais je vous rejoins sur la question de l'amortissement. Il ne s'agit pas de calculer ce qu'on a donné à une entreprise au cours des dix dernières années et de lui demander de tout rembourser en cas de rachat. Mais ce qui lui a été transmis pour son développement ne saurait, selon moi, servir une opération économique de valorisation. Quoi qu'il en soit, si une telle proposition devait être soumise à l'Assemblée nationale, je ne doute pas qu'elle serait amplement débattue avant d'être éventuellement adoptée.

Quant au ministère du numérique, nous ne nous exprimons pas sur son organisation, car elle relève des prérogatives du premier ministre. Cela étant, il serait logique que l'Ariane (autorité référente pour l'intelligence artificielle et le numérique de l'État) relève de ce ministère, pourquoi pas de plein exercice et doté de services importants. Cet aspect est lié à la définition des besoins de l'État et à la manière dont ils sont communiqués à l'écosystème, afin que celui-ci développe les

produits adéquats. C'est pour cette raison que nous avons besoin qu'un acteur impulse cette logique au sein des ministères.

**M. le président Philippe Latombe.** Nous en venons aux trois modifications du rapport que nous devons porter à la connaissance de la commission d'enquête.

**Mme Cyrielle Chatelain, rapporteure.** La première modification concerne le secret fiscal, page 95. Nous avons reçu des données de la part de la DGFIP (direction générale des finances publiques), mais nous ne pouvons les divulguer dans la mesure où elles permettent de faire le lien entre des opérateurs et des montants. Nous avons essayé de regrouper ces opérateurs, mais ils ne sont pas en nombre suffisamment important pour préserver le secret. En conséquence, nous proposons de nous en tenir à un ratio entre le montant de l'impôt sur les sociétés acquitté et de conserver le montant global issu de la taxe sur les services numériques, qui s'élève à 542 millions d'euros concernant les plateformes.

**M. le président Philippe Latombe.** Notons qu'il faudra réfléchir à une modification du règlement des assemblées parlementaires concernant ces situations monopolistiques, afin de pouvoir légalement porter de tels éléments à la connaissance du public. Dans cette attente, je ne peux que soutenir la proposition de la rapporteure. Le ratio entre le chiffre d'affaires et l'impôt sur les sociétés est le seul moyen dont nous disposons pour donner une information de manière anonymisée.

**Mme Cyrielle Chatelain, rapporteure.** La deuxième modification a trait au secret des affaires, qui s'applique aux contrats passés entre les administrations et les fournisseurs. Dans l'absolu, j'estime que les citoyens devraient avoir un droit de regard sur toutes les dépenses publiques, mais après réflexion, je vous propose un tableau montrant les différences, parfois importantes, entre les administrations dans ce domaine. Certaines s'acquittent d'un montant minime par utilisateur, quand d'autres affichent au contraire des dépenses très importantes par poste, à l'instar du ministère de la justice en raison de son manque de compétences internes en la matière.

**M. le président Philippe Latombe.** Comme précédemment, je ne peux que soutenir cette modification nous permettant de respecter le secret des affaires. La Cada (Commission d'accès aux documents administratifs) m'a confirmé que certains chiffres, que me refusaient des administrations, ne peuvent être rendus publics. Comme nous sommes de nouveau confrontés à des situations monopolistiques, nous proposons donc un tableau avec différentes couleurs – il faudra aussi prévoir un dégradé en noir et blanc – et renseignant des montants globaux, ce qui nous permet d'anonymiser les informations.

**M. Nicolas Bonnet (EcoS).** Si des valeurs absolues donneront effectivement des informations importantes concernant les montants versés aux opérateurs étrangers, en l'occurrence américains, serait-il possible de disposer également des chiffres par utilisateur ?

**Mme Cyrielle Chatelain, rapporteure.** Le tableau figurant page 213 répond à votre demande, étant entendu que nous ne disposons pas des chiffres pour l'ensemble des ministères : tous ne nous ont pas communiqué leurs dépenses par utilisateur. Parmi les ministères qui apparaissent dans les couleurs les plus sombres, celui de la défense affiche à la fois des dépenses élevées et un nombre de postes important. Le ministère de la justice fait aussi état de montants conséquents, mais pour un nombre d'utilisateurs très inférieur. Quant aux affaires sociales, si les montants engagés sont nettement plus réduits, le nombre de postes concernés l'est aussi.

**M. Vincent Thiébaut (HOR).** Les chiffres relatifs à la gendarmerie sont intéressants !

**M. le président Philippe Latombe.** Avec l'audition d'Arthur Mensch, celle des représentants de la gendarmerie est celle qui a fait le plus parler. La commission d'enquête sur l'audiovisuel public, qui s'est tenue en parallèle de la nôtre, a monopolisé l'attention médiatique, mais les chiffres donnés par la gendarmerie ont été repris de nombreuses fois. C'est d'ailleurs en cela que les auditions publiques et le rapport sont utiles : souligner les choix précoces de certaines administrations pourrait en conduire d'autres à s'en inspirer pour suivre le même chemin.

En l'espèce, je ne vois pas d'autre solution que celle proposée par la rapporteure, sachant que le tableau indique les chiffres pour l'année 2025 ainsi qu'une moyenne des années précédentes, ce qui permet de constater les évolutions.

Je précise enfin que certains ministères ne connaissent pas avec précision leur nombre d'utilisateurs.

**Mme Cyrielle Chatelain, rapporteure.** La troisième modification concerne le projet Campus IA. Les éléments qui nous ont été fournis par écrit ne me semblaient pas relever du secret des affaires, mais un point a peut-être échappé à ma vigilance. L'opérateur émirien Khazna est pressenti pour réaliser la première tranche du projet, mais l'annonce publique n'a pas encore eu lieu, quand bien même le lien entre cette entreprise et MGX, qui soutient le projet, est connu. C'est à contrecœur que je retirerai cette information, car j'estime qu'elle est d'intérêt public, mais je m'en remettrai à la décision de la commission d'enquête.

**M. le président Philippe Latombe.** Je constate que la commission s'en remet à votre sagesse, madame la rapporteure. J'indique à cet égard, que l'information peut déjà être trouvée en creusant un peu.

**Mme Cyrielle Chatelain, rapporteure.** Dans ce cas, je conserve l'information, étant rappelé que j'indique bien que cet opérateur n'est que pressenti.

**M. le président Philippe Latombe.** J'assumerai juridiquement votre choix !

Je vous remercie, chers collègues, pour ces modifications nécessaires.

*La commission d'enquête **adopte** le rapport.*

**M. le président Philippe Latombe.** Je rappelle que le dépôt du rapport sera publié au *Journal officiel* de demain matin, mais que compte tenu du délai de cinq jours francs que nous impose l'article 144-2 de notre règlement, il ne pourra être publié qu'à partir du mercredi 15 juillet. À ce titre, aucune communication ne pourra être faite sur son contenu jusqu'à cette date. Et je vous prierai de nous remettre les exemplaires qui vous ont été fournis pour cette réunion.

Je remercie l'ensemble des administrateurs et des agents qui nous ont accompagnés.

J'espère que ce rapport sera vivant et que nous discuterons de manière informelle de tous les textes liés à cette commission d'enquête qui nous seront soumis, dans l'optique de déposer des amendements allant dans le sens des recommandations et plus généralement d'éclairer les collègues qui n'ont pas participé à nos travaux. À cet égard, je vous remercie par avance de la publicité que vous ferez du rapport à partir du 15 juillet, afin que l'ensemble de l'écosystème puisse s'en emparer et réagir.

# PERSONNES ENTENDUES PAR LA COMMISSION D'ENQUÊTE

*Les comptes rendus des auditions sont consultables à l'adresse suivante :*

*https://www.assemblee-nationale.fr/dyn/17/organes/autres-commissions/commissions-enquete/ce-vulnerabilites-numeriques/documents?typeDocument=crc*

Les auditions sont présentées dans l'ordre chronologique des réunions de la commission d'enquête.

***Mardi 10 mars 2026***

– M. Henri Verdier, directeur général de la fondation Inria, ancien ambassadeur pour le numérique

– Table ronde réunissant :

- M. David Chavalarias, directeur de recherche au CNRS, directeur au Centre d'analyse et de mathématiques sociales de l'EHESS, et directeur de l'Institut des systèmes complexes de Paris Île-de-France (ISC-PIF)
- M. Robin Berjon, informaticien, directeur de l'agence Supramundane
- Mme Maud Quessard, directrice du domaine « Europe, espace transatlantique, Russie » à l'Institut de recherche stratégique de l'école militaire (Irsem)

***Mardi 17 mars 2026***

– MM. Emmanuel Marcovitch, président de section à la première chambre de la Cour des comptes, conseiller maître, Patrice Huiban, conseiller référendaire et Laurent Zerah, conseiller référendaire en service extraordinaire

– Mme Soizic Pénicaud, cofondatrice de l'Observatoire des algorithmes publics

– M. Laurent Vilboeuf, directeur par intérim de la Plateforme des données de santé (Health Data Hub)

***Mercredi 18 mars 2026***

– M. Dominique Luzeaux, général de division, chargé de mission « transformation numérique » auprès du commandant suprême allié pour la transformation de l'Otan

– Mme Catherine Mayenobe, directrice générale déléguée de la Caisse des dépôts, directrice des opérations et du pilotage de la transformation opérationnelle, M. Arnaud Martin, directeur des risques opérationnels, M. Patrick Laurens-Frings, directeur de la transformation opérationnelle, digitale et des systèmes d'information du groupe, et M. Philippe Blanchot, directeur des relations institutionnelles, internationales et européennes

***Mercredi 25 mars 2026***

– Table ronde réunissant des associations sur le thème de la protection des données personnelles :

- La Quadrature du net * : M. Bastien Le Querrec, juriste
- Amnesty International * : Mme Katia Roux, chargée de plaidoyer
- Ligue des droits de l'homme : Mme Maryse Artiguelong, coresponsable du groupe de travail « Libertés et technologies de l'information et de la communication » et M. Pierrick Clément, avocat

– Mme Meredith Whittaker, présidente de la fondation Signal

***Jeudi 26 mars 2026***

– M. Aiman Ezzat, directeur général de CapGemini, et Mme Karine Brunet, directrice mondiale des opérations et du delivery et membre du comité de direction générale du groupe

– M. Martin Untersinger, journaliste au Monde, et MM. Antoine Schirer et Sébastien Bourdon, journalistes indépendants

– M. Max Schrems, fondateur de l'association NOYB (None of your business)

– Collectif Eurostack représenté par Mme Cristina Caffarra, économiste, spécialiste de la concurrence et de la régulation des plateformes numériques et M. Yann Lechelle, entrepreneur, président-directeur général de probabl.ai

***Mardi 31 mars 2026***

– Mme Mélanie Dulong de Rosnay, directrice de recherche au Centre national de la recherche scientifique (CNRS), co-fondatrice du Centre internet et société (CIS) du CNRS, et Mme Ramya Chandrasekhar, chercheuse au CIS

***Mercredi 1er avril 2026***

– Table ronde sur la protection des données personnelles :

- Mme Nataliia Bielova, directrice de recherche au centre Inria de l'université Côte d'Azur
- M. Julien Rossi, maître de conférences en sciences de l'information et de la communication à l'UFR Culture et communication et au Centre d'études sur les médias, les technologies et l'internationalisation (Cémti) de l'université Paris 8

– Table ronde réunissant des directeurs des systèmes d'information d'organismes de recherche :

- CNRS : Mme Marie-Pierre Fontanel, directrice des systèmes d'information, et M. Thomas Borel, responsable des affaires publiques

- Commissariat à l'énergie atomique et aux énergies alternatives (CEA) * : M. Baptiste Grigy, directeur des systèmes d'information

- Institut national de recherche pour l'agriculture, l'alimentation et l'environnement (Inrae) : M. Louis-Augustin Julien, directeur général délégué ressources, et M. Jean-Michel Vansteene, directeur des systèmes d'information

- Institut national de la santé et de la recherche médicale (Inserm) : M. Damien Rousset, directeur général délégué à l'administration, et M. Sammy Sahnoune, directeur des systèmes d'information

***Jeudi 2 avril 2026***

– Table ronde sur les infrastructures numériques, réunissant :

- Mme Ophélie Coelho, chercheuse associée à l'Institut des relations internationales et stratégiques (Iris) *, doctorante au CIS et au centre d'analyse et de recherche interdisciplinaires sur les médias (Carism-Paris-Assas)

- Data for Good : Mme Lou Welgryn, secrétaire générale, et Mme Alexandra Lutz, chargée de plaidoyer

- Mme Francesca Musiani, directrice de recherche au CNRS, co-fondatrice et directrice du CIS

– M. Bernard Benhamou, secrétaire général de l'Institut de la souveraineté numérique

***Mardi 7 avril 2026***

– M. Michel Paulin, président du comité stratégique de filière « solutions numériques de confiance » du Conseil national de l'industrie, ancien directeur général d'OVH, et Mme Julia Mouzon, déléguée permanente du comité stratégique de la filière logiciels et solutions numériques de confiance du Conseil national de l'industrie

***Mercredi 8 avril 2026***

– M. Nicolas Guillou, juge à la Cour pénale internationale

– Table ronde sur les services de paiement :

- Mme Maya Atig, directrice générale de la Fédération bancaire française (FBF) *, et M. Jérôme Raguénès, directeur numérique et moyens de paiement

- M. Erick Lacourrège, directeur général des moyens de paiements de la Banque de France, et M. Olivier Fliche, directeur du pôle Fintech-Innovation de l'Autorité de contrôle prudentiel et de résolution (ACPR) *

- Mme Martina Weimert, directrice générale de European Payments Initiative/Wero

- M. Philippe Laulanie, directeur général du Groupement des cartes bancaires (GIE CB)

***Jeudi 9 avril 2026***

– Table ronde sur les acheteurs publics, réunissant :

- M. Edward Jossa, président de l'Union des groupements d'achats publics (Ugap) *
- M. Thomas Jan, directeur général adjoint en charge de l'innovation et de la stratégie numérique de l'Union des hôpitaux pour les achats (UniHa)
- MM. Lionel Schweitzer et Jean-Christophe Thorel, administrateurs de la Centrale d'achat du numérique et des télécoms (Canut)

– Table ronde réunissant des directeurs de systèmes d'information de ministères :

- M. Audran Le Baron, directeur du numérique pour l'éducation au ministère de l'éducation nationale
- M. Mathieu Weill, directeur de la transformation numérique du ministère de l'intérieur
- M. Yves Billon, chef du service du numérique au secrétariat général des ministères économiques et financiers

***Mardi 14 avril 2026***

– Mme Stéphanie Schaer, directrice interministérielle du numérique, et M. Jérémie Vallet, son adjoint

***Mercredi 15 avril 2026***

– M. Thierry Breton, ancien commissaire européen au Marché intérieur, ancien président-directeur général d'Atos SE

– Mme Marie-Laure Denis, présidente de la Commission nationale de l'informatique et des libertés (Cnil), M. Thomas Dautieu, directeur de l'accompagnement juridique, et M. Florent Della Valle, chef du service de l'expertise technologique

***Jeudi 16 avril 2026***

– Mme Christel Heydemann, directrice générale du groupe Orange *

– Mme Maya Noël, directrice générale de France Digitale *

***Mardi 21 avril 2026***

– M. Arnaud Caudoux, directeur général adjoint de Bpifrance, M. Lionel Chaine, directeur des systèmes d'information, et Mme Sophie Rémont, directrice en charge de l'expertise et des programmes au sein de la direction de l'innovation

– Table ronde réunissant des fournisseurs de cloud :

- M. Sébastien Lescop, directeur général de Cloud Temple *
- M. Eric Haddad, président exécutif de NumSpot *
- MM. Philippe Miltin, directeur général d'Outscale Dassault Systèmes *, et David Chassan, directeur de la stratégie
- M. Octave Klaba, président-directeur général d'OVHcloud *, et Mme Solange Viegas Dos Reis, directrice juridique
- M. Damien Lucas, directeur général de Scaleway

***Mercredi 29 avril 2026***

– Le collectif #Fab8, représenté par M. Antoine Duboscq, président de Wimi, M. Thomas Fauré, président de Whaller, et M. Alain Garnier, président de Jamespot

– Mme Hela Ghariani, directrice de la Plateforme des données de santé (Health Data Hub)

– Audition conjointe de :

- MM. Laurent Choukroun, directeur général d'Oreus, et Julien Lescoulié, directeur technique
- M. Charles-Antoine Beyney, directeur général de DataOne

***Jeudi 30 avril 2026***

– M. Vincent Strubel, directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi)

– M. Henri d'Agrain, délégué général du Club informatique des grandes entreprises françaises (Cigref) *

***Mardi 5 mai 2026***

– M. Umberto Berkani, rapporteur général de l'Autorité de la concurrence et M. Julien Neto, rapporteur général adjoint

***Mercredi 6 mai 2026***

– Table ronde sur le logiciel libre réunissant :

- M. Renaud Chaput, directeur technique de Mastodon
- MM. Loïc Dayot, membre du conseil d'administration de l'April *, et Étienne Gonnu, chargé de plaidoyer
- M. Pierre-Yves Gosset, coordinateur des services numériques de Framasoft
- M. Nicolas Vivant, fondateur de France Numérique libre, directeur de la stratégie et de la culture numériques de la commune d'Echirolles

***Jeudi 7 mai 2026***

– Audition commune de :

- M. Tomasz Blanc, chef du service des systèmes d'information de la direction générale des finances publiques (DGFIP)

- Général Marc Boget, directeur de l'agence du numérique des forces de sécurité intérieure (ANFSI)

– Audition commune de :

- M. Benjamin Delozier, chef du service des politiques écologiques et sectorielles à la direction générale du Trésor, et M. Victor Amoureux, chef du bureau concurrence, numérique, économie du logement

- MM. Thomas Courbe, directeur général des entreprises (DGE), et Loïc Duflot, chef de service de l'économie numérique de la DGE

- M. Florent Kirchner, directeur du pôle souveraineté numérique au Secrétariat général pour l'investissement (SGPI)

– M. Luca Belli, professeur de gouvernance et régulation numériques à la fondation Getulio Vargas de Rio de Janeiro

***Mardi 12 mai 2026***

– M. Arthur Mensch, cofondateur et directeur général de Mistral AI *, et Mme Audrey Herblin-Stoop, directrice des affaires publiques et de la communication

– M. Fabrice Coquio, président-directeur général de Digital Realty *

***Mercredi 13 mai 2026***

– Table ronde réunissant des représentants en France des Gafam :

- Mme Corine de Bilbao, présidente de Microsoft France *, et M. Philippe Limantour, directeur technologie et cybersécurité

- M. Sébastien Missoffe, directeur général de Google France * et M. Frédéric Geraud de Lescazes, directeur des affaires publiques de Google Cloud

- M. Julien Lépine, représentant en France d'Amazon Web Services Europe, Moyen-Orient, Afrique (AWS EMEA *), et M. Arnaud David, directeur des affaires publiques France et Union européenne de AWS

– M. Cédric O, ancien secrétaire d'État chargé du numérique

***Mercredi 20 mai 2026***

– Audition commune de :

- M. David Amiel, ministre de l'action et des comptes publics

- Mme Anne Le Hénanff, ministre déléguée auprès du ministre de l'économie, des finances et de la souveraineté industrielle, énergétique et numérique, chargée de l'intelligence artificielle et du numérique

** Ces représentants d'intérêts ont procédé à leur inscription sur le registre de la Haute Autorité pour la transparence de la vie publique.*

# PERSONNES RENCONTRÉES À BRUXELLES PAR LE PRÉSIDENT ET LA RAPPORTEURE

Lundi 20 avril 2026

**Commission européenne, direction générale des réseaux de communication, du contenu et des technologies**

– M. Thibaut Kleiner, directeur chargé des réseaux du futur

– M. Ivo Volman, directeur chargé des données

**Représentation permanente de la France auprès de l'Union européenne**

– M. Cyril Piquemal, représentant permanent adjoint

– Mme Marie-Léa Rols, conseillère télécommunications, numérique et postes

– Mme Marie Dugré, conseillère, adjointe du chef de service justice et affaires intérieures

**European Digital Rights (EDRI)**

– M. Jan Penfrat, conseiller principal

– M. Siméon De Brouwer, conseiller

**Contrôleur européen de la protection des données**

– M. Leonardo Cervera Navas, secrétaire général

– M. Brendan Van Alsenoy, responsable de l'unité « politiques et consultation »

– Mme Fanny Coudert, cheffe d'unité, supervision et application de la réglementation

**Bureau européen de la protection des données**

– Mme Anu Talus, présidente

– Mme Isabelle Vereecken, cheffe du secrétariat

**Commission européenne, cabinet de Mme Henna Virkkunen, vice-présidente exécutive chargée de la souveraineté technologique, sécurité et démocratie**

– M. Xavier Coget, membre du cabinet en charge des questions diplomatiques, des affaires extérieures, de la compétitivité et des start-ups

– M. Benjamin Bögel, membre du cabinet responsable de la politique de cybersécurité de l'Union

**Parlement européen**

– Mme Alexandra Geese, députée européenne, membre de la commission de l'industrie, de la recherche et de l'énergie, rapporteure sur la souveraineté technologique européenne et les infrastructures numériques

# CONTRIBUTIONS DES GROUPES POLITIQUES ET DES DÉPUTÉS

## CONTRIBUTION DE M. PHILIPPE LATOMBE, PRÉSIDENT DE LA COMMISSION D'ENQUÊTE ET DÉPUTÉ DE VENDÉE

Les travaux de la commission d'enquête sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France sont venus valider les analyses qui sont les miennes depuis plus de six ans. Je retrouve donc dans les préconisations qui en sont issues un certain nombre de propositions que j'ai déjà eu l'occasion de promouvoir à de nombreuses occasions, tant dans mes écrits (rapport sur la souveraineté numérique, questions orales et écrites, articles, tribunes) que dans mes prises de parole publiques, au sein de colloques et de tables rondes.
Je prendrai pour exemple la création d'un ministère de plein exercice avec des compétences transversales, permettant de lutter contre le développement en silos de l'architecture numérique de l'État et d'élaborer une véritable stratégie pour un secteur, le numérique, qui est maintenant indissociable de toutes les activités humaines.
Je me suis aussi à maintes reprises exprimé sur la nécessité d'une DINUM recentrée sur son cœur de métier (qui ne s'éparpille pas à concurrencer le secteur privé par exemple), mais aussi dotée de moyens plus importants pour remplir sa mission de base.
J'appelle de mes vœux depuis longtemps la mise en œuvre d'un Buy European Act, afin que nous puissions, en Europe, être en position de force pour défendre notre économie et booster nos entreprises face à une concurrence souvent déloyale des autres puissances économiques qui, elles, pratiquent depuis toujours la préférence nationale, dans leurs achats publics.
Je suis aussi favorable à toutes les mesures de protection face aux législations extra-européennes, et ce, à tous les niveaux et pour toutes les technologies critiques.

Enfin, je suis d'accord sur une nécessaire modernisation de la protection des données personnelles, dans la continuité des valeurs qui sont les nôtres (respect de la vie privée, protection des droits et libertés, transparence, limitation des finalités, minimisation des données, exactitude et durée de conservation limitée, sécurité, responsabilisation), qui ont été initiées par le RGPD.

Il serait par ailleurs prudent de créer des ambassades de données (et d'ainsi stocker des copies de nos données gouvernementales critiques, dans des serveurs situés à l'étranger, tout en conservant leur protection juridique. L'objectif serait d'assurer la continuité de l'État en cas de catastrophe, de cyberattaque ou de conflit. L'Estonie, par exemple, a mis en place une ambassade de données au Luxembourg pour sécuriser certaines de ses données nationales. L'Ukraine, elle, a adopté une approche distribuée : la Pologne a été le premier pays à héberger des copies de registres gouvernementaux et de données critiques de l'État ukrainien dans une infrastructure cloud sécurisée située sur son territoire. Des discussions et des coopérations ont ensuite été engagées avec l'Estonie et la France pour accueillir d'autres données stratégiques et renforcer la résilience numérique de l'Ukraine. L'Estonie dirige également un important programme européen visant à renforcer la cybersécurité et la sécurité des données des administrations ukrainiennes. Nous pourrions nous aussi accueillir des ambassades de données étrangères. Il s'agirait là pour la France de se positionner dans le cadre d'une diplomatie du numérique qui est en train de se constituer.

Enfin, la perspective d'un moratoire sur l'implantation de nouveaux centres de données (data centers) sur le territoire national, proposé par la rapporteure, me semble une mauvaise idée. Il nous faut trouver un « point de patinage » entre les investissements directs étrangers et la

conservation d'une partie substantielle de la puissance de calcul. Un data center de grosse taille représente un investissement de plusieurs dizaines de milliards de dollars que nous ne pouvons envisager sans attirer des capitaux étrangers. Il nous faut aussi garder la main sur l'atout concurrentiel que représente une électricité décarbonée, stable, abondante et bon marché, issue de notre parc nucléaire, sur cet héritage industriel collectif qui nous permet de peser en Europe et dans le monde, et donc trouver un point d'équilibre. Ce pourrait se faire à l'image de ce que les Chinois ont mis en pratique dans la dernière décennie du siècle dernier, en accueillant les IDE dans le cadre de joint-ventures qu'ils contrôlaient, en y étant majoritaires.

Apprenons de nos erreurs passées et n'hésitons pas à nous inspirer de ce qui a particulièrement bien fonctionné sous d'autres cieux.

## CONTRIBUTION DU GROUPE RASSEMBLEMENT NATIONAL

# Contribution du Rassemblement National

Les députés du Rassemblement National remercient les services pour l'organisation et le bon déroulement des auditions, ainsi que l'ensemble des personnes entendues pour la qualité de leurs contributions.

Le secteur du numérique français et européen souffre d'une dépendance structurelle à des solutions extra-européennes, notamment avec les solutions américaines, pour ses logiciels et ses infrastructures les plus critiques. Alors que le numérique est désormais indispensable à la vie des citoyens, au fonctionnement des entreprises et à la continuité de nombreux services publics, cette dépendance relève d'un véritable danger pour notre souveraineté.

En matière de données personnelles, les États-Unis disposent d'un puissant arsenal juridique (le Cloud Act et le FISA). Il autorise leurs autorités à accéder aux données hébergées par des acteurs soumis à leur juridiction, y compris lorsque ces données sont stockées en Europe. La Chine dispose d'un mécanisme similaire avec la loi sur le renseignement national de 2017, qui contraint toute entreprise à coopérer avec les services de renseignement de l'État.

Cette dépendance se matérialise notamment par la présence des grands éditeurs américains, tels que Microsoft, au sein des administrations publiques et des ministères. Si les applications métiers reposent majoritairement sur des fournisseurs français, celles-ci demeurent vulnérables par le recours à des logiciels américains sous-jacents et par l'hébergement d'applications critiques chez des prestataires américains. Jusqu'à une période récente, le Health Data Hub était hébergé sur Microsoft Azure : pendant de nombreuses années, des données de santé, par nature critiques et vulnérables, ont ainsi été hébergées par un acteur américain.

Plus largement, cette dépendance expose la France au risque des ingérences étrangères. En cas de tensions internationales, les États-Unis disposent d'un moyen de pression considérable : la menace de couper l'accès à leurs services numériques et à leurs réseaux de paiement. Ce levier place la France en position de faiblesse. Sur le plan économique, les entreprises se trouveraient exposées à une paralysie brutale, sans alternative immédiate. Dans la vie quotidienne, l'accès aux moyens de paiement, aux services en ligne et aux outils numériques devenus indispensables pourrait être suspendu, avec des conséquences directes et immédiates pour des millions de Français. Les domaines critiques et sensibles peuvent également être frappés, à l'image du secteur de la santé, dont les hôpitaux dépendent de solutions étrangères. Il est inacceptable que la souveraineté de la France sur des fonctions aussi essentielles puisse dépendre du bon vouloir d'un acteur extérieur.

Alors que les menaces informatiques étrangères sont pleinement identifiées, le Rassemblement National a déploré qu'une administration aussi stratégique que Bercy ait pu expérimenter, au sein de ses services, un outil reposant sur une intelligence artificielle chinoise. Ce n'est qu'à la suite de cet incident qu'un modèle de la société française Mistral AI a pris le relais. Le Rassemblement National se félicite de ce choix, mais déplore qu'il n'ait été fait qu'après coup, une fois le risque avéré. L'exemplarité de l'État commande de privilégier d'emblée les solutions souveraines, et non de n'y recourir qu'en réaction à un incident. Plus largement, le déploiement de l'intelligence artificielle dans les administrations ne saurait se faire au prix d'une nouvelle perte de maîtrise technique et économique, à l'image du quasi-monopole des moteurs de recherche américains.

Les GAFAM acquittent un niveau d'impôt manifestement sans rapport avec leur activité réelle en France, ce que confirme ce rapport. La faible valeur ajoutée déclarée sur le territoire national se traduit par des recettes fiscales minimes.

Le développement des data centers constitue un enjeu de souveraineté à part entière qui ne doivent pas être uniquement portés par des hyperscalers américains et des investisseurs internationaux. L'IA agentique désigne une nouvelle génération de systèmes capables de planifier, décider et agir de manière autonome pour atteindre des objectifs complexes, au-delà

de la simple exécution d'instructions isolées. Le rapport situe le marché anticipé à un niveau considérable et pointe la consommation électrique de ces technologies. Or, grâce à notre mix énergétique, cette consommation, quoique élevée, peut être satisfaite par le nucléaire, une énergie propre, décarbonée et abordable. Cet outil allégera les agents des tâches chronophages pour qu'ils se concentrent vers missions moins ingrates et à plus forte valeur ajoutée, contrairement à ce qu'affirme la rapporteure.

La rapporteure retient l'open source parmi les alternatives aux solutions propriétaires étrangères. Le Rassemblement partage l'intérêt pour le logiciel libre, dont l'Agence nationale de la sécurité des systèmes d'information reconnaît les avantages en matière de transparence et de maîtrise des environnements numériques. Un code intégralement ouvert peut être repris, audité, modifié et opéré par n'importe quel prestataire compétent, ce qui écarte le risque d'être prisonnier d'une solution. Cependant, la souveraineté ne réside pas dans la localisation d'un siège social, mais dans la capacité à ne jamais dépendre captivement d'une solution technique. Or la France est exemplaire dans le partage de code au sein du secteur public, mais bien plus faible en matière de politique industrielle : entre 80 % et 90 % des logiciels contiennent aujourd'hui du code open source, mais la valeur qui en découle est trop souvent captée par des entreprises étrangères. Sans opérateur français capable de déployer et de maintenir ces solutions à l'échelle de nos grandes administrations, l'ouverture du code profite parfois davantage à nos concurrents qu'à notre industrie.

Alors que l'Union européenne multiplie les normes, que la France surtranspose trop souvent, les autres pôles avancent. L'excès de réglementation ne saurait tenir lieu de politique industrielle, et la surtransposition ne fait qu'aggraver notre décrochage face aux grandes puissances numériques.

Le Rassemblement National, sous l'autorité de Marine le Pen et de Jordan Bardella, appelle à tirer toutes les conséquences : la souveraineté numérique ne se décrète pas, elle se construit par une politique industrielle volontariste, par l'exemplarité sans faille de l'État dans ses propres choix technologiques, et par le refus catégorique de troquer une dépendance étrangère contre une autre. Une stratégie adossée à des filières souveraines dotées d'une véritable masse critique, un financement pérenne et une gouvernance interministérielle enfin unifiée sont les premières briques d'une reconquête stratégique et souveraine.

# ANNEXE N° 1 :
# LISTE DES ENTITÉS AYANT RÉPONDU À UN QUESTIONNAIRE ÉCRIT DE LA RAPPORTEURE

## I. QUESTIONNAIRE SUR LES ACHATS NUMÉRIQUES ET LE STOCKAGE DES DONNÉES DES ADMINISTRATIONS DE L'ETAT

– Direction interministérielle du numérique

– Commissariat au numérique de défense

– Direction du numérique pour l'éducation

– Direction générale de l'enseignement supérieur et de l'insertion professionnelle

– Service du numérique des ministères économiques et financiers

– Direction de la transformation numérique du ministère de l'intérieur

– Direction générale de la gendarmerie nationale

– Direction générale de la police nationale

– Directeur du numérique du ministère de la justice

– Direction du numérique du ministère de l'Europe et des affaires étrangères

– Direction du numérique du ministère de la transition écologique

– Service du numérique du ministère de l'agriculture, de l'agro-alimentaire et de la souveraineté alimentaire

– Direction du numérique des ministères chargés des affaires sociales

– Direction numérique du ministère de la culture

## II. QUESTIONNAIRE SUR LES ACHATS NUMÉRIQUES ET LE STOCKAGE DES DONNÉES DES ADMINISTRATIONS DE PROTECTION SOCIALE

– Caisse nationale de l'assurance maladie (Cnam)

– Caisse nationale des allocations familiales (Cnaf)

– Caisse nationale d'assurance vieillesse (Cnav)

– Assistance publique-hôpitaux de Paris (AP-HP)

– France Travail

## III. QUESTIONNAIRE SUR LES ACHATS NUMÉRIQUES ET LE STOCKAGE DES DONNÉES DES OPÉRATEURS D'IMPORTANCE VITALE (OIV)

– ADP

– EDF

– Enedis

– NaTran (ex GRTgaz)

– RATP

– RTE

– SNCF Réseau

– Storengy France

– Veolia

## IV. AUTRES QUESTIONNAIRES ÉCRITS

– Ambassade de France en Allemagne

– Commission nationale de l'informatique et des libertés (Cnil)

– Direction générale des entreprises

– Direction générale des finances publiques

– Direction générale du Trésor

– Institut national de la statistique et des études économiques (Insee)

– Préfecture de la région d'Île-de-France

– Union des groupements d'achats publics (Ugap)

# ANNEXE N° 2 :
# QUESTIONNAIRE ADRESSÉ PAR LA RAPPORTEURE AUX ADMINISTRATIONS DE L'ÉTAT

ASSEMBLÉE NATIONALE

COMMISSION D'ENQUETE SUR LES DEPENDANCES STRUCTURELLES ET LES VULNERABILITES SYSTEMIQUES DANS LE SECTEUR DU NUMERIQUE ET LES RISQUES POUR L'INDEPENDANCE DE LA FRANCE

RÉPUBLIQUE FRANÇAISE
LIBERTÉ–ÉGALITÉ–FRATERNITÉ

**Questionnaire de Mme Cyrielle Chatelain, rapporteure, sur les achats et usages numériques des ministères**

La commission d'enquête visant à identifier les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique examinera en particulier la vulnérabilité des administrations publiques vis-à-vis de technologies et d'infrastructures digitales développées ou opérées par des acteurs extra-européens.

A ce titre, le présent questionnaire, adressé aux ministères et aux grandes entreprises publiques assurant des services publics vitaux, a pour objet de disposer d'éléments chiffrés sur l'ensemble des achats de votre ministère dans le domaine du numérique et de mesurer la prise en compte des sujets de vulnérabilité, de dépendance à des technologies clés et de protection des données sensibles.

Les réponses au questionnaire sont attendues au plus tard le 10 avril 2026.

A la suite de la réception du questionnaire complété, une table ronde réunissant un panel d'entités publiques sera organisée, durant laquelle les réponses reçues sont analysées et commentées.

## I. Déploiement des outils SI au sein du ministère : état des lieux des applications et fournisseurs principaux

### A. Logiciels et services support

1. Remplir l'onglet « Logiciels support » du fichier Excel associé.

2. Pour les achats de logiciels et licences destinés aux services supports :
   - Quels sont les outils de contractualisation : appels d'offres, contrats cadres, etc.
   - Quels sont les critères d'arbitrage : coût, qualité, résilience
   - Quelles sont les raisons qui expliquent le choix ou non de solutions :
     - open source
     - françaises ou européennes
     - développées par l'Etat

3. Comment est assurée la gestion du SI : est-elle réalisée en interne ou bien via une infogérance ? Quelles sont les dépenses associées, et les fournisseurs correspondant ?

### B. Logiciels métiers

4. Quels sont les enjeux principaux concernant le déploiement des outils SI dans votre entité ? Quelles ont été les principales tendances observées au cours des 5 dernières années ? Quelles évolutions prévoyez-vous pour les 5 prochaines années ?

5. Remplir l'onglet « Logiciels métier » du fichier Excel associé. Il est requis de fournir les informations pour les applications remplissant les critères suivants :
   - Applications dont le défaut est susceptible d'engendrer une atteinte à l'ordre public, à la sécurité publique, ou à la vie des personnes
   - Applications dont le défaut est susceptible d'engendrer l'interruption de l'exercice d'une mission de service public essentielle

6. Réalisez-vous des développements en interne pour les applications métier ? Si oui, avec quelles ressources humaines, techniques et financières ? Quelle part représentent les développements en interne dans votre parc d'applications ?

7. Quels sont les outils de contractualisation mis en œuvre : contrats-cadre, appel d'offres ? Quelle sont vos procédures de qualification pour les prestataires en charge de l'élaboration de vos applications métier ? Quels sont les critères d'arbitrage : références techniques du prestataire, coût, qualité, résilience ? Comment vous assurez-vous que les PME et ETI puissent passer les critères d'éligibilité ?

8. Innovation et qualité : quels sont les enjeux de votre domaine ? quelle est votre appréciation de l'offre française sur la qualité de l'offre fournie (différenciation technique, service support, etc.) ?

9. Compétitivité coût : quelle est votre appréciation de l'offre française ? existe-t-il des différences importantes entre les acteurs ? Comment arbitrez-vous entre les coûts de développement initiaux/coûts de licence et coûts de MCO ?

### C. Services cloud

10. Remplir l'onglet « Cloud » du fichier Excel associé.

11. Sollicitez-vous des services de cloud commercial ne répondant pas à la qualification SecNumCloud pour des données présentant un caractère personnel ou des données d'une sensibilité particulière (au sens de la circulaire « Cloud au centre » du 31 mai 2023) ? Si oui, pouvez-vous justifier les choix effectués ?

12. Quel est le surcoût constaté des solutions répondant à la qualification SecNumCloud par rapport aux solutions commerciales classiques ? Même question pour les cloud d'Etat Nubo et Pi, si ces clouds sont utilisés par votre ministère ?

13. Quels sont les services que vous jugez nécessaires et qui ne sont pas fournis par les opérateurs répondant à la qualification SecNumCloud ?

### D. Outils d'IA

14. Remplir l'onglet « Outils IA » du fichier Excel associé.

## II. Dépendances et stratégies techniques visant à assurer la résilience des systèmes informatiques de l'entité

15. Avez-vous élaboré une cartographie des dépendances vis-à-vis de vos fournisseurs clés et acteurs non européens ?

16. Avez-vous élaboré une cartographie des process clés gérés par votre ministère et des plans de résilience associés ? Quelles sont les dépendances non substituables à un horizon cout terme (inférieur à 3 ans) ?

17. Quelles stratégies mettez-vous en œuvre limiter les dépendances et vulnérabilités du SI du ministère :
    - Diversification du portefeuille de fournisseurs, procédures de qualification
    - Stratégies contractuelles : propriété des logiciels et/ou des codes sources, etc.
    - Stratégies techniques : utilisation de l'open source, développement de solutions conteneurisées (dockérisation, kubernetes, etc.)

## III. Stratégies de déploiement des systèmes informatiques et gouvernance

18. Quels sont vos effectifs dédiés à la gestion des SI. Quelle est la part des fonctionnaires et des contractuels ? Avec combien de prestataires à temps plein contractualisez-vous ?

19. Existe-t-il un organe chargé des règles déontologiques en matière de SI (protection des données personnelles, définition des algorithmes, etc.) ?

20. Quelles sont vos interactions avec la DINUM et les autres entités prescriptrices de l'Etat :
    - Niveau de support fourni et nature des échanges
    - Adéquation des recommandations aux besoins

21. Quelle est votre appréciation des services et logiciels fournis en interne par l'Etat
    - Développement des outils logiciels par la DINUM : adéquation aux besoins, rapidité de développement, qualité du service support
    - Développement des outils logiciels par d'autres entités de l'Etat

22. Quelle est votre appréciation des services fournis par l'UGAP en matière d'achats de logiciels et services numériques :
    - Adéquation du portefeuille à vos besoins
    - Compétitivité des prix proposés par rapport aux prix qui pourraient être obtenus dans le cadre d'appels d'offres organisés directement en propre

23. Quelles sont vos interactions avec la DGE et les autres entités en charge de la politique industrielle :
    - Echanges sur les besoins clés et les entreprises présentant les plus avancées technologiquement
    - Participation aux comités de sélection
    - Eventuellement contribution aux financements via prises de participation ou autres moyens (facilitation d'accès à des contrats cadres, etc.)

## ANNEXE N° 3 : LISTE DES SIGLES ET ACRONYMES

- ACPR : Autorité de contrôle prudentiel et de résolution
- Ademe : Agence de la transition écologique
- AIFE : Agence pour l'informatique financière de l'État
- Anfsi : Agence du numérique des forces de sécurité intérieure
- Anssi : Agence nationale de la sécurité des systèmes d'information
- ANTS : Agence nationale des titres sécurisés
- Arcep : Autorité de régulation des communications électroniques, des postes et de la distribution de la presse.AE : autorisation d'engagement
- Arcom : Autorité de régulation de la communication audiovisuelle et numérique
- ASP : Agence de services et de paiement
- CASD : Centre d'accès sécurisé aux données
- CEA : Commissariat à l'énergie atomique et aux énergies alternatives
- CEPD : Comité européen de la protection des données
- CGE : Conseil général de l'économie
- Cigref : Club informatique des grandes entreprises françaises
- Cisirh : centre interministériel de services informatiques relatifs aux ressources humaines
- CJUE : Cour de justice de l'Union européenne
- Cnaf : Caisse nationale des allocations familiales
- Cnam : Caisse nationale de l'assurance maladie
- Cnav : Caisse nationale d'assurance vieillesse
- Cnil : Commission nationale de l'informatique et des libertés
- CNMP : Comité national des moyens de paiement
- CNRS : Centre national de la recherche scientifique
- CPI : Cour pénale internationale
- CSF : comité stratégique de filière
- DAE : direction des achats de l'État
- DGCCRF : direction générale de la concurrence, de la consommation et de la répression des fraudes
- DGDDI : direction générale des douanes et droits indirects
- DGFIP : direction générale des finances publiques
- DITP : direction interministérielle de la transformation publique
- DPC : Data Protection Commission
- DPF : *Data Privacy Framework*
- DPRC : Data Protection Review Court
- Dinsic : direction interministérielle du numérique et du système d'information et de communication de l'État
- Dinum : direction interministérielle du numérique
- Drees : direction de la recherche, des études, de l'évaluation et des statistiques
- DSI : direction des systèmes d'information
- Edic : Consortium pour une infrastructure numérique européenne
- ESN : entreprise de services du numérique
- ETP : équivalent temps plein
- FBF : Fédération bancaire française
- HATVP : Haute autorité pour la transparence de la vie publique
- HDS : hébergeur de données de santé
- IGF : Inspection générale des finances

- Inserm : Institut national de la santé et de la recherche médicale
- Inrae : Institut national de recherche pour l'agriculture, l'alimentation et l'environnement
- Iris : Institut de relations internationales et stratégiques
- IRN : indice de résilience numérique
- MEAE : ministère de l'Europe et des affaires étrangères
- OFAC : Office of Foreign Assets Control
- OIV : opérateur d'importance vitale
- PDS : Plateforme des données de santé
- SNDS : système national des données de santé
- RGPD : règlement général sur la protection des données
- RTE : Réseau de transport d'électricité
- TFUE : Traité sur le fonctionnement de l'Union européenne
- Ugap : Union des groupements d'achats publics
- Viginum : service de vigilance et de protection contre les ingérences numériques étrangères