

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 dans le secteur du numérique et les risques pour l'indépendance de la France est composée de : M. Philippe Latombe, président ; Mme Cyrielle Chatelain, M. Édouard Bénard ; M. Nicolas Bonnet ; M. Éric Bothorel ; M. Jérôme Gosselin ; M. Sacha Houlié ; M. Arnaud Le Gall ; M. Aurélien Lopez-Liger (25 avril 2026) ; M. Paul Midy ; Mme Laure Miller ; Mme Josy Poueyto ; Mme Sophia Chikirou ; Mme Virginie Duby-Muller ; M. Thomas Gassilloud ; M. Arnaud Saint-Martin ; M. Emeric Salmon ; M. Hervé Saulignac ; M. THOMAS RAMBAUD ; Mme Isabelle Rauch ; Mme Sophie-Laurence Roy ; M. Alexandre RAMBAUD ; M. Aurélien Taché ; M. Vincent Thiébaut ; Mme Mélanie Thomin.

- ▶ 5. Le verrouillage des utilisateurs : une pratique au cœur des stratégies des fournisseurs de logiciels
- ▶ 6. Les vulnérabilités liées aux infrastructures et aux composants clés
- ▶ C. LE PÉRIMÈTRE DE LA COMMISSION D'ENQUÊTE
- ▶ **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 JUSTIFIE UN TRAITEMENT PARTICULIER
 - ▶ 1. Objectifs
 - ▶ 2. Plan de travail
 - ▶ B. LES DÉPENDANCES SYSTÉMIQUES : UNE APPROCHE GLOBALE
 - ▶ 1. Objectifs
 - ▶ 2. Plan de travail

▶ **PREMIÈRE PARTIE : LE DIAGNOSTIC**

- ▶ **CHAPITRE 1 – MICROSOFT, VMWARE, ORACLE, CES TROIS LOGICIELS QUI NOUS GOUVERNENT – LES DÉPENDANCES DES ADMINISTRATIONS AUX SOLUTIONS AMÉRICAINES**
 - ▶ A. LES APPLICATIONS MÉTIERS : LE RECOURS PRINCIPALEMENT AUX SOLUTIONS DES FOURNISSEURS FRANÇAIS, DES VULNÉRABILITÉS LIÉES À CERTAINS MINISTÈRES
 - ▶ 1. Données sources
 - ▶ 2. Modes de développement des applications métiers : la prédominance des logiciels spécifiques
 - ▶ 3. Dépendances à des fournisseurs extra-européens
 - ▶ B. LOGICIELS SUPPORTS : LA DÉPENDANCE À TROIS ACTEURS AMÉRICAINS, MICROSOFT, ORACLE ET VMWARE
 - ▶ 1. Dépendance généralisée aux outils Microsoft : systèmes d'exploitation, suite bureautique Office 365
 - ▶ 2. Dépendance structurelle aux outils Oracle (gestion des bases de données), VMWare (virtualisation) et dans une moindre mesure IBM et Red Hat
 - ▶ 3. État du déploiement des solutions open source au sein des administrations : l'exemple à suivre de la gendarmerie nationale, les transitions programmées engagées par d'autres ministères
 - ▶ C. VULNÉRABILITÉ DES DONNÉES ET DÉPENDANCES DES INFRASTRUCTURES DE STOCKAGE
 - ▶ 1. Un impératif de protection des données sensibles formalisé par la loi sur le Cloud au centre de l'État
 - ▶ 2. Un hébergement en interne largement privilégié
 - ▶ a. Une forte maîtrise de l'hébergement des systèmes d'information dans le périmètre régalien
 - ▶ b. Un hébergement majoritairement interne pour les ministères et les infrastructures historiques
 - ▶ c. Un recours plus fréquent aux offres de cloud commercial parmi les

- ▶ 4. L'utilisation préoccupante et systématique de clouds extra-européens
- ▶ B. LES ENTREPRISES PRIVÉES : UNE PRISE EN C
BALBUTIANTE, PAS D'ACTIONS CONCRÈTES
- ▶ C. LE CAS PARTICULIER DU SECTEUR BANCAIRE ET DES OUTILS DE
PAIEMENT
 - ▶ 1. La détection de la dépendance à des fournisseurs critiques de tech
numériques imposée par le règlement Dora
 - ▶ 2. La souveraineté des moyens de paiement : de la protection de la sou
des paiements par carte bancaire au développement de nouveaux mo
paiement
 - ▶ a. Paiements par carte bancaire : une dépendance réduite mais qui
toutefois menacée
 - ▶ b. Le développement de nouveaux outils de paiement : le paiement insta
à terme, l'euro numérique

▶ 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'ACTIVITÉ
PUBLIC : LA CONTRIBUTION DES GAFAM À L'ÉCONOMIE FRANÇAISE
- ▶ A. ACTEURS FRANÇAIS ET AMÉRICAINS DU NUMÉRIQUE
DÉSÉQUILIBRE FLAGRANT
 - ▶ 1. Secteur des logiciels : les filiales françaises de Microsoft et Oracle
Top 5 des éditeurs français
 - ▶ 2. Plateformes en ligne : une domination écrasante de Google, Facebook
Amazon
 - ▶ 3. Cloud : OVH, un chiffre d'affaires comparable à celui des *hyperscalers*
un modèle d'affaires opposé
- ▶ B. FAIBLE VALEUR AJOUTÉE, RECETTES FISCALES MINIMES
CONSÉQUENCES D'UNE ACTIVITÉ OFFSHORE
 - ▶ 1. Un taux de valeur ajoutée très bas, témoignant de la contribution réduite
Gafam à l'activité économique nationale
 - ▶ 2. Des recettes d'impôt sur les sociétés très faibles compensées par l'absence
de la taxe sur les services numériques
 - ▶ 3. Le rôle joué par l'Irlande et le Luxembourg
- ▶ C. LES DÉPENSES DE LOGICIELS : 1,5 MILLIARD D'EUROS EN MOINS
AU PROFIT DES ACTEURS EXTRA-EUROPÉENS, 1 MILLIARD EN PLUS
DÉPENSES SUBSTITUABLES DÈS AUJOURD'HUI
 - ▶ 1. Dépenses de l'État dans le domaine du numérique : vision globale
 - ▶ 2. Dépenses de logiciel : le très fort positionnement des acteurs extra-eu
 - ▶ a. Données des administrations d'État
 - ▶ b. Ensemble du secteur public
 - ▶ 3. Des choix contestables au regard des conséquences fortes sur
l'administration
 - ▶ a. Montant des dépenses logicielles des administrations au profit de

DONNÉES

- ▶ 1. Une captation massive et opaque des données personnelles, intermédiaire des *data brokers*
- ▶ 2. Des risques importants pour la sécurité intérieure et les droits fondamentaux
- ▶ 3. Un cadre réglementaire largement contourné en pratique
- ▶ 4. Les données de géolocalisation
- ▶ D. UNE APPLICATION INÉGALE DU RGPD
 - ▶ 1. Le rôle bloquant de l'Irlande
 - ▶ 2. Des sanctions insuffisamment dissuasives ?

▶ CHAPITRE 5 – ESPIONNAGE ET PRESSIONS SUR PERSONNALITÉS POLITIQUES : LES MENACES STRATÉGIQUES DANS UN CONTEXTE DE MONTÉE DES TENSIONS GÉOPOLITIQUES

- ▶ A. UN RISQUE D'ESPIONNAGE INDUSTRIEL OU POLITIQUE
 - ▶ 1. Des produits extra-européens soumis aux législations extraterritoriales
 - ▶ 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
 - ▶ b. Des barrières techniques à l'efficacité non démontrée
 - ▶ c. Une nécessaire immunité au droit extraterritorial
- ▶ B. LA MENACE D'UNE COUPURE DES SERVICES NUMÉRIQUES
 - ▶ 1. Le ciblage de personnalités : le cas du juge Guillaud
 - ▶ a. Une suspension automatique des services numériques américains
 - ▶ b. Le retrait des moyens de paiement
 - ▶ c. Une regrettable inaction de l'Union européenne
 - ▶ d. Le risque d'une systématisation des sanctions ciblées
 - ▶ 2. Une coupure générale des services numériques
 - ▶ a. Un scénario critique auquel il convient de se préparer
 - ▶ b. Une vulnérabilité liée à l'interruption des mises à jour

▶ TROISIÈME PARTIE : LES CAUSES D'UN ENRACINEMENT PROFOND

▶ CHAPITRE 6 – LE DROIT DE LA CONCURRENCE : TOUJOURS UN TEMPS DE RETARD

- ▶ A. LES GAFAM : DES POSITIONS DE DOMINATION GRÂCE À LA MAÎTRISE DE L'ENSEMBLE DE LA STACK DU NUMÉRIQUE
- ▶ B. LE DROIT DE LA CONCURRENCE FACE AUX GAFAM : DES SANCTIONS MULTIPLES ET 17 MILLIARDS D'EUROS D'AMENDES TOTAL
 - ▶ 1. Les vingt-six sanctions envers les Gafam au titre du droit de la concurrence depuis 2010
 - ▶ 2. Le cloud : l'intérêt de mesures ciblées pour faire cesser les pratiques problématiques

NUMÉRIQUES

- ▶ 1. Une répartition très inégale des ressources humaines numériques qui s'ajoute à des stratégies ministérielles fragmentées
 - ▶ a. Une externalisation limitée au sein des ministères qui disposent d'une unité numérique dédiée
 - ▶ b. D'autres ministères disposant d'une bonne maîtrise globale mais avec des dépendances élevées sur certaines compétences critiques
 - ▶ c. Des ministères contraints d'externaliser toute la gestion de leur système d'information, faute de compétences internes
- ▶ 2. Une perte de maîtrise qui favorise un enfermement dans des solutions européennes
- ▶ 3. Un effort de réinternalisation des compétences à peine amorcé et maintenant suspendu
- ▶ **B. L'ÉBAUCHE D'UNE STRATÉGIE DE SOUVERAINETÉ NUMÉRIQUE SANS VÉRITABLE PILOTAGE INTERMINISTÉRIEL**
 - ▶ 1. Des exigences de souveraineté aisément contournées
 - ▶ a. Un dispositif d'audit des grands projets numériques de l'État qui ne permet pas d'appliquer des critères de souveraineté
 - ▶ b. En pratique, un impact trop limité
 - ▶ c. Un récent renforcement du dispositif d'audit, qui conserve des angles morts
 - ▶ 2. Une mutualisation inachevée de solutions numériques souveraines
 - ▶ a. Les clouds interministériels
 - ▶ b. Les produits numériques interministériels au défi d'une généralisation à l'ensemble de l'État
- ▶ **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**
 - ▶ **B. L'OMNIBUS NUMÉRIQUE : UN REcul DE LA RÉGULATION EUROPÉENNE QUI DONNE SATISFACTION AUX BIG TECH**
 - ▶ 1. L'introduction de failles béantes dans la protection des données personnelles
 - ▶ a. Une grave entaille à la définition des données personnelles
 - ▶ b. Une fragilisation des droits d'accès, d'information, d'opposition et d'effacement
 - ▶ c. Un blanc-seing pour utiliser des données personnelles dans l'entraînement et l'exploitation des systèmes d'IA
 - ▶ d. L'intégration de la régulation des cookies dans le RGPD : en pratique, un transfert de compétence à l'Irlande
 - ▶ 2. À rebours des objectifs affichés de simplification et de soutien aux entreprises, des propositions qui accroissent l'insécurité juridique au profit des plateformes
 - ▶ a. Une simplification manquée
 - ▶ b. Un « énorme cadeau » aux Big Tech
 - ▶ c. Une absence d'étude d'impact malgré l'ampleur des modifications en cours
- ▶ **CHAPITRE 10 – LE FINANCEMENT DES ENTREPRISES NUMÉRIQUES**

- ▶ D. L'ABSENCE DE RÉACTIONS SIGNIFICATIVES AU NIVEAU EUROPÉEN
- ▶ **CHAPITRE 11 – LE DÉPLOIEMENT DE L'IA : LE RISQUE D'UNE DÉFINITIVE DE TOUTE MAÎTRISE**
 - ▶ A. LES CONSÉQUENCES ÉCONOMIQUES
 - ▶ 1. Révolution ou évolution ? Bulle ou pas bulle ?
 - ▶ 2. L'impact économique de l'intelligence artificielle sur l'emploi : la nécessité d'une vigilance
 - ▶ a. IA : quel effet sur l'emploi ?
 - ▶ b. Quelle est la proportion de tâches de l'économie pour lesquelles les travailleurs sont susceptibles d'être remplacés par des outils d'IA ?
 - ▶ c. Quel est l'impact global sur l'économie : croissance ou décroissance, augmentation ou réduction du nombre d'emplois ou diminution ?
 - ▶ d. Les limites actuelles des travaux économiques
 - ▶ 3. Déploiement de l'IA : impacts pour l'économie française dans la conjonction de la crise européenne et mondiale
 - ▶ a. Les gains économiques sont-ils réels ?
 - ▶ b. Une captation de valeur par les hyperscalers, qui renforceront leur domination ?
 - ▶ B. LES RISQUES TECHNIQUES
 - ▶ 1. Risques généraux liés à la diffusion généralisée de l'IA, et en particulier l'IA agentique
 - ▶ 2. Le sujet critique de la cybersécurité
 - ▶ C. DE NOUVELLES VULNÉRABILITÉS SOCIALES ET CULTURELLES
- ▶ **CHAPITRE 12 – LES DATA CENTERS : INSTRUMENTS CLÉS DE LA DOMINATION DES GAFAM ?**
 - ▶ A. POURQUOI IMPLANTER DES DATA CENTERS EN FRANCE ?
 - ▶ 1. Raisons techniques
 - ▶ 2. Raisons économiques
 - ▶ 3. Raisons juridiques
 - ▶ B. ÉTAT DU DÉPLOIEMENT : DES PROJETS QUI BÉNÉFICIERONT À LA GRANDE MAJORITÉ AUX HYPERSCALERS
 - ▶ 1. Une capacité électrique réservée représentant 24 % de la puissance du parc nucléaire français et qui pourrait encore augmenter
 - ▶ a. Data centers en service
 - ▶ b. Data centers en construction ou en état avancé
 - ▶ c. Data centers en projet
 - ▶ 2. Les data centers développés en France seront-ils utilisés par des opérateurs européens ?
 - ▶ C. LA TRAJECTOIRE DE DÉVELOPPEMENT DES DATA CENTERS EN FRANCE : ELLE SOUTIENRA LA DÉVELOPPÉE POUR LE RÉSEAU ÉLECTRIQUE FRANÇAIS
 - ▶ 1. Des volumes d'électricité disponibles suffisants
 - ▶ 2. Des problèmes locaux liés à des congestions du réseau, entraînant des tensions avec d'autres usages de décarbonation

- ▶ a. Contribuer aux communs
 - ▶ i. Le défi du financement
 - ▶ ii. De premières initiatives de soutien public
 - ▶ b. Diffuser la culture des communs numériques dans la sphère professionnelle
 - ▶ i. Le frein des compétences
 - ▶ ii. Pour une contribution des agents publics aux communs
 - ▶ c. Activer le levier de la commande publique
 - ▶ d. Prévenir l'appropriation par les Big Tech
- ▶ **B. LA NÉCESSAIRE GÉNÉRALISATION DES STANDARDS OUVERTS**
- ▶ 1. Les atouts de l'interopérabilité
 - ▶ 2. Une obligation qui monte en puissance
 - ▶ 3. Le rôle clé de la puissance publique pour investir et définir des standards ouverts partagés
- ▶ **C. RÉDUIRE LES IMPACTS NÉGATIFS DE L'IA**
- ▶ 1. L'IA frugale
 - ▶ 2. L'IA open source
 - ▶ a. La définition des modèles ouverts : OSAID 1.0, ou le débat sur la propriété des données d'entraînement
 - ▶ b. La traduction réglementaire : le risque de l'open-washing
- ▶ **CHAPITRE 14 – PROPOSITIONS**
- ▶ **A. POUR UN MODÈLE DE NUMÉRIQUE OUVERT ET LIBÉRATEUR**
- ▶ 1. Principes
 - ▶ a. Le modèle que nous rejetons
 - ▶ b. Le modèle que nous voulons
 - ▶ 2. Écueils et conditions de succès
 - ▶ a. La difficulté d'agir seul dans un contexte européen
 - ▶ b. Le défi de créer une dynamique profonde, à même d'amorcer un changement de modèle
- ▶ **B. LES LEVIERS**
- ▶ **LEVIER N°1 : LES COMMUNS NUMÉRIQUES**
- ▶ 1. Pour une France du Libre et de l'Open Source
 - ▶ 2. Le logiciel libre : pilier de l'éducation au numérique
 - ▶ a. Généraliser l'usage des logiciels libres à l'école
 - ▶ b. La préservation du patrimoine numérique et la diffusion de la culture de l'informatique
- ▶ **LEVIER N°2 : COMMANDE PUBLIQUE ET COMMANDE PRIVÉE**
- SERVICE D'UNE FILIÈRE D'EXCELLENCE FRANÇAISE, OPEN SOURCE**
- ▶ 1. La commande publique
 - ▶ a. Administrations d'État
 - ▶ b. Collectivités territoriales

- CONTRIBUTION DE M. PHILIPPE LATOMBE, PRÉSIDENT COMMISSION D'ENQUÊTE ET DÉPUTÉ DE VENDÉE
- CONTRIBUTION DU GROUPE RASSEMBLEMENT NATIONAL
- ANNEXE N° 1 : LISTE DES ENTITÉS AYANT RÉPONDU QUESTIONNAIRE ÉCRIT DE LA RAPPORTEURE
- ANNEXE N° 2 : QUESTIONNAIRE ADRESSÉ PAR LA RAPPORTEURE AUX ADMINISTRATIONS DE L'ÉTAT
- ANNEXE N° 3 : LISTE DES SIGLES ET ACRONYMES

– 1 –

AVANT-PROPOS DU PRÉSIDENT

Il est des sujets qui exigent davantage que le débat politique. Parce qu'ils engagent l'intérêt général, interrogent l'efficacité de l'action ou mettent en lumière les attentes de nos concitoyens, ils appellent une méthode 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 rigueur de leurs travaux et par l'indépendance de leurs analyses, elles constituent des expressions les plus abouties de la mission de contrôle du Parlement. Elles permettent de dépasser les impressions, les approximations ou les préjugés pour établir les faits, comprendre les responsabilités et proposer des solutions utiles à l'action publique.

Mais la véritable singularité d'une commission d'enquête réside dans sa méthode. Elle rassemble des parlementaires issus d'horizons 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 exacerbés, il me semble essentiel de le rappeler. Toutefois, l'exercice de la commission d'enquête impose à chacun une même discipline : écouter avant de conclure, vérifier avant de juger, 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

appartenances politiques, au renforcement de la confiance entre nos
leurs institutions.

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

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

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

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

En 2021, dans le rapport de la mission d'information sur la
numérique nationale et européenne, j'écrivais : « La constru
souveraineté numérique nationale et européenne doit être le fil rouge d
politiques mises en œuvre dans la décennie à venir. Il s'agit en effet d
absolu. Sans cette boussole, le risque est grand de voir les capacités
individus, des entreprises et des États se réduire progressivement, faute
le " nouveau monde " numérique, alors que de nouveaux acteurs, publ
se sont emparés de leviers d'influence pour servir leurs propres intérêts
de constater que, cinq ans plus tard, nous n'avons pas vraiment progres

D'aucuns s'étonneront que la commission d'enquête ne
intéressée à la cybersécurité et aux failles des entités nationales,
privées. Ce n'est pas un oubli mais la conviction, peut-être illusoire,
essentiel allait être rapidement mené à son terme et qu'il n'était pas né
la commission l'abordât. La menace d'une action menée par la
européenne contre la France, devant la CJUE, avant la fin de l'année
d'une amende devraient sans doute permettre d'espérer l'inscription

INTRODUCTION

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

A. UN CHOIX MARQUÉ PAR LE CONTEXTE GÉO 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 repenser notre modèle de société et nos valeurs : l'Homme n'est pas une somme de données à exploiter. Le cyberspace, loin de l'utopie égalitaire de ses débuts, est devenu un lieu d'affrontement mondial, où s'exercent des luttes d'influence, des conflits de logiques sociales et économiques antagonistes. La révolution numérique et la maîtrise des données ont fait émerger des acteurs économiques qui rivalisent avec les États. Dans ce contexte, et face à de redoutables défis, comment conserver une capacité autonome d'appréciation, de décision et d'action ?* » ⁽¹⁾.

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

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

En réalité, ces dépendances sont la résultante de plusieurs décennies de mondialisation, au cours desquelles cinq géants ont constitué des empires industriels et se sont progressivement implantés en Europe. Google, Apple, Amazon, Meta et Microsoft dominent et maîtrisent une très grande partie de l'infrastructure et des services numériques qui constituent notre quotidien. Les dépendances qu'ils ont créées étaient jusqu'alors présentes mais silencieuses, et ne menaçaient pas directement le fonctionnement des pays.

Elles sont désormais un levier de menaces supplémentaire, au même titre que les ressources énergétiques importées ou les droits de douane. Le Président de l'Assemblée Écologiste et social a pris l'initiative de la création de la commission d'enquête sur la souveraineté numérique c'est en raison du contexte géopolitique. Le second mandat de Donald Trump a

seraient déployés une intelligence artificielle générative compatible avec les valeurs démocratiques et non antisémites. S'agissant de la société Palantir, son fondateur, Peter Thiel, a déclaré en 2017 que depuis 2009 que liberté et démocratie ne sont plus compatibles tant que l'IA existe. Mark Zuckerberg, son PDG actuel, a publié sur X le 18 avril 2026 un manifeste intitulé *République technologique*. Ce manifeste plaide pour une nouvelle ère fondée sur l'IA, dénonce les politiques d'inclusion, le pluralisme et la 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, afin de pouvoir ensuite dégager des actions concrètes. Quelles sont les vulnérabilités critiques qui peuvent affecter le fonctionnement de notre pays ? Comment les remédier ? Telles sont les deux questions qui ont guidé les travaux de la commission d'enquête.

B. TYPOLOGIE DES VULNÉRABILITÉS DANS LE SECTEUR NUMÉRIQUE

Les dépendances structurelles dans le secteur du numérique ont été 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 fausses informations, d'inexactes ou trompeurs. Les acteurs menant ce type d'attaques voient leur efficacité **décuplés avec l'utilisation de l'intelligence artificielle**, laquelle permet de mener des actions plus crédibles dans des volumes beaucoup plus importants. La généralisée de l'intelligence artificielle comme vecteur d'information constitue également un risque de diffusion de fausses informations par « empoisonnement du contenu ». Dans son rapport « Défis et opportunités de l'intelligence artificielle dans la lutte contre les manipulations d'information » ⁽¹³⁾, Viginum (14) a ainsi : « la diffusion massive des outils génératifs interroge (...) fait craindre une élévation structurelle du niveau de menace liée aux ingérences 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 sur 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 réalisées sur l'impact des algorithmes dans le débat public ⁽¹⁵⁾ : « À la suite d'une étude très récente, menée notamment par Germain Gauthier, on a publié le mois dernier dans *Nature*. Aux États-Unis, des individus qui n'utilisent pas l'algorithme standard de X y ont été exposés pendant sept semaines. Cette période soit assez courte, elle a suffi pour que 5 à 7 % d'entre eux aient été exposés à des contenus qu'ils n'auraient pas vus autrement ».

motif économique (rançons). A ce titre, les PME/TPE/ETI sont d'entités la plus affectée (37 %), devant les collectivités territoriales. Les menaces cyber constituent ainsi un coût économique potentiel pour les entreprises ciblées ou leurs utilisateurs et usagers directs ou indirects. Les attaques d'espionnage poursuivent également un motif économique, en lien avec l'identité des victimes visées.

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

Durant les quelques mois où se déroulait la commission, plusieurs cas de fuites de données majeures liées à des cyberattaques ont été constatés, telles que celles ayant visé l'opérateur de tiers payant Almetry ^([8]) ou l'Agence nationale des titres sécurisés (ANTS) ^([9]). Ces nombreux cas démontrent l'importance du sujet ainsi que la régularité et la diversité des cyberattaques.

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

Avec le recours aux technologies numériques, les personnes physiques, les entreprises ou les administrations publiques confient l'ensemble de leurs données à des acteurs tiers. Historiquement, ces données étaient stockées sur des 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 plus en plus 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 les réseaux de télécoms.

Cette situation désormais établie génère trois problématiques :

– **La légalité du stockage et du traitement des données opérées.** Pour les particuliers, le consentement est-il recueilli de façon valide et proportionnée ? Pour les entreprises, la protection de leurs données commerciales et de leur propriété intellectuelle est-elle assurée ? L'Europe est pionnière sur le terrain de la protection des données personnelles avec le Règlement général sur la protection des données (RGPD), entré en vigueur 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 concurrence par les acteurs extra-européens dans le secteur du numérique : Google, Amazon, Microsoft. Le Clarifying Lawful Overseas Use of Data Act (CLOUD Act) de 2018 permet aux autorités américaines disposant d'un mandat d'arrestation ou d'une autorisation du juge dans le cadre d'une enquête criminelle d'exiger des entreprises américaines qu'elles fournissent les données qu'elles possèdent sur des personnes ou des entités situées à l'étranger.

acquièrent une connaissance très fine des individus, des entreprises et des administrations. Cette connaissance est vendue au plus offrant pour de la publicité ciblée. D'autre part, les informations détenues sont circulent entre de très nombreux acteurs, rendant impossible le l'utilisation qui en est faite. Les exemples d'utilisations non so malveillantes sont ainsi nombreux.

Lors de son audition devant la commission d'enquête, Mme chargée de plaider au sein de l'association Amnesty International a conclusions des travaux menés depuis plusieurs années par l'OC « *L'ensemble de ces recherches met en évidence l'existence d'une économie commun, fondé sur un profilage intrusif, une collecte de données personnelles et le recours à la publicité ciblée, qui constitue le fonctionnement de ces plateformes. Ce schéma se retrouve de manière puisque les plateformes cherchent en permanence à accroître la données collectées afin d'élaborer des profils toujours plus précis, de commercialisés auprès des annonceurs, tandis qu'elles recourent, de temps, à des algorithmes sophistiqués pour déduire des centres d'intérêt indicateurs de bien-être, comme c'est le cas de TikTok. L'objectif pour à personnaliser les contenus, à maintenir les utilisateurs en ligne le plus possible et à remporter cette guerre de l'attention, souvent au détriment humains.* »

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

5. Le verrouillage des utilisateurs : une pratique au cœur de la stratégie des fournisseurs de logiciels

Aux fondements de l'économie numérique se trouve la notion de réseau : plus une solution ou une infrastructure est utilisée, plus elle rend son utilisateur, plus elle agrège de nouveaux participants, verrouille le réseau 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 construisent des architectures qui rendent difficile la migration vers une autre solution. Ils ont le pouvoir de vendre des services de maintenance et des prestations complémentaires pendant le développement dans la durée. Tant pour les acteurs économiques que les particuliers, le changement de système est coûteux et requiert de nombreux 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 du service lorsque ce vendeur n'est plus en mesure d'assurer la continuité de la solution (incident de service, faillite) ou bien ne le souhaite plus (choix de l'entreprise ou décision des autorités).

Le risque de dépendance augmente dans un secteur où le marché est

La construction et le maintien des infrastructures sont dépendants de l'approvisionnement en composants clés. Comme rapport de l'Institut de relations internationales et stratégiques (Iris) *la production de composants électroniques s'est largement délocalisée de l'Europe et de l'Asie vers les pays d'Asie, d'abord le Japon puis la Corée du Sud 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. 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 18 %, alors que la Chine représente désormais 18 % de l'offre mondiale (...). En ce qui concerne les échanges internationaux, plus de la moitié des exportations de composants sont assurées par trois pays asiatiques (Chine, Taïwan, Corée). En ce qui concerne les composants spécifiques au développement de l'industrie artificielle, la concentration est encore plus forte puisqu'ils sont produits par deux pays : la Corée avec Samsung et surtout Taïwan avec TSM* ».

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

TYPOLOGIE DES RISQUES ET VULNÉRABILITÉS SYSTÉMIQUES DANS LE DOSSIER 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 vulnérabilités structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France. La proposition de résolution du groupe Écologiste et social ^([13]) listait plusieurs axes d'études qui devaient embrasser un champ très large de problématiques. Ainsi que le relevait de M. Philippe Latombe lors de l'examen de la recevabilité de la proposition de résolution ^([14]), « l'exposé des motifs de la proposition de résolution évoque à la fois les cyberattaques d'ampleur menées par des acteurs privés, les ingérences d'ingérence et les outils de surveillance de masse déployés par des États, les stratégies développées par les grandes entreprises du numérique et les liens liés à la législation européenne du numérique (...). Il importera donc à la commission d'enquête de veiller à ordonner au mieux ses travaux ».

manière approfondie la situation des collectivités territoriales. Certains provenant de la centrale d'achat publique Ugap (Union des groupements 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 **entreprises ou secteurs clés** prennent une place spécifique dans la stratégie française tant leur défaillance pourrait revêtir des conséquences importantes. Il peut être des entreprises industrielles, bancaires, des médias, etc. Les réglementations européennes et françaises créent d'ores et déjà des dépendances spécifiques aux entités économiques essentielles, comme par exemple les infrastructures critiques 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 publication est attendue**. 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, etc.) ou dont la fragilisation aurait des conséquences immédiates (exemple : gestionnaires de réseaux d'infrastructures, etc.). Les entreprises, même non chargées de missions essentielles, sont également des acteurs dont les difficultés peuvent avoir des répercussions à grande échelle, que soit le secteur considéré : grande distribution, agro-alimentaire, énergie, construction, assurance, etc.

– Enfin, **l'économie générale** est constituée de l'ensemble des acteurs économiques, 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 tensions avec les États-Unis et les entreprises américaines, la dépendance des administrations et des entreprises ou services publics vers des solutions logicielles et cloud non européennes fait courir le risque de compromission des systèmes critiques. L'objectif est de mesurer ces dépendances et d'évaluer 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 précédent), la rapporteure a défini les objectifs suivants :

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

– Déterminer dans quelle mesure des stratégies techniques et organisationnelles 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 des technologies américaines ?

– Comprendre la place des acteurs et de l'emploi français dans le développement des services informatiques à la sphère publique et le rôle de la communauté

Grands instituts de recherche publics	Table ronde réunissant des DSI d'organismes de recherche
Opérateurs d'importance vitale	Questionnaire à destination d'une sélection d'entreprises opérant un service critique d'importance vitale (voir liste)
Transverse	Table ronde réunissant les centrales d'achat publiques ⁽¹³⁾ Questionnaire à destination de l'Ugap

Enfin, le secteur bancaire, et plus particulièrement la question de paiement, a fait l'objet d'une étude de cas, dans la mesure où ce secteur est en partie contrôlé 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 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'asseoir leur position dans le marché des services numériques. Microsoft a dégagé 160 milliards de dollars de revenus de ses activités en 2023, Google 165 milliards, Amazon 140 milliards et Meta 60 milliards. Ensemble, ces sociétés prévoient d'investir plus de 650 milliards en 2026 dans l'IA. 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'asseoir la domination technologique, grâce à des investissements colossaux dans les infrastructures clés, en particulier les data centers.

Dans un secteur en voie d'accélération, **les années à venir sont propices pour endiguer le renforcement de positions dominantes qui aggrave 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 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'augmenter la dépendance de certaines avec le déploiement rapide de l'intelligence artificielle générative ?

- **Décrire l'usage de la donnée personnelle à des fins de marketing** en identifiant les risques pour la protection de la vie privée. En novembre 2023, la Commission européenne a publié une proposition de règlement sur la protection des données numériques, qui modifie des réglementations structurantes et historiques : le RGPD, le règlement sur l'intelligence artificielle (Artificial Intelligence Act) et le règlement sur les données (Data Act). La commission propose des modifications comme une simplification des lois numériques existantes et une adaptation européenne à des fins de compétitivité, alors que de nombreux acteurs

– opérateurs économiques de l’État : Caisse des dépôts, Banque 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 pour rencontrer des représentants des institutions européennes.

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

*

* *

La spécificité du travail de la commission d’enquête tient au fait qu’elle a conduit ces deux analyses en parallèle. Des travaux avaient été menés sur chacun des deux axes. Dans un rapport datant de septembre 2025, le Haut-compte avait ainsi examiné les enjeux de souveraineté des systèmes d’information civils de l’État ^([20]). De la même manière, le Sénat, dans sa commission des finances, sur les coûts et les modalités effectifs de la commande publique et l’impact de leur effet d’entraînement sur l’économie française de juillet 2025 ^([21]), a analysé des enjeux de la souveraineté numérique dans la commande publique des administrations confondues. D’autres rapports ont pu analyser l’impact du phénomène des dépendances numériques au niveau de l’ensemble de l’économie.

Le travail de la commission d’enquête, combinant une approche 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 sectoriels.

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

- 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 services réalisés par chacune des directions numériques des ministères. Enfin, certains systèmes d'information ont été auditionnés par la commission d'enquête.

A. LES APPLICATIONS MÉTIERS : LE RECOURS PRINCIPAL AUX FOURNISSEURS FRANÇAIS, DES VULNÉRABILITÉS DANS CERTAINS CAS

1. Données sources

Les constats suivants reposent sur les données recueillies auprès des administrations sollicitées. 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 leur parc applicatif, d'autres ont communiqué une sélection des applications jugées pertinentes au regard de l'objectif de la commission d'enquête.

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

Néanmoins, les informations collectées sont cohérentes avec les données transmises par ailleurs, et peuvent donc être considérées comme fiables pour dresser un état 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 achetées pour les besoins propres des ministères et de produits achetés sur étagère. Pour les solutions à façon, les développements sont réalisés par des entreprises de services informatiques ou bien pilotées en interne, le cas échéant avec l'appui de prestataires intégrés au développement. Les proportions de chacune des catégories d'application sont présentées dans les administrations et les effectifs dont elles disposent pour les tâches de développement.

Les questionnaires envoyés aux administrations ont permis de recueillir les informations sur :

- la répartition des logiciels entre logiciels sur étagères et logiciels développés spécifiquement pour les besoins de l'utilisateur ;
- la répartition des développements entre développements externes et développements internes et développements assurés par une équipe interne avec des renforts externes (notamment interne).

Les chiffres recueillis auprès des administrations montrent que :

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

– les coûts de développement engagés pour la réalisation de l’application ;
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 des applications critiques (catégorie 1 à gauche et catégorie 2 à droite). Il ressort de ces données que :

– les fournisseurs français sont très majoritaires, avec respectivement 81 % et 228 % 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 compris entre un et trois ans) et douze applications pour la catégorie 2 (dont une application non substituable et une application substituable comprise entre un et trois ans).

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

Allemagne		5
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 n'est pas la France.

APPLICATIONS CRITIQUES DÉVELOPPÉES PAR DES FOURNISSEURS ÉTRANGERS DONT LE DÉVELOPPEMENT OU D'EXPLOITATION SONT SUPÉRIEURS À 1 MILLION D'EUROS

Administration	Nom de l'application	Objet	Nom du fournisseur
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. 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
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	Clinysis

Enfin, s'agissant des stratégies techniques et contractuelles mises en œuvre par les administrations pour se prémunir de la dépendance aux fournisseurs, le tableau ci-dessous résume le nombre d'applications pour lesquelles chaque administration est propriétaire, le nombre d'applications open source (en ligne) et les applications qui sont développées en open source. Par exemple, la Caisse nationale des allocations familiales (Cnaf) ne dispose pas d'applications open 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 de 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, 84 % 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 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 ⁽¹²⁴⁾	2	1	3
Non propriétaire			
Propriétaire	2	1	3
DGDN ⁽¹²⁵⁾	25	7	32
Non propriétaire	9	1	10
Propriétaire	16	6	22
DGPN ⁽¹²⁶⁾	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

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

– l’interconnexion des outils Microsoft avec l’ensemble des applications autour. Ainsi que l’indiquent les ministères sociaux : « *La sortie de Windows du travail paraît peu réaliste à date, aucune solution actuelle sur étagère n’offre la fonctionnelle nécessaire pour garantir la continuité de service et le niveau de service des agents des ministères, dans un contexte notamment de très forte pression et de nombreux effectifs. Il est difficile d’envisager une sortie de Windows à court terme en tant que central dans les environnements de travail, tant pour les postes utilisant de nombreux outils métiers et dispositifs périphériques. Le système d’exploitation est profondément intégré à l’écosystème métier et applicatif, aux mécanismes de mises à jour annuelles et aux chaînes de support, rendant toute substitution brutale une rupture de continuité de service. D’autant que le SI des MSO [maladies à signalement obligatoire] présente encore de fragilités structurelles (obsolescence, sécurité) non réglées. Une telle opération supposerait enfin des investissements importants en adaptation logicielle, en accompagnement des usages, qui ne peuvent être conduits que dans une trajectoire 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 logiciels commerciaux. Microsoft, par exemple, est très profondément ancré dans l’écosystème d’information, au-delà de ce que l’on voit comme le système d’exploitation et les applications. Il pilote aussi la gestion de nos identités avec Active Directory ou la gestion des ressources 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* » ⁽¹²⁷⁾.

– la nécessité d’inscrire dans le temps long le processus de basculement des 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), VMWare (virtualisation) et dans une moindre mesure IBM et Red Hat

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

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

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 2026, à migrer un 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 nombreuses. Il s'agit principalement de faire évoluer les architectures techniques des produits informatiques beaucoup conçus entre 2000 et 2010, pour réduire la dépendance aux éditeurs propriétaires de techniques sélectionnés à l'époque comme les serveurs d'application (Oracle), les bases de données (Oracle, IBM). La voie poursuivie par le ministère consiste à remplacer progressivement ces composants par des équivalents open source (Tomcat, PostgreSQL). Des crédits sont programmés en 2026 sur ce sujet et une trajectoire pluriannuelle est définie relativement aux technologies Oracle et IBM.

« (...) La solution de virtualisation VMware n'est pas substituable par une solution open source. Son usage est extensif. Son périmètre fonctionnel est bien supérieur à ce qui est obtenu avec la virtualisation et sous-tend un véritable cloud privé. Les coûts de gestion et d'administration sont une fraction de ceux communément nécessaires pour des solutions alternatives comme Openstack. Des expérimentations sont en cours pour substituer 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. Le ministère est une technologie phare dans ce domaine, sous-tend la nouvelle application nationale de la scolarité du 1^{er} degré, équipant en cible l'ensemble des 42 000 écoles publiques du territoire national. Cette application est en déploiement progressif jusqu'à septembre 2026, et se substitue à une application équivalente basée sur Oracle et IBM.

« Les bases de données et les serveurs d'application Oracle ne sont pas obsolètes. Ils ont moins de 3 ans. Au-delà des réécritures applicatives, qui sont des opportunités évidentes de modernisation technologiques mais limitées à des cycles de vie applicatifs assez longs, des travaux d'adaptation des applications existantes ont été menés sur plusieurs cas concrets pour résoudre des instabilités applicatives. Par ailleurs, dans un contexte de ressources limitées, les travaux techniques d'adaptation des applications souffrent systématiquement de la concurrence des besoins métiers et de leur traduction en évolutions fonctionnelles, rendant difficile l'injonction de réformes ou politiques publiques d'urgence ».

Enfin, s'agissant des **ministères économiques et financiers**, le constat est identique : « Il n'y a pas aujourd'hui de cartographie des dépendances formelles des Ministères Économiques et financiers, mais un certain nombre d'aspects de dépendances ont pu faire l'objet de travaux spécifiques ponctuels ou portés sur des cycles plus longues : logiciel de gestion de base de données Oracle, logiciel statistique, solution de virtualisation VMWARE ». Ainsi que l'expliquait Tomasz Blanc, chef de 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 certaines dépendances extra-européennes subsistent, que nous nous efforçons de maîtriser. Nos principales dépendances concernent les infrastructures matérielles, achetées de manière 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'achat de matériels et des marchés afin de maîtriser au mieux ces dépendances. S'agissant des logiciels, nous avons mis en place une stratégie de réduction des dépendances ».

CNAM	X	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 ⁽¹²⁹⁾	X		X		
Intérieur - DGNP	X	X	X		
France Travail	X		X		

Source : réponses aux questionnaires de la rapporteure.

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

3. État du déploiement des solutions open source au sein des administrations : à l'exemple à suivre de la gendarmerie nationale, les transitions engagées par d'autres ministères

La gendarmerie nationale est un modèle : elle a mené un programme de l'intégralité de ses systèmes d'information vers des solutions en open source. Les outils bureautiques, mais aussi les systèmes d'exploitation et les solutions métier, font fonctionner les applications métiers. *« Dès le début des années 2000, la gendarmerie nationale a opéré un virage numérique stratégique en privilégiant la maîtrise de l'indépendance vis-à-vis des éditeurs en ayant recours aux logiciels libres, d'optimiser l'interopérabilité, rationaliser la maintenance et garantir la performance et une fiabilité optimales des SI.*

« En outre, l'utilisation des logiciels en open source permet de maîtriser l'obsolescence programmée des solutions offertes par les éditeurs. L'intégration du poste de travail gendarmerie est réalisée en interne afin de répondre à la maîtrise technique, industrielle, des données et des coûts. Des équipes dédiées à l'architecture logicielle du poste (choix du système d'exploitation et de sa configuration, des applicatifs installés, sécurisation du poste de travail) et peuvent s'appuyer sur un service de support de proximité pour le déploiement et l'assistance utilisateurs de l'ensemble des postes de travail.

« Cette stratégie d'internalisation se retrouve en particulier :

« – pour les outils bureautiques, avec un recours quasi général à Microsoft Office, contraint pour des raisons de compatibilité avec les systèmes d'information, notamment judiciaires, ou le format de fichiers échangés avec des entités extérieures ; marginal : moins de 2 % du parc des postes de travail en sont équipés ;

« – pour les messageries individuelles, organiques (boîtes d'unités), fonctionnelles (boîtes fonctionnelles partagées pour des besoins particuliers), toutes reposant sur des logiciels libres (suppression des tous derniers comptes Outlook début 2010).

D'autres administrations ont adopté ces solutions de façon partielle pour la partie bureautique. **Les ministères économiques et financiers transition partielle vers les solutions open source, qui touche d'autres ministères bureautiques.** Toutes les directions ne sont pas concernées, mais celles qui l'ont sont la majorité des agents, en particulier la DGFIP.

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

Concernant les dépendances au système d'exploitation Windows ainsi qu'à Oracle, IBM et VMWare, « Le logiciel libre constitue le pilier central de [la stratégie] 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 d'un éditeur, nous avons structuré dès 2005 un marché de support devenant un service s'appuyant sur des entreprises françaises spécialisées. Cette approche repose sur l'expertise de haut niveau et une correction réactive des bogues, pour un coût inférieur aux licences classiques. Les résultats concrets valident ce choix puisque la priorité est systématiquement donnée au logiciel libre pour tout nouveau projet. Le recours au prélevement à la source, dont la brique de collecte des revenus est intégrée à la stratégie, a permis de réduire notre parc Oracle » ^([30]).

Le **ministère de l'intérieur** poursuit la même démarche d'intégration de solutions open source pour les briques essentielles de son système d'information. Ce ministère poursuit une politique du numérique cherchant à favoriser les solutions libres. Cette approche poursuit plusieurs objectifs de maîtrise technique, industrielle et financière des coûts. Toutefois, des contraintes techniques et organisationnelles limitent les 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 Microsoft Office. Ainsi, on recense pour l'administration centrale, (...) 3 470 PC, pour l'administration territoriale (...), 4 793 licences sur 73 320 PC. Le 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. L'administration nationale fait office de précurseur, avec une politique volontariste ayant limité l'usage de Microsoft Office à moins de 2 % du parc des postes de travail.

« – Les logiciels libres Firefox, Thunderbird, et VLC sont également

logiciels. Les administrations stockaient historiquement leurs applications en interne, en s'appuyant sur le parc de data centers de l'État, qui comptait 58 centres réduits à 58 après des efforts de rationalisation. Le basculement vers le cloud a poussé l'État à formaliser une doctrine qui impose un hébergement sur des infrastructures françaises pour les données les plus sensibles afin d'en conserver la maîtrise. Pour éviter l'exposition de données sensibles à des fournisseurs américains ont cependant été mis en place des mesures de protection.

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 du cloud en nuage, la stratégie de l'État sur le cloud a dû pleinement intégrer les enjeux de sécurité. La doctrine Cloud au centre, introduite par la circulaire du Premier ministre du 14 mars 2018, s'est ainsi efforcée d'articuler l'objectif de généralisation du cloud avec des mesures de protection des données.

Tout en demandant aux administrations de recourir au cloud pour leurs données numériques, la circulaire leur impose de s'orienter vers l'un des clouds internes ou l'offre commerciale disposant de la qualification SecNumCloud de l'Anssi : « *le système ou l'application informatique manipule des données d'une sensibilité élevée qu'elles relèvent notamment des données personnelles des citoyens français, des données économiques relatives aux entreprises françaises, ou d'applications métiers des agents publics de l'État* » ⁽³¹⁾.

Le référentiel SecNumCloud

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

Le référentiel comporte plus de 200 exigences, à la fois techniques, organisationnelles et humaines, dans quatorze domaines (les ressources humaines, la gestion du risque, le contrôle, la gestion des identités, la cryptologie, la sécurité physique et environnementale, la gestion de 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 en France ou dans l'Union européenne ; aucune entité extra-européenne ne doit détenir seule plus de 25 % des données ; plus de 39 % collectivement ; le prestataire doit être autonome dans l'exploitation ; 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 des infrastructures extra-européennes, 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 obtenu la qualification en décembre 2025.

La qualification n'est délivrée par l'Anssi qu'à l'issue d'un processus formel comprenant un audit sur site, qui vise à vérifier que la solution candidate satisfait aux critères. La qualification est accordée pour une durée maximale de trois ans, renouvelable annuellement.

Le Parlement a élevé cette exigence au niveau législatif par l'adoption de la loi n° 2024-410 du 21 mai 2024, dite loi Sren. Remplissant les deux conditions précitées, l'article 31 de la loi impose à l'État, à ses opérateurs, et à certains groupements de veiller à ce que le service en nuage garantisse « *la protection des données traitées ou stockées contre les accès non autorisés des autorités publiques d'États tiers non autorisé par le droit de l'Union européenne* ». La définition des critères de sécurité à remplir, la liste des groupes d'intérêt public concernés, et les modalités de dérogation temporaire étaient renvoyées au Conseil d'État.

Alors que le décret était attendu dans un délai de six mois à compter de la loi, il n'a été publié que le 14 avril 2026. Il prévoit que les offres commerciales doivent obtenir une qualification attestant leur conformité au référentiel de l'Anssi. Cette qualification d'exigence requis en matière de sécurité des systèmes d'information, de l'hébergement des données, ou la protection contre tout accès par des autorités d'États tiers. Les administrations ayant engagé un projet de migration vers le cloud pourront solliciter une dérogation auprès du ministre de l'Intérieur pour une durée maximum de dix-huit mois si une offre acceptable est disponible en France. Cette dérogation est 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 mesuré de fournir un recensement exhaustif des modalités d'hébergement des données d'information de l'État. En l'absence de mesure consolidée des dépenses des centres ministériels (achats de serveurs, capacité de stockage, consommation d'énergie, achats de services cloud, qui ne sont pas tous correctement identifiés dans le budgetaire et comptable de l'État – Chorus –, il n'est en effet pas possible d'avoir un regard et d'évaluer l'avancée de la migration vers le cloud. Il n'existe pas de recensement centralisé et systématique des données sensibles à l'échelle internationale, la cartographie étant laissée à la responsabilité de chaque ministère.

Les données collectées par la rapporteure auprès des administrations sur leurs contrats cloud, complétées par leurs réponses écrites, dégagent cependant une tendance : **le stockage interne est largement privilégié, avec une ouverture variable vers les solutions commerciales selon les missions de chaque ministère et la nature des données amenées à traiter.** Ces résultats sont corroborés par la direction interministérielle des systèmes d'information (Dinum), qui indique que « *malgré une augmentation significative du recours au cloud de l'ordre de 60 %), l'hébergement interne demeure encore largement prépondérant. À l'État, les montants concernés restent en valeur absolue modérés, de l'ordre de quelques dizaines de millions d'euros* » ⁽¹³³⁾.

MODALITÉS D'HÉBERGEMENT DES SYSTÈMES D'INFORMATION DES MINISTÈRES

Ministère	Recours aux clouds internes	Recours aux clouds commerciaux
Affaires étrangères	Cloud Pi pour France Visas Réflexion pour recourir au cloud Pi pour la diffusion restreinte.	Oui – uniquement SecNu

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 l'hébergement consistant à héberger nos propres systèmes, dans des centres de données appartenant à la puissance publique. Concernant les systèmes d'information les plus sensibles, en effet nous permettrons la moindre dépendance, même intra-européenne ou nationale. On a fait la remontée des résultats des élections, par exemple, on n'a pas très peur que l'économie, quel qu'il soit, puisse interférer dans le processus, tout simplement parce qu'on a des raisons de confiance dans la vie démocratique de notre pays. (...) La capacité d'héberger nos systèmes dans nos infrastructures, comme le font nos collègues de la Défense, est une première. Le deuxième opérateur interministériel, garantit une forme de continuité, car il ne peut pas agir sur ces systèmes ni les interrompre. Cela permet de maîtriser les enjeux liés à ces infrastructures – et nous savons quel défi cela représente. » ^([34])

En raison des capacités limitées du cloud Pi, le ministère recourt également aux offres hébergeant satisfaisant aux exigences de sécurité de la qualification SecNumCloud, pour les données les plus sensibles.

L'Anfsi, qui assure la direction des systèmes d'information pour la gendarmerie nationale, applique ce principe de façon encore plus stricte. Le général Marc Boget, a ainsi affirmé conserver toutes les données sensibles des services de renseignement souverains de Rosny-sous-Bois et de Nogent-sur-Marne, opérés par les équipes de la gendarmerie nationale : « Comme un trésor que l'on protège, nos données sensibles ne sortent jamais de nos infrastructures car même un SecNumCloud ne peut offrir les garanties de sécurité nécessaires à l'exploitation directe par des gendarmes au sein de nos propres casernes » ^([35])

Certaines données non sensibles, notamment celles qui ont vocation à être partagées 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 les données sensibles, j'ai instauré un barrage interdisant toute intrusion de l'extérieur vers l'interne depuis l'extérieur. Toutefois, ce dispositif devient inopérant lorsqu'il est utilisé par les usagers, ces derniers n'ayant pas de droit d'accès. J'utilise donc un cloud externe, hébergé chez un prestataire rigoureusement sélectionné, où je vais stocker les données pour les rapatrier. Ce processus repose sur une coupure protocolaire évitant ainsi tout lien direct avec mes systèmes internes. »

La DGFIP, garante du secret fiscal et du secret des affaires, conserve à l'essentiel de ses données dans ses propres infrastructures exploitées par les services des contrôleurs ou inspecteurs des finances publiques, comme l'a expliqué le directeur de la DGFIP devant la commission d'enquête : « En pratique, la quasi-totalité de nos données sensibles, est hébergée en interne dans nos propres centres de données. Le recours au cloud demeure tout à fait exceptionnel et ne concerne que les données publiques, comme les données pour l'exploitation de photos aériennes au sein de notre SI. » Si 25 % du cloud Nubo, la DGFIP conserve toujours une part élevée on premise (sur site) pour les données sensibles à l'hébergement interne, même quand la sensibilité des données ne peut pas s'expliquer par des besoins de standardisation des filières d'hébergement : « La grande majorité des données sensibles, qu'elles soient fiscales ou personnelles, sont hébergées en interne, même pour les particuliers que pour les professionnels, nous ne souhaitons pas développer une architecture spécifique pour les rares applications qui n'en contiendraient pas. Nous privilégions la standardisation massive en maintenant ces applications sur les architectures existantes utilisées pour le reste de nos activités. »

Cette vigilance semble s'imposer de façon transversale au sein de

cloud interne pour demeurer autonomes.

Le ministère de la transition écologique privilégie ainsi une stratégie interne selon une « *logique de souveraineté et de sécurité* » comme développée et décrites : « *Les serveurs hébergeant les systèmes d'information et les données, les outils bureautiques et collaboratifs sont pour l'essentiel situés dans les ministères, sur des machines "on prem" ou sur le cloud ministériel, avec un hébergeur SecNumCloud ou chez IMT pour certaines briques. En utilisant des serveurs pour l'essentiel des services et en imposant des niveaux élevés de sécurité, le ministère limite les surcoûts d'infrastructure et réduit sa dépendance à des fournisseurs externes.* » Environ 70 % du parc applicatif ministériel est ainsi hébergé sur SecNumCloud, 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 technologies de virtualisation VMWare et de technologies de stockage américaines, notamment.

Le ministère de l'éducation nationale a mis en place, en 2018, la plateforme nationale 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 du ministère. La direction du numérique pour l'éducation indique ainsi que le ministère « *très essentiellement ses applications en interne (on premise) dans des infrastructures interministérielles ou au sein d'hébergements dédiés privés. Par exception, certaines applications traitent des données dont la sensibilité l'autorise et que le ministère, pour ses avantages singuliers, le ministère opère des hébergements dans le cloud public.* » L'hébergement des sites web institutionnels du ministère de l'éducation nationale centrale et des services déconcentrés, ainsi que celui des systèmes d'information de la jeunesse et sports – au total, 150 services numériques – sont cependant externalisés à un acteur français.

Le ministère de l'agriculture et de la souveraineté alimentaire dispose d'une propre plateforme d'hébergement, reposant sur des infrastructures situées en France.

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

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

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

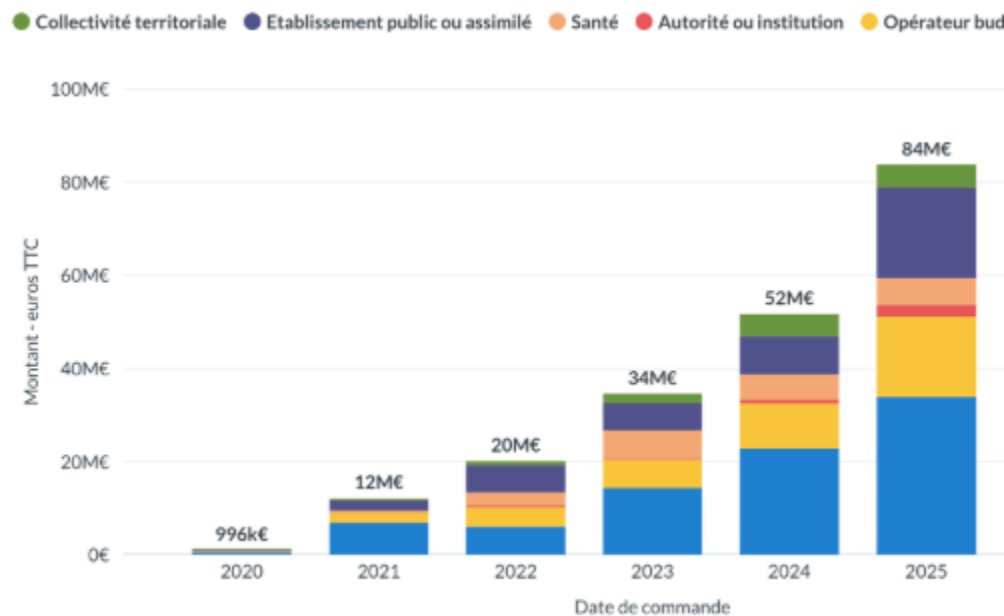
Selon la même logique, les ministères sociaux ont basculé leurs systèmes d'information vers le cloud, en ayant systématiquement recours aux offres commerciales pour leurs projets ou les refontes significatives. Ils continuent d'héberger une partie de leurs données d'information dans des centres techniques informatiques ministériels et en dehors, à des infogérances effectuées par la société Orange Business pour un montant de 15 millions d'euros par an, tout en externalisant l'hébergement des données sensibles.

et l'environnement (Inrae) s'appuient sur des centres de données régionaux du ministère de l'enseignement supérieur et de la recherche, et généralement des universités, au sein desquels ils ont installé leurs propres capacités de stockage. Concernant le CEA, M. Baptiste Grigy a déclaré : « *le CEA a un système d'information à 99 % sur site (on premise). Notre informatique est localisée dans nos propres données, répartis et redondés sur différents sites, et il existe une culture traditionnelle 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 comme principal moteur, comme le montrent les chiffres des achats de services informatiques externes. Les derniers bilans de la doctrine Cloud au centre de la Dinumeration ont montré une multiplication par quatre des commandes sur le marché Nuage public de l'État 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 sélection des fournisseurs sélectionnés ainsi que sur le recours à des offres labellisées SSI.

a. Un hébergement des données majoritairement assuré par des fournisseurs européens

Lors de son audition par la commission d'enquête, la directrice générale de la Direction nationale de l'enseignement numérique a fait valoir qu'en 2025, **sur le périmètre strict des administrations de l'État, 99 % de la commande publique de l'État est orientée vers des offres essentiellement françaises**.

La part de fournisseurs européens descend à 89 % lorsqu'on étend le périmètre à l'ensemble des fournisseurs de l'État, et elle n'est plus que de 70 % sur l'ensemble du marché.

relevait dans son bilan de décembre 2025 que « les acteurs extra-européens d'ailleurs peu dans le marché Ugap (baisse des remises octroyées, priorités collectivités ou les établissements publics qui n'ont pas l'obligation de recourir à Ugap) ». Les dépenses adressées aux hyperscalers continuent cependant de croître pour atteindre 21,7 millions d'euros en 2025, contre 12,9 millions en 2024, et se tournent vers le haut par une unique commande pluriannuelle de 7 millions passée auprès d'un regroupement d'intérêt économique.

RÉPARTITION DE LA COMMANDE DE SERVICES CLOUD SUR LE MARCHÉ DE L'UGAP PAR
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
OVH	30 188 241	23 398 682	11 930 055	29%	96%	173	125	88
AWS	11 063 684	2 521 894	2 879 082	339%	-12%	27	23	21
Outscale	9 842 714	4 456 937	4 311 474	121%	3%	46	39	28
Microsoft	8 647 561	9 275 789	7 644 970	-7%	21%	106	84	55
Scaleway	6 673 104	4 303 666	2 459 123	55%	75%	59	41	30
Cegedim	4 137 525	260 823	14 409	1486%	1710%	9	5	1
Cloud Temple	3 229 099	2 848 330	1 960 160	13%	45%	12	10	10
Oracle	2 158 683	982 534	1 353 795	120%	-27%	17	14	16
Scalingo	2 051 331	1 756 692	797 878	17%	120%	21	14	7
GCP	1 979 484	1 035 772	860 991	91%	20%	24	14	15
Kyndryl	1 649 021					1	-	-
Numspot	688 668					3	-	-
Upsun	492 705	435 051	208 611	13%	109%	9	7	3
Ecritel	475 323					5	-	-
Clever Cloud	336 538	168 529	13 956	100%	1108%	13	5	3
S3NS	72 751					5	-	-
Orange	8 822	127 852	60 446	-93%	112%	1	3	2

Source : Dinum, février 2026.

Ces chiffres n'offrent cependant qu'une vision partielle des dépenses des établissements hébergées sur des offres commerciales. Ils ne permettent pas d'appréhender l'ensemble des dépenses qui ne reposent pas sur le marché interministériel de l'Ugap mais sur d'autres marchés – Resah, Canut ou Sipperec – ou qui sont passées directement par l'administrateur ou le prestataire de services. De même, les achats de logiciels en mode SaaS ou le hébergement en nuage, ne sont pas retracés.

Le périmètre des SI de l'État à surveiller comporte également des dépenses dans la mesure où les choix en matière de numérique des établissements d'enseignement supérieurs ne sont pas centralisés. La Dinum relève ainsi que les établissements de santé ou ceux relevant de l'enseignement supérieur et de la recherche (ESR) ont fait des efforts de mutualisation : « les premiers n'étaient pas dans le champ d'application de la loi Sren 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 le hébergement d'infrastructure leur appartient du fait de leur indépendance statutaire ».

Certains opérateurs continuent cependant de dépendre très largement de fournisseurs extra-européens. C'est notamment le cas de France Travail, dont 83 % des dépenses de services cloud de l'année 2025 étaient concentrées sur trois fournisseurs : essentiellement ServiceNow, mais également AWS et Microsoft Azure. Les données concernées sont à caractère personnel, mais France Travail estime que cela ne tombe pas dans le champ d'application de l'article 31 de la loi Sren. Les hébergements de données représentent également près de 98 % des dépenses de cloud de la Cnaf.

b. Un recours croissant aux offres certifiées SecNumCloud

En 2025, les offres qualifiées SecNumCloud ont représenté 12,9 millions d'euros de dépenses, contre 12,9 millions en 2024.

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

	d'Office 365			
France Travail	ServiceNow (US)	x	x	
	AWS (US)			
	Microsoft (US)			
	Kyndril (US)			
	Microsoft (US) pour hébergement SaaS d'Office 365	x	x	

Source : Réponses écrites.

La diffusion des **logiciels en mode SaaS (*Software as a service*)**, hébergés et fournis à la demande, a de fait complexifié la préservation de la maîtrise d'information. Pour les administrations qui privilégiaient l'hébergement on-premise d'applications, comme en attestent les ministères économiques et financiers, « *l'offre logicielle en mode SaaS a obligé à ajuster la stratégie (...), l'hébergement d'une offre logicielle n'étant pas systématiquement proposé par l'éditeur* ». Le Baron, directeur du numérique pour l'éducation, a confirmé cette bascule : « *L'absence de solutions apportant les garanties de sécurité nécessaires : « La hausse des redevances annuelles s'explique aussi par la difficulté croissante que nous avons à héberger les éditeurs en interne, on préfère aller vers le SaaS (software as a service) facilité collective, ce qui nous amène à la réflexion sur le SecNumCloud : l'offre nous soumettre une offre suffisamment souveraine et sécurisée, eu égard aux défis que nous faisons face ? »* »⁽³⁶⁾

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

a. Office 365

Les ministères sociaux, le ministère de la justice et le ministère de la culture ont la connaissance de la commission d'enquête leur **utilisation des services de Microsoft Azure qui accompagnent la suite Office 365, dans le cadre d'une dérogation au Cloud au centre**, justifiée par l'absence d'une alternative souveraine opérationnelle.

Les autres administrations utilisatrices de Microsoft ont pourtant tout fait pour éviter l'installation en local. Le directeur du numérique pour l'éducation a ainsi précisé à l'audition que le ministère de l'éducation nationale, bien qu'ayant doté les agents de la suite Office, n'utilisait pas les services cloud de Microsoft, mais une suite bureautique installée sur les postes : « *Toute la collaboration a lieu sur les outils précédemment, des outils libres et hébergés soit dans nos data centers internes, soit dans des clouds souverains* ». Le basculement obligatoire vers le cloud, impliquant des *hyperscalers*, a même pu constituer un accélérateur de projets de migration vers des outils libres, comme pour le CNRS avec Sharepoint : « *Microsoft nous pousse vers le cloud de 2029, ce qui est orthogonal avec les injonctions de souveraineté* », a expliqué Pierre Fontanel, directrice des systèmes d'information. « *Nous avons donc cherché à sortir de cette dépendance en utilisant soit des outils que nous proposons en interne, soit de la Dinum* ». ⁽³⁷⁾

Le maintien d'un hébergement sur site suppose d'être en mesure d'assurer le développement et le coût supplémentaire qu'il peut induire. M. Damien Lacroix, directeur adjoint de la direction de la sécurité des systèmes d'information, a précisé à l'audition que le ministère de l'éducation nationale, bien qu'ayant doté les agents de la suite Office, n'utilisait pas les services cloud de Microsoft, mais une suite bureautique installée sur les postes : « *Toute la collaboration a lieu sur les outils précédemment, des outils libres et hébergés soit dans nos data centers internes, soit dans des clouds souverains* ».

compétences, repose sur la solution SaaS de l'éditeur américain Salesforce, sélectionné pour ses « *qualités fonctionnelles exclusives sur le marché* » ses services numériques pour l'éducation.

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

La Cour des comptes relevait ainsi que « *le ministère a choisi cette solution pour l'amélioration de la performance de sa gestion des ressources humaines au regard de la souveraineté, dont le risque pouvait paraître moins tangible* » ^([40]). Salesforce a été reconnu, dans une réponse à une demande de précision du ministère, qu'il proposait de répondre à des demandes d'accès aux données des clients de la part d'autorités étrangères. L'Anssi ont rendu un avis négatif, considérant que la protection des données extraterritoriales était insuffisante. M. Audran Le Baron observait cependant, suite à une audition, que des mesures de sécurité avaient été mises en place : « *afin de garantir la sécurité de données personnelles traitées par l'éditeur, un important travail de filtrage a été mené pour déterminer qu'elles pouvaient ou non être stockées sur le cloud et y transiter de manière transitoire avant d'être effacées une fois traitées* ». Ce projet devait dû être régularisé *a posteriori* par l'actualisation de la doctrine Cloud au centre. Le ministère a alors considéré que, bien que les données soient d'une sensibilité élevée, la violation n'est pas susceptible d'engendrer une atteinte à l'ordre public, à la sécurité ou à la santé ou à la vie des personnes ou à la protection de la propriété intellectuelle, et n'ont donc pas à être hébergées chez un prestataire SecNumCloud.

La police nationale et la gendarmerie nationale hébergent leurs données des victimes sur les plateformes non SecNumCloud, portées respectivement par la police nationale et l'éditeur américain Salesforce, en l'absence d'offres équivalentes identifiées par la rapporteure de l'objectif d'évoluer vers une plateforme communale SecNumCloud.

La rapporteure a pris connaissance d'autres cas de non-conformité de la loi Sren, mais sans risque de soumission à des lois extraterritoriales où l'hébergeur est français. L'AIFE héberge la plateforme pour les achats de services chez un hébergeur français mais non qualifié SecNumCloud, alors que les données entrent dans le champ de l'obligation. Les ministères économiques et financiers ont choisi dans leur réponse écrite à la rapporteure, tout en annonçant un plan de migration, le terme : « *L'application est relativement ancienne (2012) et lorsque l'AIFE l'a migrée sur 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. Les solutions SecNumCloud s'étant enrichies depuis, l'AIFE va lancer une étude pour migrer l'application sur une architecture SNC, avec un objectif de bascule à mi-2027.* »

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

de modèles d’IA open source ou propriétaires, notamment celles du français hébergées par des acteurs français. Cependant, les travaux de la commission en évidence des cas d’usage **du modèle Claude d’Anthropic, de Copilot Gemini de Google ou de GPT d’OpenAI** au sein de plusieurs ministères : sécurité sociale, de l’AP-HP et de France Travail. Ces différents modèles sont portés par les *hyperscalers* Microsoft, AWS ou Google. Le ministère de l’écologie, qui a construit un portail permettant d’accéder à différents modèles génératives (PIAG), recommande néanmoins aux agents de privilégier SecNumCloud, lorsqu’ils ont à traiter de données sensibles.

DÉPLOIEMENT DE L’IA GÉNÉRATIVE DANS LES ADMINISTRATIONS CON

Affaires sociales	Les ministères disposent du système d’IA Copilot dans le cadre de leur co détiennent quelques licences pour le modèle Claude d’Anthropic, quoique da 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 plusieurs modèles d’IA génératives adaptés à différentes tâches et plusieurs niveaux de le modèle Mistral, hébergé sur l’offre SecNumCloud d’Outscale ; GPT sur Microsoft et Perplexity. L’utilisation de Mistral représente plus de 90 % des dépenses totales de l
Agriculture	Le ministère a accès au portail des IA génératives (PIAG) du ministère de la trans
Ministères économiques et financiers (MEF)	Les ministères économiques et financiers ont déployé les modèles LLM de également disposer de quelques licences pour Claude. Le principal contrat de l’A SSAI, qui repose sur le modèle Watson et les services de cloud d’IBM, en partena
Intérieur	Le ministère a développé une plateforme d’IA générative souveraine, MIRAI, qui e a vocation à migrer vers le cloud Pi ou une offre SecNumCloud pour les u Il dénombre 120 initiatives en matière d’IA, regroupant des usages très divers, dont solutions développées par des tiers, dont très majoritairement des entreprises françai
DGFIP	La DGFIP a déployé des modèles de langages libres dans ses data centers, reposa 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 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 l en juin 2026. Sur le volet pédagogique, le ministère a déployé avec le fournisseur Docaposte l remédiation en français et mathématique qui doit bénéficier à 800 000 élèves. I partenariat d’innovation intelligence artificielle (P2IA) avec l’entreprise Lalil algorithmes d’apprentissage de la lecture, destiné à 40 000 enseignants et 400 000 Certaines régions académiques ont mis en place des systèmes d’IA générative d 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 Yolo v7, hébergé dans les data centers de la gendarmerie nationale pour garan données. Ce projet, qui a débuté en 2019, a représenté 4 millions d’euros de dépen d’intégration, et 700 000 euros de dépenses de licences et de MCO en 2025. L’Anf vers la plateforme d’IA GénIAI du ministère des armées qui repose sur des modèles
Justice	Le ministère a déployé son outil interne d’IA générative, baptisé « Mon assist l’assistant IA de la Dinum. Il compte 90 000 utilisateurs. En parallèle, l’incubate « Mon assistant pénal » et « Mon assistant civil », avec l’appui de la Dinum, pou 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 fo audio et vidéo, de traduction et de synthèse, avec un hébergement souverain. L interne, avec l’appui de prestataires, pour un coût de développement et d’intégrati
France Travail	L’opérateur a conclu un contrat avec Mistral AI pour l’utilisation de ses modèles également à des outils reposant sur des modèles américains (GPT, Claude, Gem hyperscalers (Google, Microsoft Azure). Google est notamment impliqué dan Aglae, fourni par GoJob, qui représentera des dépenses significatives en 2026.

« À la DSIH, nous appuyons à l'IA le modèle de maîtrise interne de langage libres sur nos propres puces GPU, hébergées dans nos centres infrastructure garantit que les données ne sortent jamais de nos murs et nécessaire pour changer de modèle aisément. Cette plateforme centralise plusieurs cas d'usage, dont le plus visible est le nouveau moteur de 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 que Mistral, à la condition impérative qu'ils soient suffisamment standardisés dans notre architecture. Cela nous permettrait de bénéficier d'éventuels gains tout en conservant la faculté de basculer à nouveau vers des modèles libres commerciale de l'éditeur ou les risques pour notre souveraineté l'exigeaient. Je vais également étudier de près le modèle Génial du ministère des armées afin de voir si ça peut nous aider à accélérer nos propres travaux. » ⁽⁴²⁾

La directrice interministérielle du numérique Stéphanie Schaer confirme que « la maîtrise du calcul qui préserve la sécurité des données est essentielle pour le déploiement de l'IA à l'État ». **Pour prévenir les risques de déploiements non maîtrisés, la DSIH est attachée à identifier des solutions répondant aux besoins de la sphère publique.** Elle porte une attention particulière aux conditions d'hébergement : « Dans le tableau répertorié de ces solutions d'IA (...), une colonne précise si la solution est hébergeable en France à l'époque où nous avons lancé l'appel, il y a un an, c'était le cas de très peu de solutions. Nous avons souhaité montrer la diversité des logiciels français qui existaient, stimuler la Tech, mais aussi donner de la visibilité à la capacité d'hébergement en SecNumCloud, chose de très important. » ⁽⁴³⁾

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

- l'API Albert, une plateforme interministérielle qui permet aux citoyens d'accéder à de nombreux modèles de langage, pour plus d'une centaine de modèles hébergés sur une infrastructure SecNumCloud ou sur le cloud interministériel ;
- la plateforme de données, qui permet d'agréger et de structurer des données, principalement issues de sources publiques, afin de les rendre exploitables par les systèmes d'intelligence artificielle ;
- l'assistant IA, un outil généraliste à destination des agents, construit sur Mistral AI en environnement SecNumCloud, qui doit être déployé auprès des agents publics en juin 2026.

L'enjeu qui se dresse devant les administrations est celui de déployer des outils sécurisés et performants dans un temps suffisamment rapide. Tant que les outils souverains développés par l'État seront perçus comme en-deçà de ce qui est fourni gratuitement par les acteurs américains, perdurera un **risque important, c'est-à-dire d'utilisation d'outils d'IA extérieurs dans le cadre professionnel**. Une enquête réalisée par le ministère de l'action et des comptes publics entre janvier et avril 2024 sur 1 867 agents montre que 89 % des personnes interrogées utilisent déjà l'IA dans leur travail, 85 % disent recourir aux outils fournis par leur employeur, **55 % reconnaissent utiliser des agents conversationnels de manière informelle**. Il existe déjà

« dépenses des grands groupes français – lesquelles approchent 47 milliards d’euros – des entreprises du CAC40 » ⁽¹⁴⁵⁾. Les administrations sont au cœur des services mais ne constituent qu’une infime partie de la vie économique et sociale de la France. La commission d’enquête a souhaité élargir son analyse en procédant par cercle de plus en plus large : elle s’agissait ainsi de comprendre les éventuels risques systémiques provenant des administrations publiques, puis de l’ensemble du tissu économique français.

A. LES ENTREPRISES PUBLIQUES : DES SYSTÈMES D’INFORMATION 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 données s’appuient sur les réponses aux questionnaires envoyés aux entreprises 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, avec une attention supplémentaire portée aux systèmes d’information industriels de la nature même de l’activité.

1. Dispositifs d’évaluation des dépendances numériques et stratégies de gestion des vulnérabilités

De par leur culture et les dispositions applicables aux opérateurs d’intérêt public (OIV), les entreprises consultées mettent en œuvre des processus qui évaluent les risques 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 pleinement été intégré à ces analyses. Les réponses aux questionnaires font état d’une prise en compte récente du risque numérique dans sa nouvelle dimension géopolitique et de la vulnérabilité à des fournisseurs extra-européens.

Comme l’indique Aéroports de Paris (ADP) : *« nous avons élaboré un processus de nos dépendances. Elle repose actuellement sur un indicateur spécifique pour l’indice de sensibilité au vendor lock-in, et un nouvel indicateur standardisé (indice de résilience numérique), plus largement reconnu. Les processus clés de gestion des plans de continuité de l’activité sont en place. Par exemple, en cas de défaillance, nous prévoyons une capacité à opérer l’aéroport sans l’IT, à capacité réduite »*. Les processus clés et les services numériques associés ont déjà fait l’objet de tests depuis de nombreuses années à EDF, et il existe un plan de continuité d’activité et de reprise d’activité, testé chaque année, destiné à pouvoir reconstruire les services essentiels en cas de sinistre. En complément, le contexte géopolitique a amené EDF à *« engager plus récemment des actions en vue de maîtriser trois risques spécifiques : les dépendances dans le domaine du numérique :*

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

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

d'indisponibilité des systèmes et de confidentialité des données. « *Mé l'analyse a pour objectif de confronter plusieurs critères qui mesur l'indépendance du système d'information de l'organisation, à trois d (nationale, européenne, extra-européenne). Il s'agit de :*

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

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

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

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

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

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

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

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

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

Pour le pilotage du réseau électrique, Enedis a fait le choix d'un Sc ses propres équipes : « *L'application repose sur des OS open-source (RedHa virtualisation est en cours de migration vers Openstack ou Kubern géographique régional dispose d'un SCADA du marché, fourni par une so est amené à migrer à moyen terme vers la solution développée par Enedis ».*

Concernant Natran, le Scada actuellement déployé repose majori solution commerciale industrielle d'origine nord-américaine, historiquement de sa richesse fonctionnelle, de sa capacité de configuration fine aux beso l'activité et de son coût d'acquisition initial compétitif. Ce système est environnement découplé des services externes, avec des mécanismes de c

historiquement opéré par Atos, avec un objectif de maîtrise opérationnelle co

3. Systèmes d'information tertiaires : les mêmes dépendances à l'administration

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

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

Pour Enedis, *« Les échanges collaboratifs s'appuient massivement sur la suite Office 365 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 une migration vers des solutions open source comparables. Par exemple, chez Enedis, la dépendance à la solution VMWare a été *« fortement diminuée à la suite du déploiement d'Openstack sur une partie du parc (40 % à date). Nous avons l'objectif à moyen terme de sortir totalement de VMware »,* de même que celle d'Oracle *« à la suite du déploiement d'Open Source Postgre sur la majorité de parc (plus de 67 % à date). Nous avons l'objectif de sortir de la solution à l'horizon 2030 ».*

ADP étudie également le remplacement de VMWare par OpenStack, une solution open source, avec comme déclencheur la très forte augmentation de tarif sur le matériel 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, ce qui est résumé dans le tableau ci-dessous.

OPÉRATEURS DE CLOUD DES SIX ENTREPRISES PUBLIQUES INTERROGÉES

	AWS	GCP	Microsoft Azure	S3NS	BLISS
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 électronique monétique				
SNCF Réseau	X		X		

tarifaires) ».

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

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

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

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

Ainsi que l'indique ADP, « *les outils de planification de la maintenance Maximo logiciel Maximo d'IBM, qui est exploité on premise. Les données relatives à la maintenance ne sont pas stockées dans le cloud. Néanmoins, la société Autodesk nous pose une difficulté : Autocad est connu de nos ingénieurs et architectes, et largement utilisé pour l'étude. Il est la référence du marché. Sa version collaborative, qui est une version collaborative de plan, tourne sur un cloud AWS, et Autodesk a refusé de nous autoriser les plans que nous déposons ne soient utilisés pour entraîner les modèles de machine learning d'un de leurs partenaires* ».

L'ensemble de ces éléments font apparaître l'absence de cadre contraignant pour ces entreprises pourtant responsables de l'exploitation de services d'importance nationale. 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 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 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* ». L'opérateur du réseau de transport de gaz explique dans le même temps que « *les mesures techniques et opérationnelles restent largement imposées par les fournisseurs et sont non modifiables, notamment celles relatives aux architectures de référence (Minimum Architecture Rules), aux modèles de responsabilité partagée et aux processus d'exploitation* ».

Chez Enedis, « *la gestion de la relation client, l'analyse de données pour le dépannage et le raccordement qui s'appuient sur la cartographie des réseaux, les analyses de données [s'appuient sur des fournisseurs extra-européens] (...). L'analyse des données*

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

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

B. LES ENTREPRISES PRIVÉES : UNE PRISE EN COMPTE BASÉE SUR DES ACTIONS CONCRÈTES

Le secteur privé représente un poids majoritaire dans l'économie française. Les entreprises non financières comptaient ainsi pour 57 % de la valeur ajoutée brute nationale en 2019, 19 % pour les administrations et 12 % pour les ménages ⁽⁴⁷⁾. Ainsi que l'indique Mayenobe, directrice générale déléguée de la Caisse des dépôts ⁽⁴⁸⁾ : « *La cybersécurité est un levier, mais ce n'est pas le seul. On estime qu'elle représente environ 20 % de nos messages forts est qu'il faut s'adresser aux 80 % restants, c'est-à-dire l'ensemble des autres leviers.* »

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

La création de l'**indice de résilience numérique (IRN)**, en janvier 2020, est un outil de mesure du degré de dépendance pour les organisations publiques : Dicaposte, Caisse des dépôts, CMA-CGM, MAIF, SNCF Aéroports de Paris, etc. France. Les grandes entreprises mettaient déjà systématiquement en œuvre des plans de risque et des plans de résilience face aux principaux risques identifiés. Phénomène de dépendance à des outils propriétaires clés est désormais identifiée comme un risque à compte tenu du contexte géopolitique, ainsi que l'indique M. Arnaud Maury, directeur des risques opérationnels de la Caisse des dépôts :

« *Sur l'IRN, certains de ses huit axes de restitution sont nés de la pandémie et préexistaient. L'axe stratégique et géopolitique, qui inclut le risque de kill chain, est nouveau et a émergé de manière concomitante avec les récentes échecs géopolitiques américaines. La notion de dépendance économique et juridique, bien que la dépendance est plus exacerbée avec l'essor de certaines solutions, comme dans la virtualisation.* »

« *En revanche, les axes de dépendance opérationnelle et de dépendance technologique existent depuis longtemps ; toutes les banques sont assujetties à des dépendances technologiques.* »

promouvoir une définition commune de la résilience numérique, partagé public comme par le secteur privé, nous paraît constituer une démarche per

Toutefois, le décalage entre la prise de conscience et la mise en œuvre concrètes est clairement souligné :

« La conscience est désormais largement partagée : il est impérieux de renforcer la résilience de l'économie européenne. Cette prise de conscience se traduit par des engagements 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 de garantir les performances, l'étendue fonctionnelle et la maturité technologique des services européens. Nous pouvons toutefois espérer une réduction progressive de cette situation par des acteurs européens comme OVHcloud, Scaleway ou encore Stackit au sein du cloud public qui commencent à proposer des services à l'échelle (...)

« Pour les grandes entreprises, celles que je connais et que je considère comme indispensables d'aboutir enfin à ce marché numérique unique, ce " digital single market " que nous parlons depuis quinze ou vingt ans, sans jamais réellement le concrétiser, nous devons commencer à raisonner en termes d'acteurs nationaux, mais d'identifier les grands opérateurs de cloud sur lesquels il conviendrait de concentrer des investissements massifs.

« Si une telle dynamique voyait le jour, appuyée par des instruments européens de certification type EUCS garantissant une protection juridique des données, un consensus émergerait rapidement parmi les grandes entreprises à désoptimiser l'organisation européenne pour multiplier des solutions fragmentées. Cette pays n'est ni viable ni soutenable. » ⁽⁵⁰⁾

Ainsi, les grandes entreprises, qui ne représentent elles-mêmes qu'une faible part de la consommation ajoutée ⁽⁵¹⁾, commencent seulement à identifier le risque engendré par l'utilisation de services propriétaires extra-européens, sans pour autant mettre en œuvre des plans de gestion du risque. Supposer que la prise en compte du risque numérique au sein des organisations de grande taille, est encore moins avancée. Le poids économique de la commande privée est inférieur à celui de la commande publique, pourrait lui conférer un rôle important dans la réduction des dépendances systémiques de notre économie. Mais la mise en place d'actions de sécurisation 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 l'heure actuelle, la sécurité des données ou de souveraineté des solutions utilisées ne sont pas des critères prioritaires en termes de choix d'outils numériques : *« Une entreprise ne va jamais de quitter une solution existante et d'engager des efforts significatifs si elle n'apporte aucun bénéfice tangible. Elle ne le fait que si cela répond à un besoin réel de son activité, à sa productivité, à sa compétitivité. En l'absence d'enjeu avéré, la sécurité, matière de sécurité, les entreprises n'ont aucun rationnel économique pour c*

Dans le prolongement des travaux sur l'IRN, la rapporteure propose d'élaborer un outil par l'édition de grilles d'achat, de cahiers des charges et de clauses types pour la commande privée vers des solutions dont la souveraineté repose sur des éléments de sécurité. renforcer les exigences de réversibilité et d'interopérabilité.

LISTE DES ENTITÉS DÉSIGNÉES FOURNISSEURS DE SERVICES TIERS ESSENTIELS E RÈGLEMENT DORA

Entité	Secteur d'activité	Siège social ma
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, ⁽¹⁵²⁾.

Dans cette même liste se trouvent les trois grands fournisseurs de Google Cloud Services, Microsoft et Amazon Web Services –, mais également de technologie déjà identifiés dans l'analyse des dépendances des administr IBM, SAP. S'y ajoutent des entreprises de services numériques et fi internationale ainsi que des opérateurs de data centers.

Les règles s'imposent à la fois aux fournisseurs désignés comme établissements financiers qui sont leurs clients. Les premiers font l'objet réalisée par des équipes conjointes d'examen (*Joint Examination Team*) aux de l'Autorité de contrôle prudentiel et de résolution (ACPR) française et France participent depuis le 1^{er} janvier 2026. Ils sont soumis, en théorie inspections, à des tests de résilience et à des recommandations correctr jusqu'à des injonctions contraignantes. Quant aux seconds, ils ont l'obligation cartographier l'ensemble de leurs sous-traitants dans ce domaine et d'analyser la localisation géographique des sous-traitants. Cette analyse de risque documentée, porte sur les risques de verrouillage technologique (ver substituabilité réelle des prestataires, la capacité à maintenir les fonctions d défaillance d'un sous-traitant ou encore la concentration des services sur d'acteurs. Ils doivent définir des plans de sortie réalistes (aussi bien au juridique et technique) avec une réversibilité des données (migr interopérabilité).

Ainsi que l'indique la Banque de France dans les réponses écrites pour la majeure partie des deux cents entités du secteur ayant été interrogées le biais d'un questionnaire sur l'application du règlement Dora, la gestion du « le pilier de Dora qui est le plus difficile à mettre en œuvre, la (re)négoci avec les prestataires informatiques constituait un véritable défi pour les e

L'application du règlement DORA oblige donc les établissements financiers à fournir une meilleure connaissance de leurs vulnérabilités aux fournisseurs stratégiques. La Banque de France fournit également des instruments d'analyse prudentielle aux autorités de surveillance. Les entreprises peuvent s'appuyer sur un recensement sérieux. Mais cela ne constitue qu'un premier pas vers une réduction des dépendances, dont toute la difficulté réside dans la mise en œuvre.

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

Ainsi que l'indique la Banque de France dans les réponses adressées aux questions, on observe une numérisation croissante des usages des Français dans les paiements. Même s'ils restent très attachés aux espèces, la carte bancaire est devenue le principal moyen de paiement en magasin (48 % des achats en 2024 contre 43 % en 2023), notamment en raison du paiement sans contact et du paiement mobile. Le commerce en ligne (25 % des transactions en France en 2024) contribue également à la numérisation des paiements. La rapporteure a souhaité comprendre dans quelle mesure ces évolutions ont des répercussions sur le niveau de dépendance de notre économie vis-à-vis des infrastructures extra-européennes.

a. Paiements par carte bancaire : une dépendance réduite mais qui reste 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 des autres pays européens grâce à la constitution historique du groupement d'intérêt économique des cartes bancaires (CB). Au moment de la création du GIE CB, l'action de l'économiste Pierre Bérégovoy a permis de donner l'impulsion politique nécessaire pour surmonter la fragmentation entre les deux réseaux concurrents Carte Bleue et Visa.

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, de la carte de paiement, des plans de l'aménagement des territoires et des télécoms. C'est donc un modèle unique, soutenu par l'État et déployé par les banques au service de nos citoyens, sous l'égide de la Banque de France pour les aspects sécuritaires et inclusifs. Cette carte est aujourd'hui française de bout en bout : de la puce, que nous pouvons fabriquer en France, à l'indépendance et libre de droits grâce à notre histoire industrielle, au terme d'un processus qui a été mené chez les commerçants, et jusqu'aux rails et usines de traitement des transactions, qui sont soit dans les banques ou mutualisées au sein de la société STET (...).

« 95 % des paiements de détail français – carte, cash, mobile – sont 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 gérés par des cartes intra-européennes et 2 % des paiements extra-européens. Le paiement est donc un enjeu domestique.

« En matière de sécurité, nous enregistrons deux fois moins de fraudes sur les cartes internationales grâce à des traitements assurés par une intelligence artificielle entraînée exclusivement sur des données françaises qui ne sont ni revendues à l'étranger, et à des systèmes totalement souverains. La fraude sur la vente à l'étranger, un problème majeur, a baissé de 45 % grâce à la mise en œuvre du règlement.

fortes : des frais de réseau appliqués par Visa et Mastercard sensiblement 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 remettre en question la place du réseau national depuis 2019.

Face à cette situation, plusieurs actions ont été menées pour réaffirmer la place du GIE CB, coordonnées par le Comité national des moyens de paiement :

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

Selon M. Philippe Laulanie, « *CB est aujourd'hui présent dans tous les modes de paiements : pour retirer du cash, pour payer en proximité avec ou sans contact, pour payer par mobile. En effet, 90 % des transactions via des solutions comme Apple Pay ou Google Pay sont des paiements par carte. Sur le plan de la sécurité, ces paiements digitaux renforcent 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 du cobadgée en matière de coût, de fraude et de protection des données (...). Malgré les incertitudes, la carte française cobadgée CB est polyvalente, ce qui n'est pas le cas dans les autres pays européens. En revanche, si le logo CB n'apparaît pas sur les cartes, l'intégralité des données de transaction échappe à notre écosystème ».*

- les engagements récents de certaines banques pour refaire du cobadging une norme. Selon M. Erick Lacourrègne, directeur général des moyens de paiement de la Banque de France ⁽⁵⁵⁾ : « *Les six grands groupes bancaires français se sont engagés à développer des cartes qu'ils émettent, et la Banque de France veille, en tant que régulateur, à ce que les entrants s'y engagent également. Il s'agit d'un sujet stratégique, car les banques américaines disposent d'une base installée mondiale et d'une rentabilité élevée. Cela leur permet de mener une politique commerciale très dynamique, qui leur assure des avantages importants ».* Toutefois, il convient de noter l'absence de discussions de ce sujet en ligne : « *Concernant le cobadgeage CB des banques en ligne, nous incitons les banques 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 resteront à convaincre, mais leur volonté ne fait pas de doute ».*

- Dans le cadre de la stratégie nationale des moyens de paiement, le développement du paiement mobile constitue un impératif stratégique pour l'écosystème. Notre stratégie s'articule autour du principe directeur du libre choix du moyen de paiement pour les utilisateurs. Le mandat du CNMP vise donc à éclairer le grand public sur les implications du choix du moyen de paiement.

- le renforcement de l'information du public. Elle porte notamment sur la visibilité de la marque lors des paiements par carte : le règlement 2015/751, aussi appelé règlement de la Commission sur le paiement par carte, donne aux consommateurs la possibilité de choisir le réseau de paiement pour leurs transactions en magasin et en ligne. En pratique, les consommateurs qui utilisent la carte cobadgée ont la possibilité de choisir le réseau de carte CB pour leurs paiements. La transparence sur la localisation des données de paiement doit également être renforcée.

« Nous avons commencé avec trois pays, en comptons désormais l'Allemagne, la Belgique, les Pays-Bas et le Luxembourg – et préparons nous l'Autriche et d'autres marchés. Nous avons également conclu un accord d'intégration pour étendre notre couverture géographique. L'objectif est d'offrir une forme de paiement instantané, basée sur un standard et des règles européennes de haute 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 croissance. Ainsi, 15 millions d'utilisateurs néerlandais vont migrer de leur solution actuelle vers Wero, car ils avaient besoin d'une solution plus moderne couvrant tous les usages, notamment le commerce physique, l'intégration de cartes de paiement internationales, ou le paiement de factures. Au Luxembourg, par exemple, les factures sont payées via un QR code. Le plus important, pour nous, est d'offrir au consommateur tout en lui garantissant un contrôle total de ses données ».

« Au-delà du cadre national et européen, nous devons utiliser les meilleures pratiques qu'offre le paiement de compte à compte pour les paiements à l'international. Aujourd'hui, dans le monde, 64 initiatives comme la nôtre. PIX au Brésil, ou encore le PIX au Mexique, sont très appréciés des consommateurs en raison du lien entre le compte bancaire et le paiement mobile. PIX a même dépassé Visa au Brésil ».

« Wero se déploie progressivement, marché par marché, et cas par cas, en fonction de l'usage. Ce mois-ci, les premières transactions e-commerce seront possibles en Allemagne et la Belgique. Grâce à notre coopération avec d'autres solutions, Wero est déjà capable de couvrir 130 millions de consommateurs sur 13 marchés. C'est une première de couvrir rapidement l'Europe et d'être un partenaire crédible pour les paiements internationaux, car la prochaine étape est l'interopérabilité mondiale ».

Preuve de l'omniprésence des hyperscalers et de la difficulté à déployer une solution intégralement souveraine, l'European Payments Initiative, le consortium Wero, a reconnu auprès de netzpolitik.org qu'une partie des données de Wero sont hébergées sur des serveurs d'Amazon ⁽¹⁵⁷⁾.

Enfin, en complément des initiatives mentionnées précédemment, se situe le lancement de l'**euro numérique**. Ce projet, qui est porté par l'Eurosystème 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 les États européens. Selon la Banque de France ⁽¹⁵⁹⁾, « le Conseil a adopté une position favorable au projet en décembre 2025 et les négociations sont en cours au Parlement européen. L'adoption est attendue en mai 2026. Si les législateurs s'accordent sur le fondement juridique de l'euro numérique cette année, cela signifie qu'un pilote restreint verra le jour en 2027 et que, suite à une décision de la BCE des gouverneurs de la zone euro, le Conseil des gouverneurs de la BCE, une entrée de l'euro numérique pour les paiements entre commerçants en Europe verrait le jour en 2029 ».

La stratégie de réduction de la dépendance aux acteurs européens du secteur repose sur la diversification des options offertes au consommateur.

produits Microsoft est généralisée, créant de ce fait une vulnérabilité à grande échelle. Les acteurs sont concernés, administrations comme entreprises privées

– Dans le domaine des logiciels « tertiaire », certaines solutions de virtualisation ou le traitement des bases de données constituent le socle de l'application applicatif des systèmes d'information des entités publiques et privées gérant des données importantes. Ces solutions sont substituables, mais à la condition d'une migration longue et coûteuse.

– La situation est contrôlée dans le domaine des SI industriels des entreprises 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 loi, est au centre, se traduit par le recours quasi-exclusif à des clouds internes ou externalisés et labellisés SecNumCloud. Des cas de non-conformité à la doctrine ont toutefois été constatés. Les opérateurs d'importance vitale se trouvent dans une situation de vulnérabilité en ayant davantage recours à des solutions de clouds américains.

– Le point de vulnérabilité le plus critique concerne le secteur des services publics aujourd'hui majoritairement appelés à des solutions américaines pour les 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.

– 1 –

DEUXIÈME PARTIE : LA PROFONDEUR DES VULNÉRABILITÉS ÉCONOMIQUES ET RISQUES SYSTÉMIQUES POUR LES PERSONNES ET LES SERVICES PUBLICS

CHAPITRE 3 – FUITES DE VALEUR ET GASPILLAGE D'ARGENT : LA CONTRIBUTION DES GAFAM À L'ÉCONOMIE FRANÇAISE

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

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

passive, à l'instar de l'eau ou de l'électricité, et que nous ne laisserions pas les acteurs étrangers gérer à notre place. Or, le cloud n'est pas passif ; il nécessite un lancement à partir de laquelle se déploie un large éventail de services numériques des données et d'applications commerciales qui nous ont rendus dépendants de ces niveaux, y compris les entreprises, les administrations et la vie quotidienne. Nous ne pouvons 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 résilience, mais de croissance économique. En effet, si vous ne captez pas les données sur laquelle reposent vos services, vous envoyez des montants considérables à l'étranger, vous auriez pu investir en Europe. Nous savons tous que la productivité en Europe est beaucoup plus lentement que celle des États-Unis, essentiellement en raison d'un manque d'investissement technologique. Dans ce domaine, nos investissements sont bien inférieurs, 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 l'étranger, le capital américain. Nous devons donc utiliser nos capacités propres, qui sont énormes, d'autant plus que l'Europe dispose également de nombreux talents. » ^([61])

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

- quelle place occupent les acteurs états-uniens dans le secteur des logiciels 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 imputée à la France ? Quelles sont les retombées en matière fiscale ?

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

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

1. Secteur des logiciels : les filiales françaises de Microsoft et Oracle et les éditeurs français

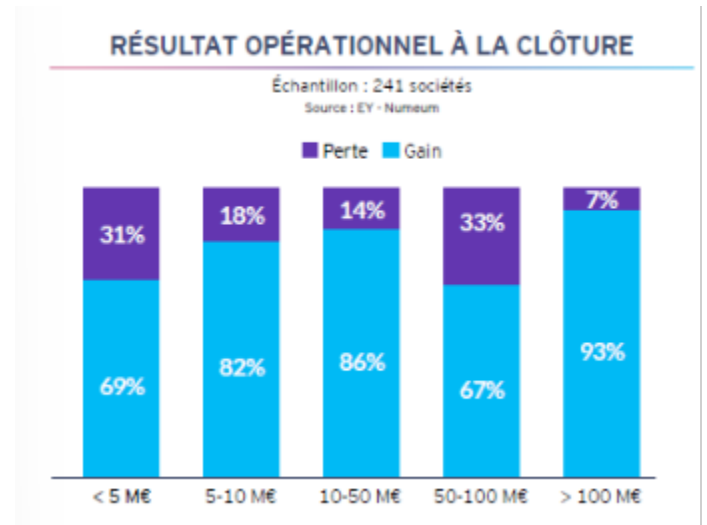
L'étude réalisée par Numeum sur les 250 plus grands éditeurs de logiciels en France comporte des données très précises sur le positionnement économique des entreprises. L'intérêt de l'étude est qu'elle se concentre sur les sociétés ayant déclaré ne pas appartenir à un groupe étranger. L'étude dresse le constat suivant :

- le chiffre d'affaires réalisé par les développeurs de logiciels professionnels (activités de conseil) était de 23,1 milliards d'euros en 2024. Parmi eux, les entreprises américaines représentent 14,4 milliards de chiffre d'affaires (62 %), contre 5,5 pour les entreprises françaises, horizontales et 3,2 milliards pour le segment des logiciels aux particuliers et professionnels.



Source : Numeum.

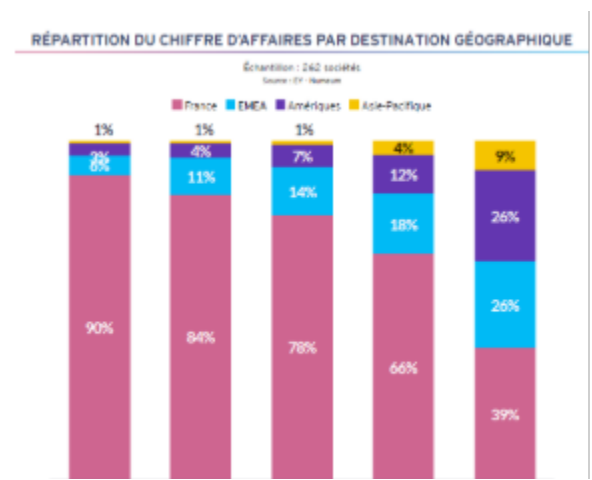
– la rentabilité des éditeurs pose question : si 79 % ont ré d'exploitation en 2024, c'est le cas de 93 % des éditeurs de plus de 100 millions de chiffre d'affaires, mais de seulement 66 % des éditeurs de chiffre d'affaire et 100 millions. Ces chiffres sont à comparer à ceux de l'ensemble des entreprises : la part des PME et des ETI déclarant un bénéfice était de 78 % en 2021, et des entreprises de 76 % ⁽⁶³⁾ ;



Source : Numeum.

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

– 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 est en fait le résultat de fortes disparités : l'internationalisation repose surtout sur quelques géants. Les 10 premiers éditeurs du classement — Dassault Systèmes, Criteo et Ubisoft — contribuent à l'internationalisation du secteur avec près de 9 milliards d'euros de chiffre d'affaires à l'international ». Le niveau d'internationalisation décroît fortement avec la taille d'entreprise.



Éditeur	Chiffre d'affaires (M€)	Nombre de salariés	Rang Top 100 fr
Microsoft France	4 744	2 021	
SAP France	1 376	1 658	
Oracle France	972	922	
VMWare France	159	422	
Red Hat	115	419	

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, 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 de l'édition sont insuffisamment positionnées dans d'autres zones géographiques. Le chiffre d'affaires par les principales d'entre elles est comparable à l'activité des leaders mondiaux sur le 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 secteurs confondus (catégorie « M73Z2 Régies publicitaires de médias »), à 5,2 milliards d'euros.

Le tableau ci-dessous présente les chiffres de l'activité réalisée par les acteurs internationaux, comparés à ceux de la plateforme française Dailymotion. Les sociétés Google France, Facebook France et Amazon online France SAS sont des acteurs publicitaires 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 est faible : seule la société Dailymotion a été incluse dans l'analyse.

Le chiffre d'affaires combiné de Google, Facebook et Amazon dans le secteur de 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 / salarié
Google France	1 747	971	
Facebook France	1 022	389	
Amazon online France SAS	983	205	
Tiktok France	78	263	
Linkedin France	65	159	
Dailymotion	54	239	
Twitter France	9	24	

Source : DGFIP, réponse aux questionnaires de la rapporteure.

Ces éléments illustrent le poids économique de ces trois acteurs sur le marché des plateformes en ligne, sans aucun acteur français comparable. Le nombre de salariés de 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, mais 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 secteur. Les chiffres de l'activité cloud de Microsoft ne sont pas disponibles car nous ne disposons pas de données précises sur ce secteur.

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

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

La rapporteure a souhaité mesurer la valeur ajoutée de l'activité réalisée par les entreprises américaines du numérique afin de mesurer leur contribution réelle à l'économie. À partir des chiffres transmis par 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 entreprises américaines) – Autres achats et charges externes ou achats de marchandises. L'estimation ainsi calculée a été comparée aux chiffres agrégés du secteur en 2022 fournis par l'INSEE. Ces éléments sont repris dans le tableau ci-après.

	Valeur ajoutée sur chiffre d'affaires (%)
<i>Secteur du logiciel – France (*)</i>	49 %
Microsoft France	18 %
Oracle France	28 %
<i>Secteur des plateformes et du cloud – France</i>	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 nettement inférieur à la moyenne du secteur, notamment pour Microsoft (18 % contre 49 % pour le secteur de l'édition de logiciels), Facebook et Amazon online (19 % et 9 % contre 42 % pour le secteur de l'activité de traitement de données). Par comparaison, ces taux sont de 65 % pour OVH.

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

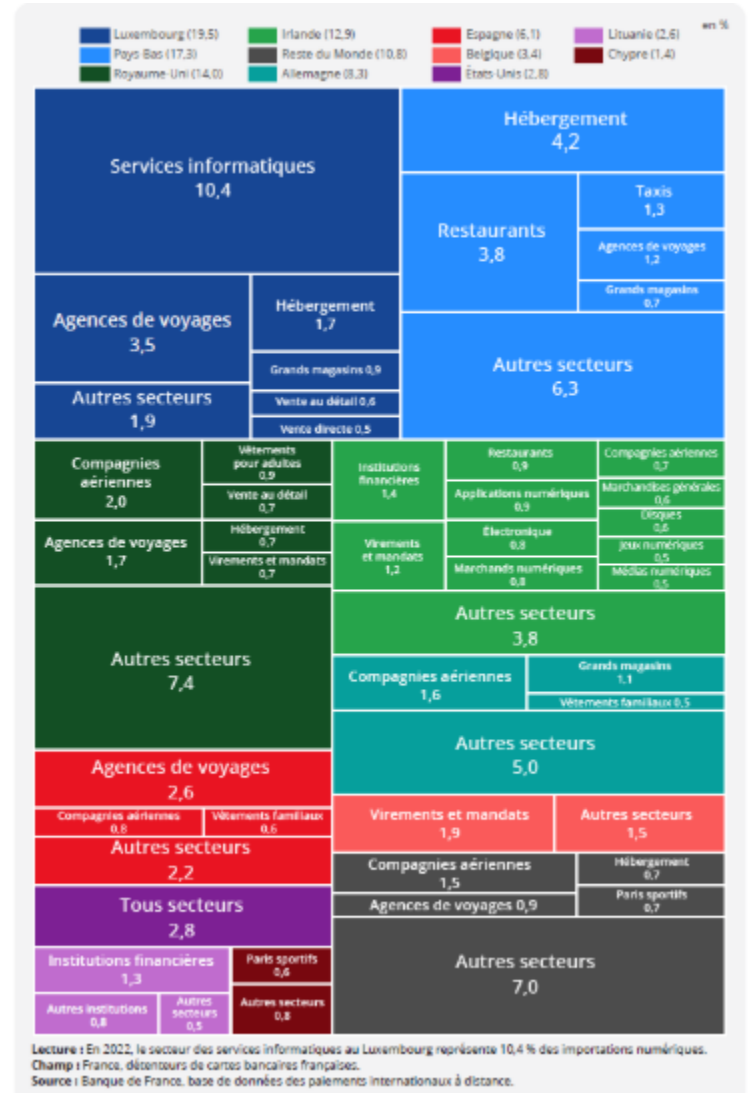
2. Des recettes d'impôt sur les sociétés très faibles compensées par la taxe sur les services numériques

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

Dans le respect 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.

France fait ressortir l'importance prise par quelques États membre d'exportation de services numériques traduit l'implantation de sièges de grandes plateformes mondiales. Ainsi que l'indique l'étude, « le siège européen d'Amazon se trouvent au Luxembourg, ceux de Meta et Google à D, ceux de Booking.com et d'Uber à Amsterdam ». Le graphique ci-dessous chaque pays dans les importations numériques françaises.

RÉPARTITION DES IMPORTATIONS NUMÉRIQUES EN FRANCE PAR PAYS ET SE



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

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

L'étude du cabinet Asterès « La dépendance technologique aux services américains : une estimation des conséquences économiques en Europe sur les 25,7 milliards d'euros d'importations françaises dans le domaine des services informatiques (computer services) comptabilisées par l'OMC, 7,4 milliards proviennent des États-Unis, 2,4 milliards des États-Unis.

Ces chiffres témoignent d'un modèle dans lequel l'essentiel de la localisée offshore. La société Microsoft France SAS agit par exemple commercial, et non comme une société de développement logiciel à proprement

le compte de résultat », même s’il convient de noter que : « Dans le cadre de Google LLC, Google France réalise une activité de recherche et développement. Les dépenses en 2024 ont été comptabilisées pour un montant de €148,770,639 v 2023. » ^([72])

**C. LES DÉPENSES DE LOGICIELS : 1,5 MILLIARD D’EUROS PAR AN
ACTEURS EXTRA-EUROPÉENS, 1 MILLIARD DE DÉPENSES SUBS
AUJOURD’HUI**

En avril 2025, le cabinet Asterès publiait une étude remarquée par Cigref, qui concluait que les entreprises américaines représentaient 80 % de logiciel en France ^([73]). Aucune étude similaire n’avait été conduite pour les a

Combien l’État dépense-t-il chaque année en licences auprès de Mic la part des logiciels américains dans les achats des administrations ? Aussi ces questions, aucun chiffre, ne serait-ce qu’estimatif, n’existait avant le c commission d’enquête.

Afin d’établir un diagnostic étayé, la commission d’enquête a d’informations précises sur les montants dépensés par les administration l’achat de licences logiciels, et a ainsi collecté des données par trois canaux d

– les réponses aux questionnaires adressés directement aux adminis Ces dernières devaient lister dans un tableau les dépenses de développement conditions opérationnelles de leurs applications métiers ainsi que les dépen leurs logiciels support ;

– un recensement effectué par le gouvernement dans le temps d’enquête, avec l’appui de l’Ugap, de la Dinum et de la direction des achats d

– les chiffres des achats réalisés par l’Ugap pour le compte d publiques.

Ces trois sources ont ainsi permis de disposer de la vision la plus c des achats effectués et de la part des logiciels extra-européens dans les solu 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 d’euros, inférieur au montant des dépenses numériques de l’État déclaré personnes auditionnées par la commission d’enquête (4,2 milliards). Ce recen pas exhaustif, mais donne toutefois une vision globale de la répartition des a dépense et de la part des fournisseurs extra-européens sur chacun des postes.

**POSTES DE DÉPENSES NUMÉRIQUES DES ADMINISTRATIONS ET PART DES FOURN
EUROPÉENS**

Poste de dépenses	Montant annuel	P
-------------------	----------------	---

658 millions d'euros), mais occupent une position très forte sur le segment support.

2. Dépenses de logiciel : le très fort positionnement des acteurs extr

a. Données des administrations d'État

L'estimation des dépenses de logiciels des administrations publiques provient de deux sources :

- les réponses aux questionnaires recueillies par la rapporteure. Le périmètre des administrations d'État, auquel s'ajoutent quatre établissements publics administratifs (France Travail, la Cnam, la Cnav et la CAF) et l'AP-HP, établissement de santé. Ce périmètre n'est pas exhaustif mais couvre les principales administrations de services publics nationaux. Certaines administrations sollicitées ont fourni des chiffres selon des périmètres incomplets (ministère de l'intérieur : direction de la police nationale uniquement) ;

- les chiffres transmis par la Dinum sur les achats publics ; ils concernent les dépenses réalisées auprès de l'Ugap ou renseignées dans le logiciel Chorus. Ce périmètre couvre exclusivement les administrations et exclut les opérateurs de l'État et le secteur large que celui couvert par la commission d'enquête.

Les dépenses de logiciels reflètent les dépendances techniques constatées. 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, pour 17,1 et 12,6 millions d'euros en 2025 sur le périmètre de la commission d'enquête (98 millions pour la Dinum).

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

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

b. Ensemble du secteur public

Par son positionnement auprès de l'ensemble des administrations, l'Ugap dispose d'une visibilité importante. Lors de son audition devant la commission d'enquête, M. Edward Jossa, président de l'Ugap, a souligné la pénétration des logiciels souverains dans les achats publics, qui serait dû notamment aux efforts de promotion : « *Nous travaillons sur les outils de distribution. Avant même les commissions d'enquête, nous avons des fiches numériques qui permet d'identifier les solutions souveraines, notamment sur le marché cloud. Sur la base de ces fiches produit de logiciels pour indiquer si les éditeurs sont de nationalité française – au sens de la loi sur la maison mère. Nous travaillons actuellement sur un outil d'intelligence artificielle d'aide à la décision pour sélectionner le logiciel qui correspond le mieux à leurs besoins. Les questions de sensibilité des données et de souveraineté* ».

« *Quels sont les résultats de cette politique ? Sur le marché des multi-éditeurs, nous sommes passés de 224 à 294 pour les autres éditeurs de l'Union européenne – ils comptent aussi en matière de chiffre d'affaires, peut-être le volume des ventes : en volume, entre 2024 et 2025, nous sommes passés de 595 millions d'euros à 64 millions pour les Européens non français. S'agissant des logiciels, nous vendons des solutions pour 55,5 % des ventes totales de logiciels de l'Ugap – Microsoft et Oracle compris. Nous voyons 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 : « *de logiciels passées en 2025 par l'État et les collectivités par l'intermédiaire de l'Ugap – c'est de 4,2 milliards d'euros – concernaient des éditeurs français ou européens.* » ⁽¹⁷⁴⁾

Les pourcentages de 55,5 % (audition de M. Jossa) et 54 % (audition de M. Amiel) étant en contradiction, Asterès pour le compte du Cigref, et, de manière générale, avec les constats qualitatifs convergents, ne dispose 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 classification des nationalités des fournisseurs. La centrale d'achat a dû procéder à des traitements manuels pour corriger ces erreurs : les éditeurs de logiciel étaient ainsi considérés à tort comme européens car la tête de groupe internationale était basée en France, alors qu'une analyse plus fine et manuelle révélait que les sociétés étaient bien des filiales d'entreprises étrangères.

Quel est le résultat final des calculs ?

Nous ne disposons finalement pas d'un chiffre global pour l'ensemble des achats logiciels de l'État. En l'absence de la classification automatique par nationalité des éditeurs, cette information est disponible seulement pour les fournisseurs de logiciels.

Le tableau ci-dessous présente les dix fournisseurs de logiciels les plus importants en termes de chiffre d'affaires. **Il est situé en première position avec 293 millions d'euros de chiffre d'affaires en 2025, soit 22 % du total, avec respectivement 69 et 61 millions de chiffre d'affaires.** Parmi les dix principaux fournisseurs, 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 RÉALISÉS EN 2025

En M€	Ministères	Collectivités territoriales	Établissements publics	Santé
-------	------------	-----------------------------	------------------------	-------

Astères.

Peut-on en déduire un chiffre pour l'ensemble des achats réalisés par l'Ugap pour le c l'hypothèse, très conservatrice, qu'aucun fournisseur hors du Top 50 n'était américain, on aboutit l'Ugap de 46 %. Avec une hypothèse raisonnable de 50 % ^([75]), cette part serait de 73 %.

Quant aux fournisseurs français, leur chiffre d'affaires auprès de l'Ugap est bien en forte au **disponibles pour le Top 50 (17 %), il est fort probable que les pourcentages de 54 et 55,5 % m 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 s 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
- les choix de logiciels effectués conduisent-ils à des situations de *vendor lock-in*, c'e propriétaires, dans lesquelles les fournisseurs seraient à même de dicter leurs conditions commerciales

a. Montant des dépenses logicielles des administrations au profit des acteurs extra-européens

Ainsi que la rapporteure l'a expliqué précédemment, les dépenses de logiciel constituent 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 fournisseurs américains (83 %) ^([76]) ;
- 361 millions d'euros d'après le recensement du gouvernement, dont 268 millions (74 %) ^([77]) ;

Pour l'ensemble des administrations (incluant les collectivités territoriales, les établissements de santé), les seuls chiffres disponibles sont ceux de l'Ugap. Ces données ne permettent pas un ch centrales d'achat davantage tournées vers les collectivités comme la Centrale d'achat du numérique établissements de santé comme l'Union des hôpitaux pour les achats (UniHA). Ils permettent cepen d'illustrer l'importance des dépenses auprès des acteurs non-européens. De plus, l'Ugap a commun part de marché sur le segment des achats de logiciels pour les administrations. En 2024, l'Uga commandes dans les logiciels, pour une taille de marché estimée à 2,950 milliards d'euros par l'ent pour l'Ugap qui peut être estimée à 40 %.

Le montant des achats via l'Ugap auprès des entreprises américaines en 2025 était au m vérification manuelle de la nationalité des groupes présents dans le top 50 des fournisseurs, soit 79 **de l'Ugap représente 40 %, on peut estimer le montant minimal d'achats auprès des entrepr environ.**

b. Montant des dépenses logicielles substituables

Les principales solutions achetées disposent d'alternatives en open source, au moins partie administrations et des opérateurs font ainsi état de transitions engagées ou en réflexion vers les soluti

- pour les solutions de bureautique : les solutions libres de type LibreOffice, ou les produits c

Gouvernement	Ministères. Dépenses de logiciels « pour les DSI » et « environnement de travail »	361	268 (74 %)	
Ugap	Achats logiciels Ugap	1 333		609 sur 769 (79 %) pour le top 50 fournisseurs
Extrapolation Ugap	Ensemble des administrations à partir de taille de marché de l'UGAP	3 300		1 500

Note : la part substituable est définie ici comme l'addition des dépenses pour des solutions fournies par Microsoft, VMWare, Oracle, et IBM, pour les administrations identifiées lors des auditions.

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

Modèle singulier parmi les administrations, la gendarmerie nationale a procédé à un basc source. Elle a ainsi limité son budget annuel de licences pour des solutions propriétaires à un million SAP. La commission d'enquête a auditionné le directeur de l'Anfsi, afin de disposer d'élém basculement vers des solutions open source. **Elles sont estimées à 534 millions en cumulé depuis 2**

« [Sur] le plan financier, nous avons évalué les économies générées par cette stratégie, qu' smartphones professionnels, équipés d'un système d'exploitation souverain. Ce choix technique n téléphones des directeurs généraux de la gendarmerie et de la police nationales ont ainsi été Pegasus. Depuis 2004, ces dépenses évitées s'élèvent précisément à 534 millions d'euros. Dans un argument de poids. » ^([78])

Le basculement vers des solutions open source entraîne des coûts de gestion de projet, au r d'accroître les besoins en main-d'œuvre en phase d'exploitation. En effet, les solutions ne sont gér services supports moins disponibles. Il conviendrait ainsi de vérifier que ces dépenses évitées compr

Les dépenses réalisées auprès du fournisseur Microsoft étant les plus importantes, le bureautique est le plus à même de dégager des économies importantes. Ainsi, pour la DGFIP, l'écon par an. Selon le chef du service des systèmes d'information, « bien que nous n'ayons pas réalisé d'e libre, l'exemple de LibreOffice est révélateur puisque son coût annuel est quasi nul là où une 10 millions d'euros par an. Pour un usage courant, nos enquêtes annuelles de satisfaction révèlent équivalentes » ^([79]).

Selon les estimations de la DSI du CNRS, la migration des solutions Microsoft vers des collaboratifs permettrait également de réaliser des économies significatives. « Pour le CNRS, cela annuels uniquement pour la partie espaces collaboratifs SharePoint. Pour la messagerie, c'était, de basculant chez Renater, cela nous coûtera 600 000 euros par an. Économiquement, il est extrême ces sujets. » ^([80])

Les dépenses de logiciel pour des produits propriétaires extra-européens représentent 300 millions d'euros pour les administrations d'État et les grands établissements publics, e administrations.

Les travaux de la commission le montrent, des solutions de substitution open source ex cas. Les montants estimés de dépenses publiques substituable par des solutions open sour minima de 185 millions et sur le périmètre de l'ensemble des administrations de 1 milliard exhaustifs, les dépenses publiques évitables sont probablement beaucoup plus importantes.

Comme cela a été mentionné précédemment, ces chiffres croisent des recensements effec d'entre eux n'étant exhaustifs. Une analyse approfondie devrait être conduite afin de disposer d'

FRANCE			
BUREAU VAN DIJK EDITIONS ELECTRONIQ	5	15	20
ADOBE	13	15	15
PEGASYS FRANCE	6	14	15
DOCAPOSTE	10	12	18
CEGID	233	293	13

Source : Ugap.

La commission d’enquête a examiné l’évolution des dépenses pour les six ^([81]) principaux fournisseurs comparant les dépenses 2025 à la moyenne des dépenses 2023 – 2025 ^([82]).

D’après les chiffres transmis à la rapporteure par les administrations, les hausses constatées entre 2025 et la moyenne des dépenses 2023 – 2025 sont comprises entre +7 % (Oracle) et + 46 % (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 fonctions de leur champ d’action réduit ;
- des hausses des prix unitaires des services, de façon unilatérale ou à l’occasion de nouveaux contrats pluriannuels.

La frontière entre les deux est parfois poreuse, lorsque les éditeurs pratiquent le *bundling* de fonctionnalités dont ils n’ont pas besoin.

Les fortes hausses de prix, liées aux pratiques tarifaires des principaux acteurs du logiciel, ont été abordées lors d’une table ronde réunissant les directeurs des systèmes d’information de quatre grands organismes de recherche : CNRS et l’Inrae.

« Côté CEA, nous venons de renégocier notre contrat Microsoft pour trois ans. L’ordre de grandeur de l’augmentation de Microsoft demande de ne pas communiquer sur les augmentations, mais je peux vous dire que l’augmentation est à deux chiffres, de l’ordre de 20 % sur trois ans, ce qui est bien supérieur à l’inflation (bundle) en incluant des produits que nous n’utilisons pas. C’était le cas de Teams, que nous n’avons pas été obligés de payer. Une décision de la Commission européenne les a contraints à sortir Teams du lot des logiciels à 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 augmentations sont significatives et pèsent sur le budget de l’État » ^([83]).

« Vous posiez la question des migrations auxquelles on pourrait renoncer à cause du coût. Or, si les éditeurs ont annoncé une augmentation de 50 % ou 60 % des coûts du jour au lendemain, nous nous sommes

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 monétaire, avec 40 % du total des hausses, contre 34 % pour les services IT, 21 % pour le hardware et 6 % pour les applications ;
- les entreprises françaises sont confrontées à des hausses de tarif importantes, supérieures à l'inflation, liées aux stratégies de *vendor lock-in* des éditeurs de logiciel, consistant à proposer des prix de licence élevés, à imposer leurs solutions propriétaires et s'assurer ensuite des revenus récurrents : « *concernant les entreprises de la Vanson Bourne – Asterès, conduite en 2022, a révélé que près de 90 % des entreprises françaises étaient touchées par ce type de pratique, selon l'hypothèse de durée du contrat, soit supérieures de plusieurs points à l'inflation. Ces résultats ont été recueillis par le Pr. Jenny, selon lesquels les prix des licences des logiciels sont " initialement compétitifs et augmentés au moment du renouvellement (vendor lock-in) ».*
- prises dans des négociations déséquilibrées, les entreprises clientes se voient imposer des conditions défavorables, groupées, qui contribuent à la hausse constatée des tarifs :

« *Concernant les ventes groupées, l'enquête Vanson Bourne – Asterès, conduite en 2022, a révélé que 80 % des entreprises s'étaient déjà vues proposer une offre groupée, avec un différentiel de coût de 26 % en moyenne par rapport aux tarifs individuels, certains répondants. Ces résultats sont confortés par l'analyse du Pr. Jenny qui, en analysant les pratiques des fournisseurs, a quantifié des majorations pouvant atteindre 90 % pour Office 365 et 300 % pour Salesforce. L'Elée, qui illustre ce type de pratique avec l'exemple de VMWare : « la fusion de milliers de références en une seule, entraîne 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 belges et néerlandaises, membres ou partenaires du Cigref ^([88]), qui confirment la vulnérabilité de ces entreprises face aux hausses des principaux éditeurs de logiciels :

« ***Les répondants déclarent une hausse moyenne du coût de leurs services de cloud-logiciel de 12 % par an sur les cinq prochaines années. La hausse la plus élevée atteint 51 % en moyenne, avec des cas extrêmes déclarés à 100 %, voire 200 à 300 % pour certains. L'accélération de l'inflation tarifaire depuis la première enquête Asterès – Vanson Bourne de février 2018, de 5,8 % par an. Le rythme d'inflation a ainsi progressé de près de trois points en quatre ans, et les cinq prochaines années s'inscrivent dans la continuité de cette trajectoire (...). Les hausses les plus importantes concernent les logiciels de productivité et de collaboration et les logiciels de socle technique et sécurité (...). Ces pratiques commerciales potentiellement abusives : vendor lock-in (40 % des répondants s'en disent victimes), l'IA by-design (32 %), l'obsolescence programmée (30 %), la bundlisation (26 %) ou encore la réduction des marges (26 %).***

L'étude du cabinet Asterès prolonge l'analyse en décrivant les impacts potentiels de telles hausses sur les grandes organisations, et de manière générale sur leur activité : « *les hausses tarifaires se traduisent par une réduction d'autres postes de dépenses. Le budget numérique représente 4,1 % du chiffre d'affaires (contre 2,8 % de leur contribution au Produit National Brut, pour les administrations). 28 % de ce budget est consacré à la trajectoire inflationniste tendancielle actuelle, cette proportion pourrait monter à 42 % à l'horizon 2027, concentrée : les cinq premiers fournisseurs captent à eux seuls 53 % du budget cloud-logiciel des entreprises, la quasi-totalité d'entre eux. Les hausses tarifaires du cloud-logiciel modifient profondément la structure des dépenses des organisations sur les cinq dernières années, avec la part moyenne des OPEX portée à 50 %, ce qui est une hausse de 10 points par rapport à 40 % en 2018, selon les répondants. Pour absorber ces hausses, 47 % des répondants déclarent réduire leurs autres dépenses, contre 28 % en 2018. Sur le budget numérique global, 14 % réalisent des gains de productivité et 6 % en répercutent le coût sur d'autres postes, augmentant leur budget numérique, les autres dépenses réduites en priorité sont la R&D et l'investissement (14 %), les marges (26 %), le recrutement (21 %) et les augmentations de salaires (12 %) ».*

Les dépenses auprès d'acteurs extra-européens n'apportent aucun bénéfice particulier à 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 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 de régulation. Le modèle numérique généré en France ne pourra pas contribuer au financement des services publics et de la protection des données numériques, qui génère 542 millions d'euros de recettes auprès des grandes plateformes extra-européennes pour contrebalancer leur modèle tourné vers l'activité offshore. En l'absence de dispositif de régulation, le modèle numérique génère pour le moment aucun retour pour la collectivité, si elle est le fait d'un acteur extra-européen.

– 1 –

CHAPITRE 4 – ATTEINTE AUX DROITS DES PERSONNES : UN MODÈLE FONDÉ SUR LA MONÉTISATION DES DONNÉES PERSONNELLES

La domination de grandes entreprises numériques étrangères affecte également la capacité de l'Union européenne de son droit et le développement de services conformes à ses valeurs. Selon le directeur général de la Commission européenne, c'est une menace directe pour la souveraineté européenne, à savoir la capacité à « *appliquer notre droit, à protéger nos données choisies dans l'expression de la souveraineté définie par notre Constitution, et de ne pas subir les règles imposées par d'autres* ». Nous n'aurions pas voix au chapitre, ce qui renvoie à toute la question du droit extraterritorial. » Si l'Union européenne est un tournant, en imposant le respect de standards de sécurité et de confidentialité élevés aux entreprises numériques, l'Union européenne, il est encore largement contourné par des plateformes qui fondent leur enrichissement sur les données personnelles et leur commercialisation à travers la publicité ciblée.

A. UN HÉBERGEMENT DES DONNÉES PERSONNELLES SUR LE TERRITOIRE AMÉRICAIN CONDUIT À DES VIOLATIONS DE LEUR VIE PRIVÉE

Du fait de leur recours aux services des *hyperscalers*, un volume considérable de données personnelles des citoyens européens trouvent hébergées dans des centres de données américains, avec un niveau de protection inférieur à celui de l'Union européenne. L'ont montré les décisions successives de la Cour de justice de l'Union européenne concernant les transferts de données personnelles.

1. Des transferts transatlantiques invalidés à plusieurs reprises par le juge européen en raison de violations fondamentales

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 qui ne garantit pas un niveau de protection adéquat. Si la Commission européenne constate qu'un pays tiers ne garantit pas un tel niveau de protection, elle ne peut prendre les mesures nécessaires pour empêcher toute transmission de données personnelles vers ce pays tiers. Si la Commission constate qu'un pays tiers assure un niveau de protection adéquat, en raison de sa législation interne ou de son cadre des négociations avec l'Union européenne, la Commission peut autoriser les transferts de données personnelles d'adéquation.

La décision d'adéquation du 26 juillet 2000 dite *Safe Harbour* a ainsi permis, pendant plusieurs années, le transfert de données personnelles des citoyens européens vers les États-Unis, avant qu'elle ne soit jugée invalide par la Cour de justice de l'Union européenne.

insuffisantes, relevant notamment le manque d'indépendance de l'ombudsman et l'absence de contrôle de renseignement américaines.

L'arrêt de la Cour a marqué un tournant, selon la présidente de la Cnil, Mme Marie-Laure Dastès : *« L'arrêt américain portait une atteinte disproportionnée à la vie privée des Européens, la Cour a remis les données vers ce pays et de facto vers les fournisseurs de services numériques soumis au droit états-unien. Cette décision ont mis en lumière l'extrême dépendance de nos administrations et des entreprises – hébergement, services d'informatique en nuage, outils de cybersécurité, outils bureautiques ou d'analyse – envers les États-Unis »*.

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 révisé le **cadre des activités de renseignement des États-Unis**. Le décret a notamment renforcé les garanties pour les Européens qui allèguent de la collecte et de l'utilisation illicite de leurs données personnelles à des fins de sécurité nationale. Il est prévu que la plainte soit transmise par les autorités européennes de Protection Officer du Bureau du directeur du renseignement national américain, qui sera chargé de vérifier si les données ont été violées et, le cas échéant, de déterminer les mesures correctives contraignantes appropriées. Il est prévu que la DPJC, créée par un règlement du Procureur général du 7 octobre 2023 et composée de juges fédéraux, 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 consommateurs.

De fait, il « *repose largement sur des garanties extralégislatives américaines – des courtes promesses –*, explique Max Schrems. *Car en pratique, comme me le signalait un parlementaire américain, le Congrès américain une loi visant à accroître les droits des étrangers, pour des raisons politiques »*. Le cadre est donc rapidement, en fonction des changements politiques, sans que l'administration ait besoin d'obtenir l'approbation du Congrès.

Il marque d'ailleurs **peu de progrès substantiels par rapport au précédent accord conclu en 2016**. *« En matière de relations publiques, la Commission européenne a géré ces questions de manière très habile, mais elle n'a pas communiqué de presse la signature de nouveaux décrets, sans préciser que ceux-ci n'étaient soumis à aucune condition. Les décrets signés sous la présidence de Barack Obama, dont les cours de justice avaient signalé l'insuffisance, ont été remplacés par ceux signés sous la présidence de Joe Biden. Les cours de justice ont d'analyse pour mesurer combien l'apport de nouveaux décrets était faible. Par exemple, la Commission européenne a introduit un principe de proportionnalité sur le modèle de celui prévu dans le droit européen. Les États-Unis introduisent un principe de proportionnalité sur le modèle de celui prévu dans le droit européen. D'interdire la surveillance de masse, dès lors que celle-ci est jugée disproportionnée par les tribunaux. À ce point, les États-Unis expliquent ne pas avoir la même définition de la proportionnalité que l'Union européenne. Les deux parties se sont accordées sur l'usage d'un terme, mais pas sur son sens. »* ⁽⁹²⁾

Dans le rapport qu'il a rendu en novembre 2024 sur le *Data Privacy Framework* ⁽⁹³⁾, le Comité européen pour la protection des données (CEPD) a noté qu'il restait encore à garantir l'effectivité du mécanisme de recours, compte tenu du fait que le cadre n'est pas encore pleinement mis en œuvre. Il a également appelé la Commission européenne à contrôler la mise en œuvre des principes de la loi américaine, et de suivre les évolutions futures liées à la loi américaine sur la surveillance de masse.

Pour ces motifs, le député Philippe Latombe, président de la commission d'enquête, a demandé à la **Commission européenne en vue d'obtenir l'annulation de la décision d'adéquation**. Sa requête vise à garantir l'impartialité et d'indépendance de la DPJC, qui a été créée par décret et non par une loi du Congrès ; d'autre part, sur la collecte massive de données personnelles de citoyens européens vers les États-Unis, sans contrôle préalable par un juge ou une administration ⁽⁹⁴⁾. Le Tribunal a rejeté la requête. Il a refusé un assouplissement des exigences par rapport à la décision *Schrems II* : il estime notamment que la loi américaine ne prévoit pas d'autorisation préalable systématique pour des collectes de données en masse, mais qu'un contrôle judiciaire est prévu. Le contentieux est toujours pendant, M. Latombe ayant introduit un pourvoi devant la CJUE.

Les géants du numérique, notamment les réseaux sociaux et les moteurs de recherche, ont collecté massivement des données personnelles à des fins de monétisation à travers la publicité ciblée. Cependant, pendant des années le RGPD pour augmenter leur patrimoine de données et renforcer leur position. Partiellement mises en conformité, elles utilisent désormais les données accumulées pour développer de nouveaux services sans avoir recueilli au préalable le consentement des utilisateurs.

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

Le **modèle économique de monétisation des données personnelles adopté par les grandes entreprises** a été critiqué par l'ensemble des chercheurs, associations et ONG auditionnés par la commission d'enquête. Les experts de la Commission Internationale sur l'impact du fonctionnement des grandes plateformes numériques sur les droits européens ont constaté que sur Facebook, ont montré « *l'existence d'un modèle économique commun, fondé sur un profilage des utilisateurs, basé sur des données personnelles et le recours à la publicité ciblée, qui constitue le moteur du fonctionnement de ces plateformes. Ce modèle fonctionne de manière constante puisque les plateformes cherchent en permanence à accroître la quantité de données collectées, toujours plus précis, destinés à être commercialisés auprès des annonceurs, tandis qu'elles recourent à des méthodes de plus en plus sophistiquées pour déduire des centres d'intérêt, voire des indicateurs de bien-être, comme c'est le cas pour les plateformes de médias sociaux à personnaliser les contenus, à maintenir les utilisateurs en ligne le plus longtemps possible et à remonter la spirale au détriment des droits humains* » ⁽¹⁹⁸⁾.

Ce ciblage repose le plus souvent sur le **dépôt de traceurs**, comme les cookies, sur le terminal de l'utilisateur, les 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 de données massives. La mesure de collecter des données personnelles grâce à son moteur de recherche Google Search, son navigateur Chrome, son service de géolocalisation Google Maps, ou l'application d'édition de contenus vidéos Youtube. De même, les entreprises disposent de millions d'utilisateurs à travers ses services de messagerie et de réseau social WhatsApp, Messenger, etc. Les données entre les différents services proposés, grâce à l'identifiant unique de l'utilisateur, leur permettent de lier les données. Ils peuvent ensuite être commercialisés auprès des annonceurs afin de choisir le contenu publicitaire à proposer à chaque personne.

C'est cet accès privilégié aux données qui **permet à Google de fonder sa domination sur le marché de la publicité** et **il participe à la fois en tant que régie publicitaire et que vendeur d'espace publicitaire**, comme le souligne la commission d'enquête : « *l'accès aux recherches effectuées par les personnes et à leur navigation internet – Chrome traque tout ce que l'utilisateur fait, sa localisation physique et à de nombreux autres paramètres en grand volume permet de deviner ce qu'ils font et de leur présenter une publicité correspondante et de se prévaloir d'un lien de causalité entre la publicité et la vente. On a montré la publicité n'a apporté aucune valeur à l'annonceur mais les grands acteurs peuvent se targuer d'être plus efficaces que les autres. Tout le système est organisé pour acheminer le maximum de données vers les grandes entreprises.* »

La masse de données détenues permet également aux entreprises de personnaliser leurs services à travers leur algorithme de recommandations, au risque de créer des biais discriminatoires ou de cibler des groupes vulnérables. La commission d'enquête n'a cependant pas traité la question des risques sur la santé et les droits fondamentaux des personnes d'ores et déjà démontrés par de nombreux travaux.

Ce profilage peut également être utilisé par des gouvernements afin de limiter l'exercice des libertés fondamentales. Les plateformes coopèrent à la mise en œuvre de dispositifs de surveillance de la population. Mereuse, la Commission d'enquête Signal, a notamment évoqué, lors de son audition, la communication par Facebook de messages privés à un cadre d'une enquête sur un avortement illégal : « *aux États-Unis, une femme a été incarcérée après avoir été accusée d'échange de messages sur Facebook entre elle et sa fille, dans l'État du Nebraska, après que cet État a été condamné après la décision Dobbs. Ces messages privés montraient qu'elle avait aidé sa fille à accéder à l'avortement.* »

Plusieurs enquêtes de la Cnil ont montré que les géants du numérique avaient adopté des cookies. De fait, **sur les 953 millions d’euros d’amendes prononcées par l’autorité sur le fond** **2019, 903 millions l’ont été à l’encontre des plus grandes plateformes étrangères**, « *non parce que 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-EU

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.
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, qui déposaient automatiquement des cookies à finalité publicitaire sur le terminal des utilisateurs dès qu’ils leur ont donné leur consentement. La Cnil avait justifié le montant des sanctions par le poids considérable de ces entreprises sur la recherche en ligne pour Google et 20 % du commerce en ligne pour Amazon –, dont les manquements concernaient des dizaines de millions d’utilisateurs. L’autorité avait souligné, en outre, les bénéfices considérables tirés par ces entreprises des 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 et Microsoft à hauteur de 60 millions également ⁽¹⁰⁴⁾, pour ne pas avoir permis à leurs utilisateurs de ne pas 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 pour avoir imposé des cookies lors de la création de comptes Google sans le consentement valide des utilisateurs : ces derniers n’ont pu accéder à l’accès aux services de Google était conditionné au dépôt de cookies, et étaient incités à choisir les cookies personnalisés plutôt que ceux liés à l’affichage de publicités génériques. La société Shein a également été sanctionnée à hauteur de 150 millions en raison d’un dépôt de traceurs dès l’arrivée des utilisateurs sur le site, sans leur demander d’informations sur la finalité publicitaire des traceurs, et d’un mécanisme de refus du consentement qui n’était pas fonctionnel.

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

En 2021, l’autorité luxembourgeoise a ainsi infligé une **amende de 746 millions d’euros** à Amazon pour avoir imposé à ses clientes personnelles des utilisateurs de sa plateforme de e-commerce en se fondant sur l’intérêt légitime de l’entreprise sans leur consentement.

SANCTIONS PRONONCÉES PAR LA DATA PROTECTION COMMISSION IRLANDAISE À L’ENCONTRE DES GRANDES ENTREPRISES EXTRA-EU

Date	Société	Montant de l’amende (en millions d’euros)
20/08/2021	WhatsApp	225

conditionner l'accès à leurs services à l'acceptation des cookies, le CJUE a estimé que la pratique pour fournir le service et que Facebook et Instagram étaient tenus d'obtenir le consentement de l'utilisateur avant d'accepter les cookies. Cette décision a été 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 la pratique consistant à bloquer l'accès à un site web ou à une application mobile aux personnes refusant les cookies. La Cnil a repris cette position dans ses lignes directrices de 2020 en prévoyant que « *le consentement ne peut être obtenu en mesure d'exercer valablement son choix et ne subit pas d'inconvénients majeurs en cas d'absence ou de retrait du consentement* ». Par une décision du 19 juin 2020, le Conseil d'État a cependant invalidé ce raisonnement, en jugeant que l'absence de consentement ne peut 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 au refus des cookies ^([108]). Elle indique par exemple que des services administratifs ne peuvent pas conditionner l'accès à l'information à l'acceptation des traceurs, puisqu'ils sont les seuls à proposer ce service. De même, l'instauration d'un service 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 prestation. Si, n'étant pas interdite en soi, la Cnil veille à ce que le tarif soit raisonnable pour qu'il y ait un véritable choix. Un *cookie wall* est limité aux finalités qui permettent une juste rémunération du service proposé (par exemple, la publicité) et ne peut pas être utilisé 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, sans le consentement des utilisateurs européens vers les États-Unis, en utilisant des clauses contractuelles types insuffisamment validées par la CJUE de la décision d'adéquation *Privacy Shield*.

Meta a également été sanctionnée plusieurs fois pour avoir manqué à son obligation de sécurité des données découlant de l'article 25 du RGPD : d'abord, en 2022, à hauteur de 265 millions, à la suite d'une fuite de données de millions d'utilisateurs de Facebook par un tiers grâce aux techniques de *scrapping* ; puis en 2024, à hauteur de 1,1 milliard, pour le stockage de mots de passe non cryptés et la fuite de données de trois millions d'utilisateurs européens.

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

Ces décisions successives ont conduit certaines plateformes à se mettre en conformité, mais la Cnil a constaté lors de son audition : « *L'objectif premier de la régulation de la Cnil a été d'offrir la possibilité à l'utilisateur de contrôler son premier écran. Cela a réclamé un travail de régulation méthodique mené durant trois ans en concertation avec les lignes directrices, puis, après avoir laissé un temps d'adaptation, lancement des contrôles et application de ces contrôles. Les sites se conforment aux règles : il est possible de refuser dès le premier écran – sur le téléphone – de cliquer sur "accepter", en général en haut à droite de l'écran. Nos contrôles se tournent désormais vers les interfaces qui tentent de contourner la règle à l'acceptation, à savoir le "continuer sans accepter" dans d'autres informations.* » ^([109])

De fait, les *dark patterns*, ou interfaces trompeuses, sont utilisées par les opérateurs pour manipuler les utilisateurs et les conduire à faire des choix qu'ils n'auraient pas effectués s'ils étaient pleinement informés. Ces interfaces multiples de confirmation de choix qui rallongent le parcours pour les utilisateurs qui ne veulent pas accepter, de cases précochées, de sollicitations répétées pour amener l'utilisateur à consentir à l'ouverture de comptes à rebours ou de messages d'urgence pour pousser à réaliser un achat... Comme l'a expliqué la Cnil lors de son audition, « *de nombreuses recherches montrent que ces dark patterns influencent les choix des utilisateurs. Nous avons mesuré leur impact sur le processus décisionnel de plus de 4 000 utilisateurs. Ces interfaces trompeuses modifient significativement la probabilité de consentement. Nous avons également constaté que ces interfaces sont utilisées de manière croissante par les opérateurs* ».

Facebook et d'Instagram pour entraîner ses systèmes d'intelligence artificielle. Les personnes peuvent 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 des vidéos, ou aux données de localisation de ses utilisateurs. Google assure que les contenus des emails qu'il génère sont contextualisés pour personnaliser l'expérience des utilisateurs, sans être i

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

L'Autorité de la concurrence constatait ainsi, dès 2024 ^([112]), que les *Big Tech* « *bénéficient d'un volume de données (ainsi, YouTube offre à Alphabet une source majeure de données d'entraînement pour ses vidéos). Elles peuvent également accéder à des données associées à l'utilisation de leurs services. Elles ont une capacité financière pour conclure des accords avec des propriétaires de données tiers. Google s'est ainsi engagé à verser (environ 55 millions d'euros) par an pour accéder aux données de Reddit, un site communautaire de discussions sociales* ».

En recourant au *web scraping*, ou l'extraction automatique de données accessibles sur le web, on œuvre ce que Mme Mélanie Dulong de Rosnay, directrice de recherche au CNRS, appelle un « *colonisme numérique* » dans ses travaux de Renata Avila, Nick Couldry et Ulises Mejias ^([113]) : « [il s'agit d']une nouvelle forme de domination s'exerce sur tous les types de données numériques – personnelles, privées, publiques, techniques, professionnelles, numériques. **La vulnérabilité provient des conditions d'utilisation des plateformes, qui imposent d'accepter de négocier. Ces termes transfèrent tous les droits à la plateforme.** Les modèles économiques du numérique reposent sur les masses de données. La vulnérabilité vient aussi des limites et des effets secondaires des licences libres. Elles sont des ressources dans des conditions proches du domaine public, ce qui est excellent du point de vue de la transparence, de la démocratie et de l'innovation, mais qui autorise l'extraction et l'appropriation de la valeur de la donnée, de la création ou à l'infrastructure, alors que les communs numériques sont produits grâce à des financements publics et des communautés. Nous sommes face au résultat d'une conception libérale de l'open data, revenant à une logique de captation, compris les grands acteurs du numérique, dès lors libres de les privatiser et d'en extraire la valeur. C'est un colonialisme. La captation des investissements et du travail bénévole ne suppose ici aucune contribution ».

Ces traitements seraient, en outre, réalisés par les grandes plateformes sans garde-fou sur l'usage des données, selon Meredith Whittaker ^([114]) : « *Les pratiques dominantes consistent à agréger des données, par exemple d'Alexa ou de Gmail, ainsi que des données provenant du web et de vos appareils connectés. Les données sont ensuite ajusté par des travailleurs, généralement faiblement rémunérés et localisés dans les pays du Sud, sous des contraintes de coûts qui pèsent sur ces entreprises, rien n'est véritablement conçu pour préserver la vie privée ou d'empoisonnement.* »

Le RGPD et la directive e-privacy continuent pourtant de s'appliquer et de pouvoir s'appliquer à des données à caractère personnel par les fournisseurs et les développeurs de systèmes d'IA. En 2024, les législateurs européens n'ont pas entendu « *modifier l'application du droit du RGPD aux données à caractère personnel* » comme il est précisé dans l'exposé des motifs ^([115]). Il y est ajouté « *le droit 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 du numérique, M. Max Schrems défend au contraire sa pleine applicabilité ^([116]) : « *On entend souvent dire que le RGPD est obsolète et qu'il est donc nécessaire d'adapter la loi à ces nouvelles technologies. Or, les valeurs et les principes qui structurent le RGPD, évoquaient déjà la possibilité que, dans le futur, les données soient utilisées de façons alors inconnues et servent à alimenter de gros algorithmes qui prendraient des décisions en fonction de la mesure de comprendre l'origine. C'est exactement pour cette raison que nous avons le droit d'accéder, de supprimer ou de faire corriger de fausses informations : le sentiment dominant, à l'époque, était déjà* ».

Ainsi, selon Mme Ramya Chandrasekhar, chercheuse au centre internet et société du CNRS, *européenne (dont les lois sur le copyright ou sur la protection des données) se voit ainsi contrelaquelle nos données sont tout simplement là pour être exploitées* ».

M. Schrems relève lui aussi une forme de **renoncement des autorités de protection des données d'IA, au risque de laisser se généraliser de graves atteintes à la vie privée** : *« quand l'IA est contrôlée par les régulateurs européens, y compris la Cnil – qui était habituellement un régulateur très fort sur bien d'autres domaines – tout autoriser, de peur de prendre du retard dans ce secteur. De ce fait, nous faisons maintenant face à des données et les utilise à des fins que nous ne pouvons pas contrôler, et que les entreprises elles-mêmes ne contrôlent pas. Une affaire en cours concerne par exemple un ressortissant norvégien dont l'intelligence artificielle a détecté que des enfants, maltraité sa femme et commis toute une série d'actes aussi horribles que fictifs. Or, quand nous demandons des informations produites par son algorithme, l'entreprise explique être techniquement incapable de fournir ces données. Les témoignages de cas similaires. Il s'agit souvent de journalistes qui, parce que leur nom apparaît en lien avec des affaires criminelles, sont mêlés par l'IA avec le contenu desdits articles et se retrouvent ainsi accusés d'avoir commis des agressions sexuelles. Que des compagnies de la Big Tech, qui engrangent des millions de données, ne puissent corriger ces erreurs ou de traiter le problème est affligeant. C'est précisément pour ces raisons que le RGPD figurent dans le RGPD. »* ⁽¹¹⁹⁾

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 capacité 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 ⁽¹²⁰⁾, a mis en évidence les **données (data brokers)**, c'est-à-dire les entreprises spécialisées dans la collecte, l'analyse et la vente de données. Contrairement aux grandes plateformes numériques, qui exploitent directement les données qu'elles collectent, les *data brokers* collectent des informations issues de multiples sources : achats en ligne ou en magasin (via les cartes de paiement), données mobiles (localisation, usages), ou encore historique de navigation sur internet.

« En réalité, quasiment toutes les applications sont concernées par la collecte de données. Les applications et des services qu'elles proposent étant gratuits, les outils sont financés par la publicité. Les données sont utilisées pour afficher et collecter des données afin de les cibler », a expliqué le journaliste M. Martin Untersinger.

Les données sont également recueillies par des entreprises tierces, via les briques logicielles qu'elles fournissent. Mme Nataliia Bielova, également auditionnée, observe ainsi : *« Ce que l'on observe, c'est la création de chaînes d'inclusion, dans lequel de nombreuses entreprises intègrent et dépendent des services des autres. Cette situation est liée à la nature dynamique du contenu web. Des composantes peuvent être chargées par des tiers. L'opérateur du site web, ce qui permet l'introduction de traceurs cachés. (...) Par exemple, un service de paiement inclure des cookies liés à une entreprise publicitaire, sans que l'utilisateur du site puisse réellement contrôler ces données spécifiques utilisées pour le traçage en ligne massif, l'industrie s'est historiquement appuyée sur les données de profils utilisateurs à partir des sites visités »* ⁽¹²²⁾. Elle estime que **les traceurs seraient présents** sur

Certains data brokers collectent également des informations dans le cadre des enchères pour les encarts publicitaires qui s'affichent sur l'écran d'un internaute. Selon la Cnil, parmi les données qui reçoivent des informations sur le profil de l'internaute, certains décident de les conserver pour les utiliser et identifier.

3. Un cadre réglementaire largement contourné en pratique

Interrogée par la commission d'enquête sur la prolifération de telles pratiques, la présidente du **pas conformes au cadre réglementaire de protection des données** : « *Sur le plan juridique, la réglementation, si elles ne sont pas illégales, sont strictement encadrées. En effet, le RGPD et la loi " informatique " doivent être informées de la collecte et des usages de leurs données, et donner leur consentement en matière publicitaires et de revente.* » ^([124]) Or, les conditions d'un consentement libre, éclairé, univoque ne sont pas remplies en l'espèce. Mme Bielova remarquait que même les opérateurs de site web qui accueillent les utilisateurs *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 des chaînes d'intermédiaires, qu'il est délicat de reconstituer. Les contrôles conduits par la Cnil en 2022 sur les pratiques des courtiers en données, ont mis en évidence deux obstacles principaux qui freinent la transparence ^([125]).

D'une part, « **la complexité technique des chaînes de collecte et de revente rend difficile la traçabilité des responsables** » ^([126]). Les entreprises ne sont en effet pas les destinataires finaux et uniques des données, mais une multitude d'intermédiaires. Reprenant une image de ses collègues allemands, M. Untersinger compare les chaînes de données mobiles à « *la lave à l'intérieur des lampes* » : « *elle bouge, se divise, se rapproche. Autrement dit, elle est fluide. Les données s'échangent, se revendent, sont modifiées, recoupées, etc. par des dizaines et des dizaines d'acteurs. Il n'est vraiment possible de suivre leur cheminement.* » ^([127])

D'autre part, les acteurs qui revendent les données sur les places marchandes « **sont pour la plupart aucun établissement en Europe, ne sont pas pérennes, ou changent souvent de nom** », ce qui empêche de les identifier ^([128]). M. Untersinger illustre ce dernier point avec le cas d'une start-up française qui, pour ne pas avoir respecté les bonnes pratiques de sa régie publicitaire : « *Cette start-up récupère des données et les revend, notamment dans des outils de surveillance proposés à des États. Une fois blacklistée par les autorités, elle en a immédiatement recréé une autre et si je n'ai pas d'informations à son sujet, il n'y a, à mon sens, aucune trace.* »

En bout de chaîne, ce sont néanmoins les grandes plateformes qui tirent parti de la collecte de données et constituent un point incontournable de la monétisation des contenus publicitaires. M. Robert, de l'agence Supramundane, a souligné la forte concentration du marché publicitaire, qui permet aux Big Tech de contrôler sur le fonctionnement des réseaux publicitaires, par lesquels transitent pourtant des centaines de millions de données.

4. Les données de géolocalisation

Compte tenu de leur rôle clé dans la réidentification des personnes, la rapporteure s'est particulièrement intéressée à **mieux encadrer la collecte des données de géolocalisation.**

Une autre enquête réalisée par *Le Monde*, consacrée aux *StravaLeaks* ^([130]), a confirmé les risques et les vulnérabilités que leur diffusion engendre. Sur cette application américaine qui permet de partager ses trajets, il est possible d'accéder en direct à la position de nombreux utilisateurs. Cela a permis aux journalistes, à la police, aux gardes du corps de chefs d'État, et donc d'identifier, non seulement leur domicile, mais aussi des lieux sensibles comme les portes-avions *Charles de Gaulle*, ou les hôtels où devait séjourner le président de la République, avec une précision remarquable.

M. Sébastien Bourdon, journaliste indépendant, revient également sur de précédents travaux de la commission : « *plupart des Maliens n'utilisant pas Tinder, les seuls profils que nous voyions apparaître étaient ceux des touristes. L'application indique si la personne se situe à 1, 2, 3 ou 4 kilomètres, sachant qu'avec une précision de 100 mètres, obtenir une localisation très précise, à quelques mètres près ; ce n'est pas très compliqué à faire.* »

niveau européen. Il doit toutefois être décliné dans différents contextes. Dans le secteur des applications, il faut 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 en ligne, le 18 juillet 2024 des recommandations relatives aux applications mobiles ⁽¹³³⁾. L'ensemble de ces recommandations vise à établir un cadre permettant d'avoir accès de manière plus sécurisée à de multiples applications mobiles.

D. UNE APPLICATION INÉGALE DU RGPD

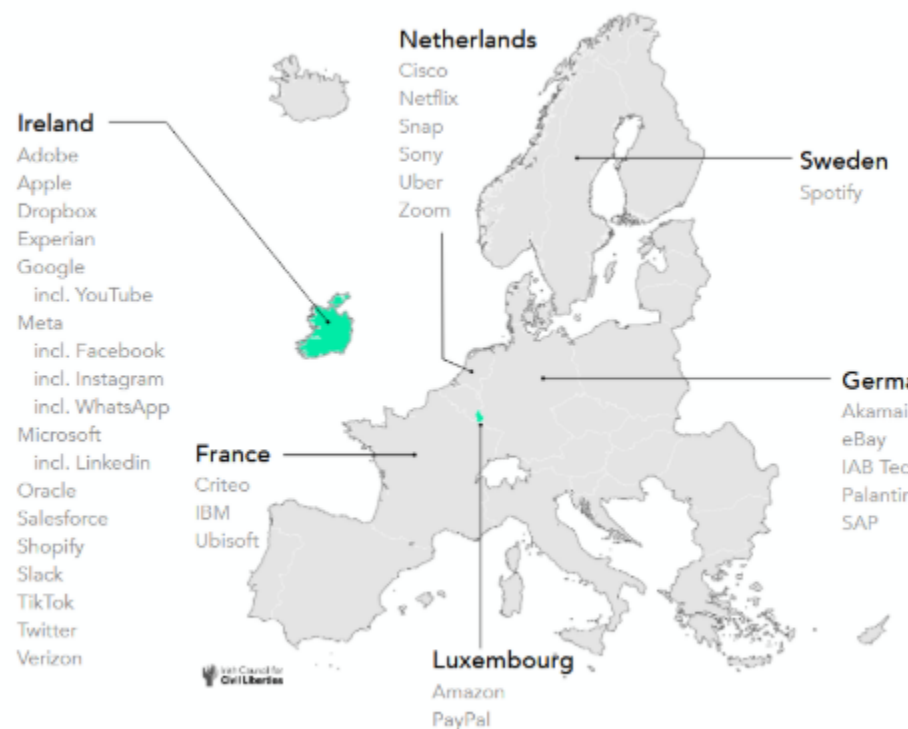
Lors de son audition, M. Max Schrems a raconté : « Un jour, le responsable d'une autorité de protection des données m'a appelé à l'issue d'une conférence pour me dire combien ce serait drôle si les mesures que j'avais exposées étaient appliquées. Il s'agissait précisément des lois qu'il était chargé de faire appliquer, c'est ahurissant ! C'est comme si un policier déclarait : " Ce serait drôle de faire quelque chose pour empêcher le trafic de cocaïne, non ? " Il faut vraiment que nous devons composer sur le terrain. Il est vrai que les chiffres disponibles à l'échelle européenne montrent que les amendes 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 4 du RGPD prévoit un **guichet unique pour les traitements de données transfrontaliers**, c'est-à-dire les traitements mis en œuvre par une entreprise dans plusieurs États européens ou qui affectent sensiblement des personnes d'au moins un autre État européen. Cette règle est chargée par l'autorité cheffe de file, qui est l'autorité de protection des données du pays où se trouve l'entreprise.

Cette règle a pour effet de **diriger une part importante des plaintes émises contre les géants du numérique européens qui en concentrent les sièges, en raison de leur cadre fiscal favorable : l'Irlande, les Pays-Bas, la France, le Royaume-Uni, le Luxembourg**. Le Cnil a ainsi transmis plus de 260 plaintes transfrontalières à un homologue, dont 51 % à la seule autorité irlandaise (Data Protection Commission – DPC).

AUTORITÉS CHEFFES DE FILE DES PRINCIPALES ENTREPRISES TECHNOLOGIQUES



	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, citoyen lambda n'a aucune chance de faire valoir ses droits* » ⁽¹³⁸⁾. L'importance des frais à engager d'exercer leurs droits : « *si, en tant que citoyen français, votre cas est transféré en Irlande, vous avez le régulateur irlandais pour son inaction, mais votre démarche n'a en réalité aucune chance de succès. 100 000 euros sur votre compte en banque. À l'issue de l'affaire Schrems II – j'étais alors poursuivi – des amendes de 100 000 euros ont été établies à environ 10 millions d'euros. Si j'avais perdu, j'en aurais été personnellement redevable. C'est un tel risque.* »

Le fonctionnement interne de l'autorité de protection des données irlandaise serait éga et ONG auditionnées. M. Bastien Le Querrec, juriste membre de la Quadrature du Net, a déclaré : « *notoirement incapable de faire face aux Big Tech* », « *marquée par des phénomènes de pantoufle* », « *traitement des plaintes et les investigations* » ⁽¹³⁹⁾. Dans le même sens, M. Max Schrems a évoqué M. Sweeney comme commissaire de la DPC, qui avait travaillé pendant six ans comme lobbyiste pour M.

Comme mentionné dans la première partie de ce rapport, les revenus liés à l'activité d'immatriculation des filiales des géants américains, représentent près de 35 % du PIB irlandais. **Le rapport de la Commission européenne concernant des acteurs majeurs de son activité économique relève, pour la rapporteure, d'un échec à perdurer.**

La rapporteure appelle ainsi les autorités françaises à défendre la suppression de la règle de 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 régulation des Big Tech qui y ont leur siège, le CEPD ayant démontré, à l'occasion de l'adoption de ses décisions coordonnées, que son organisation collégiale, associant l'ensemble des autorités européennes compétentes, facilitera l'adhésion des entreprises.

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

2. Des sanctions insuffisamment dissuasives ?

Le RGPD a renforcé le pouvoir de sanction des autorités de protection des données personnelles. **Les amendes prononcées atteignent cependant rarement ces plafonds, ce qui peut conduire à une perte de 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 l'amende, parmi lesquels : la nature, la gravité et la durée de la violation ; le fait que la violation soit intentionnelle ou négligence ; les catégories de données à caractère personnel concernées par la violation ; ou toute autre circonstance.

décision de la Commission nationale pour la protection des données luxembourgeoise, qui avait versé 743 millions d'euros contre Amazon. Comme l'a détaillé M. Thomas Dautieu, directeur de l'accomplissement, *la loi a validé les manquements relevés par l'autorité luxembourgeoise, mais elle a annulé la décision de l'autorité luxembourgeoise justifiée par les manquements. L'autorité de protection des données luxembourgeoise doit donc reprendre sa décision initial en fonction des manquements.* » ^([144])

Les législateurs nationaux et européens doivent clairement affirmer le souhait d'uti-
liser les règles réglementaires existants, notamment par l'application de sanctions véritablement dissuasives.

– 1 –

CHAPITRE 5 – ESPIONNAGE ET PRESSIONS SUR LES PERSONNALITÉS POLITIQUES : LES 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. Verdier estime « systématique ». « *Dans le cas des États-Unis, cette pratique s'appuie sur un cadre juridique américain à accéder aux données sous juridiction américaine. Quant à la Chine, l'espionnage y est très répandu. Cette dépendance nous expose à des risques majeurs en cas de conflit et nous rend vulnérables à la perte de l'information* » ^([145]), souligne-t-il.

1. Des produits extra-européens soumis aux législations extraterritoriales

Des législations américaines à portée extraterritoriale obligent de fait les fournisseurs de services numériques 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. S'il visait à l'origine la recherche d'informations ciblées sur des acteurs étatiques étrangers, il a été étendu par l'article 702 qui autorise le gouvernement américain à surveiller les communications électroniques de personnes non américaines, 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 ont demandé, pendant une période maximale d'un an, le ciblage de personnes étrangères soupçonnées de se trouver hors des États-Unis. Cet amendement de la Constitution, qui requiert un mandat pour toute perquisition contre des citoyens américains, a été rejeté. La Cour de surveillance du renseignement étranger (Foreign Intelligence Surveillance Court) a statué l'année suivante, en 2015, que l'article 702 était inconstitutionnel. La Cour a statué l'année suivante, en 2016, que la collecte de données sur des personnes non américaines était inconstitutionnelle. Les flux de données des *US persons* bénéficient d'une protection plus forte que celle prévue en Europe et leur surveillance est jugée inconstitutionnelle. Pour l'avenir, la Cour a statué que *le gouvernement peut faire ce qu'il veut* » a fait observer Max Schrems lors de son audition ^([146]).

Dans son bilan annuel de 2025, la Cour de surveillance du renseignement étranger a déclaré que 91 des 100 mandats accordés, 91 ont été modifiés, 15 ont été partiellement rejetés, et 4 pleinement rejetés ^([147]).

Adopté en 2018, le **Cloud Act** permet aux autorités américaines, disposant d'un mandat ou d'un ordre de production de données hébergées, même à l'étranger, par des entreprises soumises au droit américain dans le cadre d'une enquête, ainsi à accélérer le temps de l'investigation, en obtenant la divulgation des données plus rapidement.

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. Ils ont tous donné des réponses qui ne correspondaient pas aux requêtes émises par les autorités américaines.

Mme Corine de Bilbao, présidente de Microsoft France, a assuré que les services juridiques de Microsoft respectaient la légalité de la demande qui leur était transmise, et notamment si elle n'était pas « *imprécise, excessive ou disproportionnée* ». Microsoft affirme s'être par ailleurs, « *engagé contractuellement à contester systématiquement les demandes qui elles relèvent du Cloud Act ou du Fisa* ». S'agissant d'AWS, M. Arnaud David, directeur des affaires publiques de AWS France, essayait de rediriger les demandes vers ses clients : « *Nous considérons en effet que nous n'avons pas la mesure où nous n'avons pas d'accès aux données. Les clients sont plus à même de le faire – prenons l'exemple de Facebook, réseaux sociaux, qui a une relation directe avec ses utilisateurs finaux* » ⁽¹⁴⁹⁾.

Ces procédures internes et recours juridiques ne permettent cependant que de retarder la réponse à la question de la rapporteure « *si un juge, après contestation, valide la demande d'accès du gouvernement à des données publiques ou privées, avez-vous l'obligation légale de les transmettre ?* », les auditionnés ont refusé de répondre clairement, à l'exception de M. Frédéric Geraud de Lescazes, directeur des affaires publiques de Google France, qui a déclaré : « *Google respecte l'État de droit : si un juge allemand, canadien, chilien, américain ou français nous demande de transmettre des données soumises au droit américain, les hyperscalers ont de fait l'obligation juridique de transférer les données aux autorités fédérales* ».

Cela confirme les propos tenus par un représentant de Microsoft devant la commission d'enquête publique qui l'interrogeait sur sa capacité à garantir que les données des citoyens français hébergées par Microsoft ne sont transmises à des autorités étrangères sans l'accord des autorités françaises. M. Anton Carniaux, directeur des affaires publiques de Microsoft France, avait reconnu sous serment : « *Non, je ne peux pas le garantir* » ⁽¹⁵⁰⁾. Il avait été licencié que par Microsoft « *absolument aucun lien* » avec son audition selon la présidente de Microsoft France ⁽¹⁵¹⁾.

Mme de Bilbao affirme que « *Microsoft n'a jamais divulgué de données d'un client des États-Unis à des autorités étrangères, y compris américaines* ». Elle a cependant dû reconnaître avoir transmis les données à un gouvernement américain : « *Pour les entreprises privées, nous avons un cas dans les trois dernières années* ». M. Arnaud David a déclaré qu'« *aucune demande adressée à AWS n'a été suivie d'une transmission 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 des données réalisées par ces entreprises.

Les rapports de transparence publiés par Microsoft ⁽¹⁵²⁾, Google ⁽¹⁵³⁾ et Amazon ⁽¹⁵⁴⁾ témoignent de la réponse aux demandes d'informations sur leurs utilisateurs, provenant de l'ensemble des autorités gouvernementales et des enquêtes criminelles. La localisation géographique des personnes morales ou physiques ciblées n'est pas connue. Au 30 septembre 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. La transmission d'informations – du contenu pour 16 % et des métadonnées pour 59 %. 115 données de contenu stockées en dehors des États-Unis – le nombre de requêtes concernant des données de contenu stockées en dehors des États-Unis ;
- Google indique avoir reçu en moyenne 287 000 demandes d'informations, dont 60 000 émanant des États-Unis. De ces dernières ont donné lieu à des divulgations.

S'agissant spécifiquement de la transmission d'informations relatives à des personnes ciblées, les données contiennent des éléments qui contredisent les déclarations d'intention des hyperscalers. Si le rapport de transparence de Microsoft indique que les données relatives à des personnes ciblées ne sont pas transmises à des autorités étrangères, y compris américaines, les données de transparence de Google et d'Amazon indiquent que des données relatives à des personnes ciblées ont été transmises à des autorités étrangères, y compris américaines.

nombre de ces demandes dans certaines fourchettes autorisées par la loi. (...) La fourchette de détermination des données est la suivante : toutes les demandes relatives à la sécurité nationale adressées à Amazon (y compris AWS) » ;

– Google indique pour sa part avoir reçu en vertu de la loi Fisa, au niveau mondial, entre 177 500 et 177 900 messages (messages, photos, vidéos), concernant de 75 500 à 75 999 comptes, et entre 0 et 499 demandes de divulgation de contenus ;

– Microsoft fait état de 0 à 499 demandes de divulgation de contenus sur la base du Fisa, concernant de 75 500 à 75 999 comptes ;

b. Des barrières techniques à l'efficacité non démontrée

Les *hyperscalers* auditionnés ont tous revendiqué la mise en place de solutions techniques pour empêcher l'accès non autorisé à leurs données 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 : « *On ne peut pas accéder légalement qu'à partir du moment où on peut techniquement y avoir accès. Or nous utilisons un certain nombre de techniques pour empêcher l'accès aux données des clients* ». La représentante de Microsoft a défendu la même position : « *On ne peut pas fournir les données lorsque les clés de chiffrement ont été utilisées et que celles-ci sont dans le coffre-fort du fournisseur de cloud computing, ou lorsqu'elles sont hébergées dans un cloud sécurisé, certifié SecNumCloud* » ^([156]).

La première garantie de confidentialité consisterait dans le chiffrement systématique des données. M. Vincent Strubel, directeur général de l'Anssi, a néanmoins souligné que « *l'argument souvent avancé est que le chiffrement des données est insuffisant car même si les données sont chiffrées, leur traitement implique que la clé de déchiffrement est connue des acteurs des données, ce qui permet au prestataire d'y accéder* » ^([157]).

Le *confidential computing*, ou informatique confidentielle, vise à remédier à cette limite en créant des boîtes étanches, qui fonctionnent indépendamment du système d'exploitation hôte et auxquels même les administrateurs n'ont pas accès. Les données entrent et sortent chiffrées, et l'application ne s'exécute qu'à l'intérieur de l'espace sécurisé. Les données et leur traitement à l'encontre des fournisseurs de cloud.

Microsoft a mis au point sa technologie de calcul confidentiel en 2014, avant de la rendre disponible en 2017. M. Philippe Limantour a expliqué que « *les clés de chiffrement font l'objet d'une hiérarchie. Au sommet, c'est le fournisseur de cloud qui gère sa propre clé, dont il est le seul détenteur – s'il perd sa clé, il perd ses données. Les clés de chiffrement sont gérées d'un mécanisme de calcul confidentiel, provenant de l'un de nos trois fournisseurs ; ces mécanismes empêchent techniquement d'accéder à la clé.* » ^([158])

Google Cloud a également mis en place un système de chiffrement reposant sur une gestion centralisée des clés, appelé EKM (*external key management*). Les entreprises clientes peuvent ainsi choisir de déposer leurs données, notamment Thalès.

Enfin, AWS a développé la solution AWS Nitro, intégrée directement à ses serveurs. Nitro permet de créer des machines virtuelles avec des processeurs et une mémoire isolée des instances du système. Invité à préciser son positionnement, AWS a affirmé : « *Par défaut, Nitro permet à tous nos clients, quand ils lancent gratuitement des infrastructures, d'avoir accès à leurs données, qu'elles soient en traitement, en transit ou en repos ; celles-ci sont soit chiffrées, soit chiffrées par défaut d'accès pour les opérateurs.* » Les clés de chiffrement sont gérées par les services d'AWS ou par des services tiers comme Devoteam ou Thales ^([159]).

Ces solutions ne seraient cependant pas encore matures sur le plan technologique. Le directeur de l'Anssi a déclaré : « *les technologies de confidential computing (...) ne sont aujourd'hui ni suffisamment fiables ni suffisamment matures pour se dispenser de la confiance accordée au prestataire* » ^([160]).

Il n'est par ailleurs pas certain que l'argument d'une impossibilité technique suffise à supprimer l'accès aux données des clients.

M. Vincent Strubel précise néanmoins que « *le SecNumCloud ne garantit pas la protection 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 imposerait une coupure des services numériques fournis à l'Union européenne, qu'elle affecte des personnes physiques ou des personnes morales. Une telle menace constitue un levier de pression considérable à l'encontre des pays et des entreprises.

Cette menace s'est matérialisée avec le blocage des modèles d'intelligence artificielle. Le 12 juillet, l'entreprise a annoncé suspendre l'accès à ces deux modèles d'IA suite aux ordres des autorités américaines. L'entreprise est ressortissant étranger, à l'intérieur ou à l'extérieur des États-Unis, y compris à ses propres « employés ».

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 en Afghanistan et du gouvernement israélien dans la bande de Gaza, **le président des États-Unis a imposé des sanctions à la CPI.** Il est notamment prévu d'imposer aux personnes visées : l'interdiction de se rendre en France et leur famille proche ; le gel de leurs avoirs détenus aux États-Unis ; et **l'interdiction pour les entreprises américaines, y compris leurs filiales et leurs employés, de leur fournir des biens et services.** Aucune entreprise ne peut contester la décision. Ces mesures sont mises en œuvre par l'Office of Foreign Assets Control (OFAC), qui tient une liste recensant les personnes physiques et morales sous sanctions économiques – essentiellement des personnes coupables de graves violations des droits de l'homme.

Comme l'indique le juge M. Nicolas Guillou, juge à la CPI ⁽¹⁶⁵⁾ : « *Une des principales difficultés a été d'élaborer en commun par l'Europe et les États-Unis pour lutter contre le terrorisme. On ne s'est pas mis d'accord au début : les sanctions ont été conçues comme émanant d'une décision de l'exécutif, quasiment sans consultation de l'Union européenne a imposé un contrôle du juge en 2008, par l'arrêt Kadi, mais c'est à peu près le seul système visant ceux qui violent le droit international pourrait être retourné contre ceux qui sont censés respecter le droit.* »

Le décret ne visait à l'origine que le procureur de la CPI, Karim Khan, mais le secrétaire d'État a étendu le champ des sanctions à dix autres magistrats de la CPI. Le décret du 20 août 2025 cible notamment le Premier ministre pour avoir autorisé l'émission de mandats d'arrêt internationaux à l'encontre du Premier ministre israélien, l'ancien ministre de la défense israélien Yoav Gallant.

Le juge Guillou a témoigné devant la commission d'enquête de l'ampleur des conséquences sur la vie quotidienne en Europe, particulièrement fortes dans deux domaines : les services numériques et la prépondérance des acteurs américains. « *Ma vie personnelle est devenue un laboratoire de la perturbation de la vie quotidienne qui m'arrive me fait réaliser l'ampleur de notre dépendance au quotidien : tout ce qui ne fonctionne plus est la dépendance.* »

a. Une suspension automatique des services numériques américains

Dans un contexte de quasi-monopole des plateformes américaines, **le juge Guillou a expliqué comment il s'est trouvé privé de nombreux services numériques :** ses réservations d'hôtel sur les plateformes américaines n'a pas pu réserver une place de concert à l'Olympia car le seul site de vente était américain et a été bloqué ; il n'a pu accéder aux grandes plateformes de musique ou de cinéma... Lors d'une conférence de presse, le juge Guillou a déclaré : « *comme dans les années 1990* » ⁽¹⁶⁶⁾. L'autre juge européenne de la CPI sanctionnée, Mme Beti Halilaj, a déclaré au Parlement européen, déclarant que ses comptes Apple, iCloud, Amazon, et Paypal avaient tous été bloqués sans préavis préalable ⁽¹⁶⁷⁾.

banque ne m'a proposé un compte avec une carte CB. (...) J'ai essayé de me rapprocher indirectement de la banque, mais elle ne souhaite avoir des clients sous sanctions ». ([169])

Le juge Guillou n'a pas pu obtenir de carte bancaire qui fonctionnerait uniquement sur le réseau des cartes de paiement émises par les banques 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 droit français, le Trésor a indiqué à la rapporteure que, **bien que certains établissements français aient pu historiquement émettre des cartes de paiement jusqu'au début des années 2010, cette pratique semble avoir disparu** ([171]).

Par ailleurs, les établissements bancaires qui lui délivreraient une telle carte pourraient s'exposer à raison de « *la tenue du compte, sur laquelle pèse également un risque de sanction.* », selon M. Eric

Il est à noter que le juge Guillou n'a pas subi de fermeture de compte jusqu'ici, mais que la situation de la banque et de la situation et examine les solutions dérogatoires qui pourraient être mises en place s'il était rapporteure spéciale des Nations Unies sur les territoires occupés, Francesca Albanese, ont vu leur rôle en Italie ([173]).

L'obstacle principal à la délivrance d'une carte bancaire serait ainsi l'application extraterritoriale de la suprématie du dollar. Si *l'executive order* 14203 ne s'applique qu'aux *US Persons* – c'est-à-dire aux citoyens américains permanents étrangers, et aux sociétés américaines, ainsi qu'à leurs filiales et employés à l'étranger – elle s'applique également aux entreprises non américaines pour des opérations qui n'ont pas lieu sur le territoire américain, par exemple le rattachement : l'utilisation du dollar ; le transit par des serveurs du système financier américain ; ou la question de l'extraterritorialité (...) est liée au dollar, par lequel les États-Unis peuvent atteindre tous les pays. Or, il est quasi impossible pour une entité financière en Europe de ne jamais effectuer de transactions en dollars. 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 effectué des paiements en dollars en violation des embargos imposés par les États-Unis à l'encontre de Cuba, de l'Iran ou du Soudan – 8,9 milliards de dollars pour la Société générale en 2018. La compétence américaine se fondait sur le fait que les transactions étaient effectuées en dollars et se traduisaient par une opération-reflet dans les chambres de compensation.

Ces précédents ne sont cependant pas transposables au cas du juge Guillou, dans la mesure où les transactions destinées seraient réalisées en euros. La situation est différente pour les ressortissants d'autres régimes de paiement du dollar, notamment en Amérique latine, où la magistrate Luz del Carmen Ibáñez Carranza, égale à la juge Guillou, a déclaré que « *principales transactions commerciales s'effectuent en dollars* ». Au contraire, « *les transactions commerciales s'effectuent dans l'espace unique de paiement en euros (SEPA) un réseau de paiement européen qui permet d'effectuer des transactions dans les pays participants sans recourir au dollar américain ni passer par le système américain* » ([175]). **Les banques européennes devraient se conformer aux sanctions américaines, même pour des transactions effectuées dans l'espace unique de paiement en euros, en raison de la conception très extensive de l'extraterritorialité, qui n'a jamais été confirmée par une jurisprudence internationale.**

L'impuissance affichée par la Fédération bancaire française pourrait dès lors s'assimiler aux mesures de **surconformité, adoptées par certaines entreprises européennes**, par crainte des conséquences néfastes de la mise en œuvre des sanctions des États-Unis. La Coalition pour la CPI a mis en évidence, dans son rapport du 23 avril 2026, cette mise en œuvre des sanctions « *des banques et des institutions financières non américaines à appliquer ces mesures extraterritoriales, qui comportent aucun lien ni aucune forme de connexion avec les États-Unis ou le dollar* » ([177]).

Tout en exprimant la solidarité du secteur bancaire à l'égard du juge Guillou, Mme M. a concédé une forme d'attentisme : « nous n'avons pas de solution à apporter ». Elle a déclaré que la Fédération bancaire française (FBF), qui investit pourtant très régulièrement le champ du lobbying aux niveaux national et européen, sous la présidence de Philippe Latombe, n'avait « *pas formulé de propositions de négociation internationale sur la question des sanctions* », quand bien même leurs clients particuliers et professionnels sont directement concernés.

Malgré les appels en ce sens, **la Commission européenne n'a jusqu'ici pas activé le règlement de blocage** ^{(180)]}. Celui-ci permet de contrecarrer les effets extraterritoriaux des législations américaines sur le règlement, lorsqu'ils portent atteinte aux intérêts des entreprises et des citoyens européens. Il prévoit

- priver d'effet sur le territoire de l'Union européenne les législations ou décisions qui prévoient des sanctions
- interdire aux opérateurs européens de se conformer aux prescriptions ou interdictions américaines, sous réserve d'une dérogation accordée par la Commission européenne si le non-respect de ces prescriptions lèse gravement les intérêts des États membres
- obliger toute personne dont les intérêts économiques ou financiers sont affectés directement par les législations à en informer la Commission sous trente jours ;
- ouvrir le droit aux opérateurs européens d'être indemnisés de tout dommage causé par des législations 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 vertu de l'insérer dans l'article 459 du code des douanes, qui prévoit des sanctions pénales à l'encontre de 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. Selon le deuxième alinéa, du règlement, elle doit pour ce faire modifier l'annexe en adoptant un acte délégué. Toutefois, la Commission a la capacité de s'opposer à son entrée en vigueur, respectivement à la majorité absolue et à la majorité qualifiée, six mois à compter de la notification de l'acte par la Commission. La Commission a mis en œuvre cette faculté pour le règlement afin d'étendre son application aux sanctions extraterritoriales rétablies par les États-Unis.

La Commission s'est cependant refusée jusqu'à présent à ajouter les sanctions américaines au règlement de blocage, faute de consensus entre les États membres. La porte-parole de la Commission, Mme Siobhan McGarry a ainsi déclaré que « *la voie diplomatique et la recherche de solutions constructives sont probablement à ce niveau que ma déception a été la plus forte*, a déclaré le juge Guillou. Selon lui, « *la souveraineté européenne, autant le Parlement européen souhaite vraiment avancer, autant il n'y a pas de risques au sein de la Commission européenne, pour l'instant.* » ^{(183)]}

Si la France, la Belgique et la Slovaquie sont favorables à l'activation du règlement, d'autres États membres n'entraînent des mesures de rétorsion américaines, notamment de nouvelles hausses de droits de douane. **groupes ou de commissaires européens ont peur de déclencher l'application du règlement, car ils craignent** selon M. Guillou.

Les opposants à l'application du règlement de blocage mettent également en avant sa faiblesse juridique et parlementaire ^{(184)]}. Les entreprises européennes se trouveraient confrontées à un **conflit de normes** européen, qui les exposerait à une double peine. Les diplomates de la Représentation permanente de l'Union européenne, rencontrées par la rapporteure et le président lors de leur déplacement à Bruxelles, confirment que le **blocage constituerait un « écran protecteur », dont pourraient se prévaloir les opérateurs américains.** Il clarifierait en outre le fait que les fournisseurs de services européens ne doivent pas être sanctionnés visant la CPI.

Le juge Guillou a indiqué à la commission ^{(185)]} : « *Nous sommes dans un moment de transition, nous ne croient-ils vraiment ou non au droit international ?* »

La rapporteure appelle la Commission européenne à activer le règlement de blocage, pour protéger la défense du mandat de la Cour pénale internationale, de l'indépendance de la justice, et de la souveraineté des États membres.

d. Le risque d'une systématisation des sanctions ciblées

fonctionne dans notre économie. Oui, il faut protéger la donnée, mais il faut également se protéger.

Le *kill switch* se matérialiserait par la suspension des ventes de logiciels américains à des services de support, de maintenance et de développement associés. L'accès aux applications et logiciels américains serait coupé, de même que l'ensemble des services numériques fournis par les grandes entreprises américaines. ***aujourd'hui d'une solution face à une coupure généralisée d'accès aux technologies américaines, demain privée de mises à jour, la situation deviendrait rapidement intenable*** », a alerté M. Vincent Strubel, président de l'Anssi ⁽¹⁸⁷⁾.

Une telle coupure serait susceptible de paralyser l'ensemble de l'économie européenne, **particulièrement critiques dans les pays européens les plus dépendants aux technologies américaines**. Lors de la panne informatique mondiale provoquée, le 19 juillet 2024, par la mise à jour défectueuse du logiciel CrowdStrike, a permis de mesurer la profondeur des vulnérabilités liées à une forte dépendance : « Des entreprises ont été trouvées clouées au sol, des hôpitaux ont été contraints d'annuler des opérations, quand des banques d'appel d'urgence ne pouvaient plus fonctionner. M. Vincent Strubel a néanmoins fait observer que la situation n'est pas **touchée, en partie grâce à une moindre dépendance à cette monoculture** » en matière de logiciels de sécurité.

L'hypothèse est envisagée sérieusement par le gouvernement, le ministre de l'action et des services a déclaré devant la commission d'enquête qu'« *il fa[llait] parer les risques de kill switch, à savoir une coupure qui rendrait notre pays vulnérable* » ⁽¹⁸⁸⁾.

Cette prise de conscience progresse également parmi d'autres États européens. M. Max Moser, ministre de l'Intérieur au Danemark s'agissant de la menace pesant sur le Groenland : « *L'armée danoise s'inquiète qu'en cas de coupure, elle ne les privent de l'accès aux services numériques de Microsoft, AWS ou Google, par exemple. L'armée ne s'applique pas d'appliquer de tels embargos – ils le font actuellement à Cuba, en Syrie ou en Iran. Je suis un mondialiste, mais je ne se produira pas. Toutefois, au vu de ce qui s'est passé au cours de la dernière année, la question des conséquences qu'aurait un tel embargo – les hôpitaux, qui utilisent Microsoft, ne pourraient pas fonctionner, par exemple.* » ⁽¹⁸⁹⁾

Un tel scénario ne serait certes pas dans l'intérêt des grandes entreprises numériques américaines, mais pourrait représenter approximativement un tiers du chiffre d'affaires. La présidente de Microsoft a tenté d'entreprendre de rassurer en déclarant que « *la probabilité d'un kill switch est extrêmement faible, voire nulle* ». Microsoft, entreprise globale, qui opère dans 180 pays et s'est engagée à augmenter de 40 % ses centres de données en Europe, ne peut pas nos investissements, il serait suicidaire d'appliquer un kill switch. L'entreprise n'est pas le gouvernement. Il est difficile de déterminer de quelle marge de manœuvre disposeraient ces entreprises, établies au sein de l'Union européenne, des injonctions de l'administration fédérale auxquelles même les grands établissements bancaires européens sont soumis.

b. Une vulnérabilité liée à l'interruption des mises à jour

Comme en matière de protection des données, **aucune des mesures techniques et organisationnelles des hyperscalers pour garantir leur capacité à maintenir leurs services dans la durée, ne semble éliminer le risque**.

Amazon a lancé, en janvier 2026, un cloud souverain européen, « *physiquement et opérationnellement autonome d'AWS* », qui reposerait sur des data centers situés en Europe et serait opéré exclusivement par des employés européens. Le contrôle opérationnel ne s'exerce depuis l'extérieur des frontières européennes ». Selon M. Julien Bouchard, directeur général de l'ANSSI : « *ce nouveau cloud d'AWS bénéficie d'une autonomie de fonctionnement, même si l'Europe devait être isolée* ». Les mesures organisationnelles ne permettront cependant pas de contrecarrer l'obligation d'appliquer les injonctions de la structure capitaliste de la société. Les injonctions des autorités fédérales s'imposent de fait à toutes les entreprises, y compris leurs filiales et leurs employés à l'étranger.

Les hyperscalers ont également mentionné les **engagements contractuels pris envers les clients** et le **coût brutal des services**. Pour son cloud souverain, AWS a pris « *l'engagement ferme que, si nous devions*

moyenne sur les cinq dernières années pour atteindre 50 000 vulnérabilités rendues publiques et exploitées dès le jour de leur publication » ^([195]). Toute la question est donc de savoir combien de temps il faut attendre pour avoir aucun accès aux mises à jour. Selon M. Philippe Limantour, « *les délais avant que les risques deviennent exploitables en semestres* ». Il existerait des « *mécanismes de défense en profondeur permettant de bloquer l'exploitation ou vingt petits pas, pour bloquer les attaques. Ainsi ce n'est pas parce qu'on trouve une faille exploitable* » ^([196]). Le représentant de Google Cloud témoignait cependant de l'existence de failles qui impliquent un risque immédiat pour la qualité du service et la sécurité des infrastructures.

Au regard de l'ampleur des vulnérabilités et de l'accélération de leur exploitation qui inquiète la rapporteure se questionne sur la capacité des opérateurs cloud reposant sur des technologies américaines à résister durant une période d'un semestre.

Le scénario d'un kill switch, dont la crédibilité a fortement gagné en ampleur au cours de la dernière année, la politique suivie par le gouvernement des Etats-Unis, aurait des répercussions techniques, économiques et sociales. 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 d'un choc 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.

– 1 –

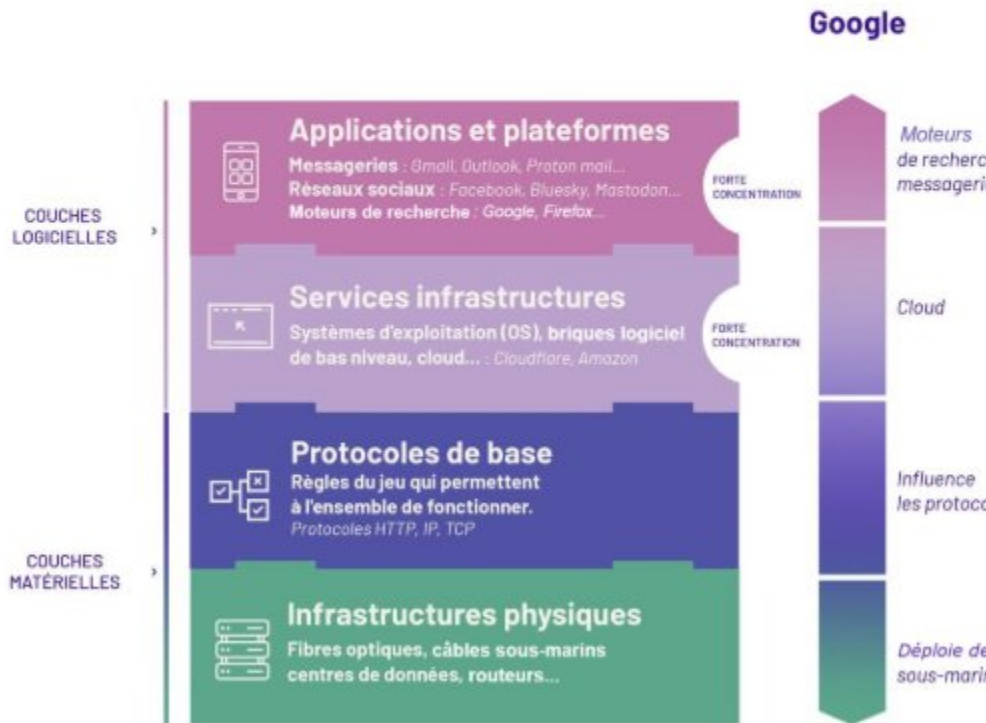
TROISIÈME PARTIE : LES CAUSES D'UN ENRACINEMENT PROFOND

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 de distribution, le socle des systèmes d'information des entreprises ou des administrations. Leur activité laisse peu de place aux entreprises européennes, 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 monopoles, leurs conditions et de constituer des rentes à leur profit. Partant du constat de l'ultra-dominance des Big Tech, comment expliquer que le droit de la concurrence n'ait pu avoir un impact sur leur activité ? Quel est le rôle de la puissance publique ?

La rapporteure a souhaité établir une rétrospective des actions envers les Gafam conduites au niveau national et européen, afin de mesurer les résultats auxquelles elles sont parvenues et de comprendre les obstacles auxquelles elles se heurtent. L'adoption du DMA est présentée par la Commission européenne comme



Source : rapporteure.

Cette concentration tout à la fois horizontale (au sein des différentes couches) et verticale, les positions ultradominantes des Gafam et produit plusieurs effets :

- les effets de réseau, qui favorisent l'acteur qui dispose du plus grand nombre d'utilisateurs
- les effets de verrouillage des clients, perçus ou réels, à travers de nombreux dispositifs système, des difficultés à récupérer ses données, absence d'interopérabilité, etc. ;
- les économies d'échelle, permettant de réaliser des revenus très importants sur un grand nombre d'individus ;
- l'accès à des données d'utilisateurs à grande échelle, contribuant à l'avance technologique
- la vente forcée de produits à travers des offres groupées (« *bundling* ») et la capacité à mettre en place des services distincts ;
- la mise en place de barrières à l'entrée pour les concurrents via la standardisation et le contrôle

En asseyant leurs modèles économiques sur ces spécificités, les grands acteurs du numérique ont pu, au fil du 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 de manière progressive des différentes couches du monde numérique, comme le décrit Mme Ophélie Coelho ⁽¹⁹⁾ : « Elles prennent possession et privatisent des nœuds importants sur presque toutes les couches technologiques. Elles sont progressivement étendus aux supports de mobilité (ordinateurs, mobiles), aux câbles sous-marins, aux couches réseau avec des réseaux privés qui se superposent aux réseaux existants, et aujourd'hui, elles prennent une prise de contrôle de passerelles techniques essentielles. Le leader en la matière reste Google qui occupe des positions fortes dans tous les domaines que j'ai cités. »

(...).

« Au-delà du nombre de câbles, il faut considérer l'évolution de leurs capacités. En 2021, appartenait aux géants du numérique. (...) je pense que d'ici dix ans, ils pourraient détenir la puissance. C'est un changement énorme (...).

« Ce mécanisme de dépendance, fondé sur une intégration verticale, influe sur l'ensemble frappant est la coupure de câbles survenue en Afrique de l'Ouest en 2024. Quatre câbles historiques africains d'internet. Ce sont les câbles Equiano, de Google, et 2Africa, le consortium incluant Meta, la majeure partie du trafic. Cet événement montre que c'est souvent dans les moments de crise qu'ils deviennent des partenaires indispensables, à l'instar de ce que l'on a pu observer avec Starlink, bien que ce dernier ne soit pas une puissance. »

L'exemple des câbles sous-marins n'est pas isolé, des constats similaires peuvent être dressés. De leur positionnement, les Gafam deviennent indispensables au fonctionnement même de nos économies. Les avantages considérables. Comment le droit de la concurrence a-t-il appréhendé le rôle de ces acteurs ? Comment endiguer la constitution de positions dominantes ?

B. LE DROIT DE LA CONCURRENCE FACE AUX GAFAM : DES SANCTIONS MULTIPLES ET 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 au fonctionnement de l'Union européenne (TFUE), qui sanctionnent respectivement les ententes et les abus de position dominante. 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, *« les sanctions nationales présentent une dimension nationale, par exemple en raison de réglementations spécifiques, l'application est nécessairement à cette échelle. Si une opération de concentration y crée une domination trop forte, la sanction est nationale. À l'inverse, si un marché dispose d'une dimension plus large, notamment européenne grâce à une réglementation harmonisée, la sanction est menée à ce niveau »*. Lorsque l'autorité nationale se saisit, elle se fonde également sur le droit de la concurrence de l'Union européenne.

Le réseau européen de la concurrence (REC) rassemble la Commission européenne et les autorités nationales de concurrence à des fins de coordination et de répartition des affaires entre niveau européen et niveau national.

Le droit de la concurrence a récemment été complété par le DMA (voir *infra*), dont l'application est assurée par la Commission européenne.

Du fait de leur centralité, les cinq grandes plateformes états-uniennes ont fait l'objet d'un nombre croissant de sanctions de concurrence, qui a abouti à de nombreuses sanctions :

- pour Google (groupe Alphabet) : douze sanctions, dont huit avec amendes, représentant un montant cumulé de 1,4 milliard 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 ;

Groupe	Autorité	Affaire	Date	Sanction (M€)	Impact
Amazon	Commission européenne	AT. 40153 Amazon e-book MFNs	Mai 2017		Amazon EU SARL : engagements rendus obligatoires (MFN) dans ses contrats de distribution d'e-books d'infraction ni amende.
Amazon	Commission européenne	AT.40462 + AT.40703 — Amazon Marketplace & Buy Box Décision	Décembre 2022		Amazon : engagements rendus obligatoires dans d'utiliser les données non publiques des vendeurs ti garantit un accès équitable et non discriminatoire Procédure close sans amende
Apple	Commission européenne	AT.39847 / Ebooks	Juillet 2013		Apple Inc. et quatre éditeurs (Hachette, HarperCollins) rendus obligatoires. Les parties mettent fin aux cl dans leurs contrats de distribution d'e-books. Procéd
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 I 1,1 Md€ pour Apple seule) pour restrictions de clie des Apple Premium Resellers (APR) et abus de dépo
Apple	Commission européenne	AT.40437 / Apple App Store Practices (Music Streaming)	Mars 2024	1840	Apple Inc. condamnée à 1,84 Md€ pour avoir im (notamment Spotify) des restrictions techniques empêchant d'orienter les utilisateurs vers des offres par 42 pour effet dissuasif.
Apple	Commission européenne	AT.40452. Apple Mobile Payments (NFC)	Juillet 2024		La Commission rend contraignants les engagements de ses appareils iOS à des fournisseurs de services 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 conda position dominante en déployant le dispositif App 7 de consentement au suivi publicitaire des tiers ne s 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 empê utilisateurs vers des offres ou canaux de distribu antisteering du DMA. Première décision de non-con
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 société Navx et de clarifier leur politique de conten prononcées en France dans le secteur de la publicité
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 rendu transparentes et prévisibles les règles AdWords app contrôles routiers, faisant suite aux mesures conserv (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 M plus favorable à Google Shopping au détriment des Confirmé par le Tribunal de l'UE le 10 nov. 2021 (T
Google	Commission européenne	AT. 40099 / Google Android	Juillet 2018	4 125	Google LLC et Alphabet Inc. condamnées à 4,34 M Android : installation obligatoire de Google S restrictions aux versions Android non certifiées. An 2022 (T-604/18).
Google	Commission européenne	AT 40411 / Google Search (AdSense)	Mars 2019	1490	Google LLC et Alphabet Inc. condamnées à 1,49 M d'exclusivité anticoncurrentielles dans les contrats les empêchant d'afficher des publicités search de co
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 Fra non objective, non transparente et discriminatoire 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 Fra rémunération des éditeurs et agences de presse au ti 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 Fra favorisé, via le serveur publicitaire DFP, leur propre des SSP concurrentes (1re décision mondiale sur les Procédure de transaction. Engagements sur l'interop
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 Fra respecté les injonctions de la décision 20-MC-01 Google enjointe de se conformer sous astreinte de 9
		Décision 22-D-12 relative à des			Google LLC, Google Ireland Limited et Google Fra

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 ces pratiques dans le cadre d'une enquête sectorielle. Constatant la prédominance de trois acteurs principaux, l'Autorité souhaitait examiner dans quelle mesure leur force de frappe financière et leurs écosystèmes de services pouvaient entraver le développement de la concurrence.

Cette enquête a débouché en juin 2023 sur la publication d'un avis décrivant l'ensemble des pratiques constatées. 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 avoir à payer les coûts de gestion des données. Mais les fournisseurs de services cloud se servent de cette pratique pour favoriser leur propre système. *« L'Autorité considère toutefois que les crédits cloud sous forme d'offres ciblées d'accès à des services cloud attirent une attention particulière. Les montants proposés parfois élevés, le vaste écosystème d'entreprises qu'ils touchent distinguent significativement des essais gratuits qui peuvent être traditionnellement observés dans d'autres secteurs »* quant à la capacité de tous les fournisseurs de services cloud à les proposer de manière rentable. Les montants pouvaient aller jusqu'à 200 000 dollars pour Google Cloud, 150 000 pour Microsoft Azure, et jusqu'à 100 000 pour Amazon. L'encadrement de cette pratique, notamment le plafonnement à un an de leur durée. Toutefois, les mesures n'ont pas été appliquées faute de publication du décret nécessaire. Le président et la rapporteure ont demandé des décrets dans les plus brefs délais.

S'agissant des *egress fees*, l'Autorité considérait qu'ils étaient déconnectés des coûts réels de sortie des données, important à la portabilité des données. Les entreprises facturaient de façon trop importante les frais de sortie, notamment fortement les entreprises souhaitant mettre en œuvre des architectures dites multi-cloud, c'est-à-dire utilisant plusieurs fournisseurs. Depuis, les principaux *hyperscalers* ont revu leurs politiques tarifaires pour anticiper les demandes d'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 la migration d'un cloud un système d'information d'une entreprise ou d'une administration sont longs et coûteux à réaliser et 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 utilisés pour l'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 open source ou des produits Microsoft ;

- des mises à jour unilatérales de certains services faisant office de standard technique, auxq

par le Data Act européen ».

En revanche, Google dénonce le maintien de pratiques de licence juridique déloyales, en parlant de *« La possibilité pour les fournisseurs de cloud de gagner de nouveaux clients (notamment les entreprises publiques) est compromise par les pratiques de licence restrictives des éditeurs de logiciels historiques qui visent à fidéliser les clients de logiciels sur site à leurs propres plateformes cloud, empêchant ainsi les fournisseurs de cloud de rivaliser efficacement. Cette situation a permis à Microsoft de tirer un profit substantiel de ses pratiques de licence restrictive et permis d'établir et de consolider sa position dominante sur le marché du cloud »*. Google relève l'examen par l'autorité britannique de la concurrence et des marchés sur le sujet : *« La CMA ⁽²⁰⁴⁾ se dit préoccupée que les licences logicielles de Microsoft nuisent à la concurrence dans le cloud et entraînent une augmentation des coûts de productivité, tout en aggravant potentiellement les problèmes de résilience. Compte tenu de l'évolution rapide de l'IA avancée dans les outils de base de Microsoft, la CMA reconnaît que les mesures correctives prises jusqu'à présent ne suffisent pas. (...) La décision d'inclure les logiciels d'entreprise de Microsoft dans cette enquête SMS est motivée par une préoccupation majeure soulevée par son enquête sur le marché du cloud, en examinant les pratiques de licence de Microsoft, mais aussi d'étudier d'autres préoccupations exprimées par les acteurs du marché concernant l'impact de la position dominante sur le marché des logiciels d'entreprise »*.

Amazon web services note que les obligations du Data Act imposant aux fournisseurs de cloud d'assurer la portabilité et d'éliminer les frais de transfert sortant de données, sont pleinement applicables. L'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse déclare qu'elle devance les obligations européennes en ayant supprimé, depuis mars 2024, les frais de transfert de données souhaitant quitter AWS à l'échelle mondiale. *« Selon Deloitte, plus de 70 % des clients européens d'informatique en nuage, et 85 % des dépenses informatiques mondiales demeurent sur site. De fait, AWS est compétitive avec ceux d'autres fournisseurs informatiques, notamment Microsoft Azure, Google Cloud et Oracle Cloud, ainsi qu'OVHcloud, IONOS et Scaleway, des opérateurs de télécommunications comme Deutsche Telekom, ou des fournisseurs émergents. » ⁽²⁰⁵⁾*

AWS indique également utiliser des normes ouvertes et soutenir les communautés open source comme PostgreSQL et Apache.

De manière générale, le secteur est décrit comme particulièrement concurrentiel, dans la mesure où il attire de *« nouveaux investissements à travers l'Europe - de Stackit (11 milliards d'euros en Allemagne), Google Cloud et Microsoft, la 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 risques potentiels pouvant surgir sur les marchés cloud si des comportements spécifiques se matérialisaient » ⁽²⁰⁶⁾*. Le marché du cloud est dynamique et concurrentiel, en France et à l'échelle mondiale. Microsoft fait état de nombreux concurrents. Sont ainsi mentionnées les questions soulevées par OVH et l'association Cloud Infrastructure Security Partners (CISPE) concernant les conditions de licence de Microsoft, qui ont été résolues à l'amiable en 2024. Microsoft précise que sa propre plainte en visant les conditions de licence de Microsoft devant la Commission européenne a été rejetée **plusieurs mois**. *Nous considérons que cette plainte n'avait aucune base juridique et que Google a créé artificiellement un litige purement commercial pour une question de droit de la concurrence. Pour Google, les entreprises ne devraient pas se plaindre de devoir rémunérer Microsoft pour ses logiciels lorsqu'il les utilise pour fournir des services cloud, comme tout éditeur, a le droit d'être rémunéré pour l'utilisation de ses logiciels. Toute affirmation contraire est compromise est manifestement fausse, comme le prouve la rapide hausse des revenus et des bénéfices de Microsoft.*

Ces évolutions confirment les constats initiaux de l'Autorité. Elles n'auraient probablement pas été possibles sans les pouvoirs publics, qu'il s'agisse de l'avis de l'Autorité de la concurrence ou de l'édiction de règlements. Elles montrent que l'encadrement réglementaire est susceptible de produire des effets correcteurs rapides, et étendus à l'ensemble de leurs usagers dans le monde.

Première limite, **toute position très forte d'un acteur ne peut pas être qualifiée de position de concurrence.** Il revient à l'Autorité de la concurrence de démontrer que le consommateur a subi un préjudice. *un acteur dominant sur un marché particulier, comme l'explique M. Umberto Berkani : « Si une position dominante n'est pas répréhensible en soi. En revanche, l'acteur concerné ne doit pas utiliser cette position sur un autre marché. Par exemple, le producteur exclusif de micros de haute qualité ne doit pas proposer également ses composants de qualité inférieure en liant les deux produits, car il gagnerait ainsi au détriment du consommateur. Une telle pratique fondamentale est qu'un monopole, même mérité, finit par augmenter ses tarifs au préjudice du consommateur. Il intervient donc pour sanctionner les pratiques qui ne relèvent plus du mérite, mais de l'utilisation abusive du pouvoir de marché dans le but ultime de protéger le consommateur. »* ^([210])

Deuxième limite, **le droit de la concurrence n'est pas forcément adapté pour appréhender les abus de position individuellement, par marché, ne sont pas sanctionnables.** *« Bien que nous ne disposions pas de données précises sur la dépendance des entreprises ou des administrations françaises, nous identifions un certain nombre de pratiques abusives en terme plutôt que celui de « dominant », car ce dernier revêt une acception juridique stricte impliquant une position dominante sur un marché donné. Or la complexité du numérique réside dans l'absence d'un secteur ou d'un marché unique, mais cristallise pas sur un marché unique, mais résulte d'une sédimentation d'activités où s'additionnent des effets d'apprentissage et mécanismes de verrouillage des clients. Si occuper la première place est une position permet ensuite de capter des informations et d'ériger des barrières à l'entrée. C'est là toute la difficulté pratique que dans l'espoir de devenir, à terme, l'unique opérateur de son marché. Sur certains segments, l'accumulation de phénomènes qui, pris isolément, se retrouvent sur n'importe quel marché, mais dont l'impact se manifeste. Les acteurs puissants dans le secteur du cloud, que vous avez cités, le sont également sur d'autres marchés. »*

« Toute la difficulté pour le droit de la concurrence, fondé sur le principe de la liberté d'entreprendre, est de définir l'action d'un opérateur que si ce dernier contrevient aux règles relatives aux ententes ou à l'abus de position dominante, il est impératif d'identifier un marché spécifique sur lequel l'acteur exerce sa domination. Dès lors qu'un acteur est dominant sur un marché, établir la dominance de l'un d'entre eux devient complexe, ce qui interroge l'applicabilité du droit de la concurrence 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 constatés. Mais lorsque nous sommes face à des prépondérances marquées, les acteurs sont en concurrence et ne s'entendent pas, il faut un autre texte pour intervenir. C'est là toute la difficulté, 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, un maillon essentiel.** Sa raison d'être est d'empêcher la constitution de positions causant un préjudice au consommateur. *conçu comme un instrument pour renforcer des positions d'acteurs nationaux « S'agissant des grandes entreprises, je retiendrais d'abord que le droit de la concurrence n'entre pas en compte dans la création de grandes entreprises. Les concentrations ne s'oppose pas à l'émergence de tels acteurs, mais consiste à analyser les pouvoirs de marché. Ainsi, lorsque les marchés examinés présentent une dimension nationale, par exemple en raison de la spécificité 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 objectifs politiques qui n'est pas son objet. D'autres moyens sont plus adaptés pour favoriser le développement de filières et de territoires. *d'être une fin en soi, constitue un moyen dont l'objectif précis est de garantir le développement de certaines filières. D'autres ambitions politiques, notamment en matière économique, il n'appartient qu'aux pouvoirs publics de décider. Le droit de la concurrence ne substituer à la représentation nationale ou aux gouvernements pour atteindre des objectifs de politique économique. Cela signifie pas que le droit de la concurrence soit hermétique à ces enjeux, mais que sa mission est de 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, les autorités de régulation n'appliquent pas complètement des textes existants : *« La Commission européenne a imposé des contraintes liées à l'application des règles de concurrence ou du DMA qui pèsent sur les entreprises françaises. En échange d'une baisse de droits de douane sur l'acier et l'aluminium. Cependant, l'adoption des règles de concurrence ne doit pas être une fin en soi, mais un moyen de garantir le développement de certaines filières. »*

pour des entreprises qui font 30 %, 40 % voire 50 % de leur chiffre d'affaires sur le marché européen, la réaction des marchés financiers. Pour nous, c'est un élément essentiel : si nous représentons un tel profit, nous devons l'utiliser dans la logique de rapport de force qui prévaut désormais – et qui est la confiance. »

L'application de sanctions pécuniaires et d'injonctions intervient au terme de procédures visant à démontrer une atteinte à la concurrence sur un marché pertinent. Elle ne permet pas de résoudre les tensions économiques et techniques entre les Gafam et les autres acteurs. De ce point de vue, le démantèlement structurel, mais il est fortement encadré, comme l'indique M. Umberto Berkani : *« À l'instar du droit américain, nous pouvons défaire des positions dominantes, bien que le standard de preuve requis soit extrêmement élevé. La liberté d'entreprendre : des mesures attentatoires aux libertés individuelles ne peuvent être appliquées qu'à des exceptions exceptionnelles »* ⁽²¹⁴⁾.

Plutôt que de mettre en œuvre cette solution ultime, la Commission européenne a souhaité compléter les mécanismes de contrôle des pouvoirs de marché *ex ante*, complétant les pouvoirs de sanction *ex post*.

C. LE DMA, L'INTRODUCTION DE MESURES DE RÉGULATION EX ANTE APPLICABLES AUX PLATEFORMES

Le DMA résulte d'une forme d'aveu d'échec, ou en tout cas du constat selon lequel le droit de la concurrence ne peut prévenir avec efficacité les agissements de grandes plateformes du numérique, compte tenu de la célérité et du choix de donner compétence exclusive à la Commission européenne pour prendre des décisions d'efficacité face à des acteurs de taille mondiale.

Ce règlement introduit des règles spécifiquement applicables aux plateformes qualifiées de « services de plateforme essentiels » par la Commission européenne qui fournissent l'un des dix « services de plateforme essentiels » visés par le texte et mentionnés dans l'annexe (accès à des données, capitalisation boursière...). Les entreprises désignées comme contrôleurs d'accès de ces services ont des obligations et d'interdictions : par exemple, permettre l'interopérabilité de leurs services avec les services de concurrents, ne pas favoriser leurs propres services et produits proposés par rapport aux services ou produits similaires de concurrents (articles 5 à 7 du DMA).

Le DMA ne constitue pas une rupture avec le droit de la concurrence. En effet, les obligations imposées sont des pratiques anticoncurrentielles sanctionnées par les autorités de concurrence. Le DMA est un outil complémentaire aux pratiques traditionnelles qui restent pleinement applicables aux pratiques non couvertes par le DMA. Il repose sur une logique *ex ante*, spécifique aux pratiques d'acteurs importants pour garantir un secteur numérique plus équitable et plus concurrentiel, les pratiques anticoncurrentielles et en protégeant les consommateurs et les entreprises. Comme l'explique la Commission : *« le nouveau niveau de régulation s'explique par la complexité de la collecte de données, issue de sources multiples, et le fait que la concurrence dispose de leviers puissants, il ne peut cependant pas tout traiter seul. Le DMA est indispensable pour gagner en réactivité face à des pratiques déjà bien identifiées, sans pour autant que cela n'appartient pas au DMA de créer de nouvelles catégories d'abus, cette mission demeurant le propre des autorités de concurrence. La complémentarité s'opère ainsi : dès lors qu'une pratique ne relève pas spécifiquement du DMA, elle continue d'être traitée par le droit de la concurrence, 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 anticoncurrentielles. Sur le fondement du DMA ont été prononcées le 23 avril 2025, à l'encontre d'Apple (500 millions d'euros d'amende) et Google (435 millions d'euros d'amende) deux décisions. Dans un document de travail d'avril 2026, la Commission a analysé les effets de la mise en œuvre du DMA sur la concurrence.

Selon la Commission, la première mise en œuvre du DMA s'est avérée efficace pour la conception technique et les dispositions contractuelles des contrôleurs d'accès, créant ainsi des conditions de concurrence plus équitables. La Commission renvoie notamment aux exemples suivants :

- les navigateurs et moteurs de recherche alternatifs, notamment Aloha, Ecosia, Qwant et DuckDuckGo ;

– les utilisateurs finaux peuvent désormais facilement transférer leurs données en dehors de compris les données issues des publications et des likes sur les réseaux sociaux Facebook, Instagram 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 à ces services ;

– les hôtels et les loueurs de voitures peuvent désormais fixer leurs propres prix et conditions, plus empêchés de proposer de meilleures offres en dehors de plateformes telles que Booking.com, ou de meilleures conditions pour les utilisateurs finaux.

Enfin, la Commission souligne qu’elle restera particulièrement vigilante s’agissant des secteurs dans lesquels elle a déjà pris des mesures. Elle continuera de suivre l’évolution du marché et d’évaluer les mesures nécessaires lors des prochains réexamens. Elle a ainsi annoncé l’ouverture de trois enquêtes, à

– deux enquêtes de marché concernant une éventuelle désignation « qualitative » d’Amazon et Google. L’instruction de la Commission conclut que ces services constituent des points d’accès majeurs pour atteindre leurs utilisateurs finaux (*important gateways*), ces services seront ajoutés à la liste des services. Amazon et Microsoft sont déjà désignés comme contrôleurs d’accès et les obligations du DMA leur seront appliquées à partir de la fin de l’année 2026 et, en cas de désignation, les obligations de conformité s’appliqueront également.

– une troisième enquête de marché vise à recueillir des informations auprès des acteurs du marché. Les obligations actuelles au titre du DMA sont efficaces pour lutter contre les pratiques dans le secteur de la vente liée et de groupage et les clauses contractuelles potentiellement déséquilibrées.

Du fait de ses caractéristiques et des positions qu’ont progressivement constituées les Gafas, les plateformes sont plus scrutées par les autorités européennes et nationales chargées de l’application du droit de la concurrence. Ces pratiques sont significatives, puisqu’elles dépassent 17,2 milliards d’euros depuis 2010. Google concentre à elle seule plus de 30 % des revenus attribués 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 prévoient de longues procédures, nécessitant de démontrer, rétroactivement et avec un haut standard de preuve, une infraction déterminée. Dans un écosystème en perpétuelle évolution, les grands acteurs internationaux continuent de bénéficier de l’apparition constante de nouvelles technologies et de nouveaux services donne systématiquement l’avantage à chaque fois aux mêmes logiques (préférence donnée à ses propres produits, vente groupée, barrières à l’entrée, négociation déséquilibrée des conditions contractuelles).

L’entrée en vigueur du DMA pourrait constituer un tournant, et ses effets devront être scrutés pour mesurer s’il a entraîné un changement profond du fonctionnement du secteur. Toutefois, et ainsi que pour les crédits cloud et des *egress fees*, la mise en application du DMA ne doit pas détourner les pouvoirs de régulation susceptibles de faire changer rapidement des pratiques tuant dans l’œuf les vellétés des nouveaux entrants.

Toute l'ambition de l'initiative Eurostack consiste justement à pousser les entreprises européennes à la mesure de couvrir l'ensemble de la stack et de concurrencer les *hyperscalers*. Le récent appel d'offres en matière d'informatique en nuage a donné à voir une dynamique similaire, les cloudeurs ayant candidi

Le défaut d'intégration n'est pas un obstacle lorsque l'on dispose des compétences internes. M. Nicolas Vivant, directeur de la stratégie numérique de la commune d'Echirolles : « *Concernant beaucoup d'intervenants déplorer le manque de solution intégrée. Pour les communes de taille moyenne, d'intégrer de façon cohérente l'ensemble des solutions dans notre système d'information. C'est notamment le cas de Nextcloud pour résumer un texte, ou de lancer une visioconférence depuis notre messagerie. Quand on s'appuyant sur des prestataires, ce travail d'intégration peut être fait. La filière du libre a raison. Une solution « tout-en-un » est un handicap face aux big tech. Mais dans les collectivités, nous pouvons le faire nous-mêmes.* » ^([227])

Des appels d'offres récents se sont également traduits par la sélection de partenaires européens pour 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 de nuage aux institutions et organismes de l'Union européenne, pour un montant maximal de 180 millions d'euros. Ils ont été sélectionnés sur la base du *Cloud Sovereignty Framework* élaboré par la Commission en octobre 2020. Ils ont été évalués sur huit critères stratégiques, juridiques, techniques, opérationnels et environnementaux ^([229]). Il s'agit de : l'opérateur luxembourgeois Post Telecom avec CleverCloud et OVHcloud ; l'offre cloud allemande de la firme télécom belge Proximus, en partenariat avec S3NS, Clarence et Mistral.

B. LES PASSEURS DE TECHNOLOGIE : LE RÔLE DES CABINETS DE CONSEIL ET DES CENTRES DE RECHERCHE

Les grandes entreprises numériques extra-européennes peuvent s'appuyer sur tout un réseau de passeurs de technologie. Les travaux de Mme Ophélie Coelho ont ainsi mis en évidence le rôle des « passeurs de technologie » : « *Ce sont, par exemple, les sociétés de conseil, souvent américaines, mais aussi des startups de technologies, qui ont été formés quasi exclusivement à des technologies propriétaires. Il est rare de trouver des technologies open source ou européennes. Une fois sur le marché du travail, ces ingénieurs deviennent des ambassadeurs de ces géants, car leur accès à l'emploi dépend de ces technologies privées.* » ^([230])

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 peuvent contribuer à perpétuer leur domination sur le marché, en recommandant à leurs clients de retourner chez eux.

Le poids de ces prestataires au sein de l'État a été mis en lumière par la commission d'enquête sur le rôle des cabinets de conseil privés sur les politiques publiques. Ses travaux ont montré que les dépenses des cabinets de conseil privés dans le segment informatique, ce qui représentait 646 millions d'euros dans le secteur public en 2021 ^([231]), ont augmenté de 50% en 2025, Capgemini ayant réalisé 588 millions de chiffre d'affaires avec le secteur public en France ^([232]).

La commission d'enquête a cherché à déterminer le rôle que jouaient ces cabinets de conseil dans la mise en œuvre de technologies. Si le directeur général de Capgemini a attesté que la décision revenait entièrement aux administrations, les coproductions peuvent être parfois floues, notamment lorsque les prestataires interviennent très tôt dans le processus. La question se pose de l'influence qu'a eue Capgemini dans le choix de Microsoft Azure pour héberger les données de EDF, plutôt que dans celui de Salesforce et AWS par EDF.

Le président et la rapporteure ont relevé les nombreux liens qu'entretient Capgemini avec les grandes entreprises numériques, notamment conclu des partenariats stratégiques avec Microsoft, AWS et Google, afin d'accroître la visibilité de ces entreprises sur le marché des technologies de ces entreprises.

signe un partenariat avec AWS pour implémenter son cloud souverain, dont il a été montré les limites à la **création de Bleu**, dont elle possède 50 % aux côtés d'Orange, qui a vocation à proposer la technologie de Microsoft. **La rapporteure a regretté une décision « qui permettra à Microsoft de que la qualification SecNumCloud aurait pu être l'occasion de développer des services numériques européennes. »** ^([235])

Certains éditeurs auditionnés ont questionné les prix élevés pratiqués par les ESN lorsqu'elles sont en décalage avec leur contribution réelle. M. Thomas Fauré, président de Whaller, a ainsi cité l'exemple du projet remporté auprès de Pôle emploi grâce à Accenture : *« Il me semble qu'à cette occasion il y a eu une sous-évaluation. On a dirigé le projet au départ, mais nous a ensuite facturé une sorte de mensualité pendant toute la durée de la rétribution pour nous avoir apporté l'affaire, sans service associé. »* ^([236])

La rapporteure relève que les ESN perçoivent un montant de crédit d'impôt recherche bien supérieur à celui que reçoivent de jeunes entreprises technologiques innovantes. À elles deux, les sociétés ont obtenu cinquante fois plus de CIR que Mistral AI en 2025. L'émission « Complément d'enquête » du 18 septembre 2025 a rapporté plusieurs témoignages suggérant que Capgemini détournait en partie le CIR de son objet principal entre deux missions. Si Capgemini a dénié ces affirmations, la rapporteure appelle l'État à renforcer le dispositif pour 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 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 une influence sur la demande. En 2025, ce sont plus de 2,6 milliards d'euros d'achats numériques – matériels, logiciels – qui ont été réalisés par le biais de l'Ugap ^([237]). La centrale d'achat de l'informatique hospitalière a réalisé plus de 2 milliards d'achats numériques par an pour ses plus de 2 000 membres des secteurs hospitalier, médico-social et médico-technique et des télécoms (Canut), dédiée aux collectivités locales et aux établissements publics, a réalisé plus de 1 milliard attendu entre 120 et 150 millions en 2025 pour plus de 3 000 bénéficiaires ^([239]). Le recours à ces structures publiques de sécuriser et d'accélérer la passation de marché, puisque les procédures de publicité et de mise en concurrence 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 a constaté que la plus grosse de ces centrales, l'Ugap, contribue à entretenir la dépendance des administrations au regard de la commande publique se bornant à *« assurer une simple intermédiation entre l'offre et la demande de solutions étrangères »*. Elle a longtemps reflété la domination des acteurs états-uniens sur le marché, comme en a témoigné M. Albert Besson : *« Au début du site internet des achats de logiciels, on voyait un gros logo Microsoft, un gros logo Oracle et un gros logo SAP. On trouvait dans un fichier Microsoft Excel. »* ^([241])

En 2025, l'Ugap a déclaré 293 millions d'euros d'achats de produits Microsoft, 69 millions d'achats de produits Oracle sur son marché multi-éditeurs ^([242]). Les réponses écrites adressées par les ministères à la rapporteure ont révélé que les 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. Son statut a explicitement la mission de contribuer au renforcement de la souveraineté industrielle et numérique. Lors de sa signature, le 2 juin 2026, de son nouveau contrat d'objectifs et de performances (COP) 2026-2030, elle a déclaré : *« L'UGAP a pour mission de soutenir la souveraineté numérique, notamment en matière numérique, ainsi que les offres des PME et des startups innovantes. »*

Dans cette dynamique, l'Ugap travaille à renforcer l'information offerte à ses clients pour



VMWARE FRANCE

Les logiciels VMware sont au cœur des infrastructures informatiques les plus complexes.

Grâce au soutien de son vaste écosystème de partenaires, et à ses offres Cloud de sécurité, de gestion des réseaux, et des espaces de travail numériques, l'entreprise propose un socle dynam...

[Une plus](#)

Exprimer mon besoin

Offre

Informations

Date de création	17 novembre 2003	Adresse du siège social	TOUR FRANKLIN 100 A 101 100 JARD BOCHLEDEU 92800 PUTEAUX
Capital	200 000 €		
Effectif	422 salariés	Maison mère	FRANCE
Catégorie d'entreprise	Entreprise de Taille Intermédiaire	Code NAF	6203Z
Chiffre d'affaires	108 277 702 €	N° SIRET	45178268400034
Date du bilan	31 octobre 2025	N° TVA Intracommunautaire	FR44451782684

Besoin d'aide ?

M. Edward Jossa a reconnu les limites de cette approche : « *La question de la souveraineté dans le domaine informatique en raison du caractère dématérialisé des produits. (...) Les fournisseurs sont souvent des filiales françaises d'entreprises étrangères et les éditeurs peuvent proposer des solutions très différents. Nous nous contentons donc de retenir la nationalité du fournisseur, c'est-à-dire le pays de sa maison mère. Cette solution est d'autant plus imparfaite qu'elle repose sur une base déclarative et non sur un mouvement, mais nous n'en avons pas trouvé de meilleure* » ^([243]). L'Union des hôpitaux pour la France a souligné ce problème.

Recommandation n° 9 : Exiger que les centrales d'achat informent leurs clients sur la nationalité des fournisseurs qu'ils proposent, en se fondant sur une méthodologie solide qui tienne compte de la soumission de l'éditeur à la loi du siège, structure de l'actionnariat, liens de dépendance effectifs).

L'inertie est également favorisée par le rôle prépondérant de trois distributeurs, qui intermédiaient les logiciels – les britanniques SCC et Computacenter et le groupe européen Econom. La société SCC ne propose un grand nombre de solutions états-uniennes, ce qui limite la capacité des acteurs publics à négocier. La rapporteure souligne qu'il revient à l'Ugap de formuler des attentes plus élevées en matière de souveraineté, en particulier elle dispose à l'égard de SCC, dont M. Edward Jossa avait déclaré, devant le Sénat, qu'elle était « *très important volume considérable que représente le marché multi-éditeurs dont elle est titulaire* » ^([244]).

Le directeur de l'UniHA a reconnu la nécessité d'endosser une telle responsabilité à l'égard des fournisseurs : « *nos plus importants fournisseurs. Vous avez raison, ils dépendent de la commande publique, et de l'achat, en droit d'être exigeants quant aux solutions qu'ils mettent en avant – c'est l'un des enjeux de la commande publique* ».

La rapporteure s'est également étonnée de l'**inaction de l'Ugap face au détournement du marché Nuage public au profit de la stratégie de *sovereignty washing* d'un acteur américain**. La rapporteure identifie bien la nationalité des différents hébergeurs par l'apposition d'un drapeau, la société états-unienne du marché pour bâtir sa propre campagne de communication, entretenant le doute sur la nationalité des fournisseurs soumission au droit extraterritorial. La rapporteure appelle ainsi les centrales d'achat à la plus grande vigilance et à ne pas trompeuses qui visent à entretenir la confusion.

M. Alain Garnier a exprimé son indignation face à l'absence de réaction publique : « *Microsoft. Nous avons laissé cette situation s'installer car, à un moment donné, c'était financière perdu l'un de mes premiers combats en m'opposant à l'entrée de Microsoft dans les écoles. Au moment dans les écoles, un autre géant américain, Coca-Cola, a voulu distribuer gratuitement des canettes et son projet a été rejeté. En revanche, faire entrer gratuitement les outils bureautiques de Microsoft est une excellente chose.* » ⁽¹²⁴⁹⁾

Le général Marc Boget confirme que cette « **stratégie de lobbying extrêmement efficace** » mais vise à rendre extrêmement difficile toute transition future vers les logiciels libres, « *puisque'un outils dès son plus jeune âge cherchera naturellement à les retrouver dans sa vie professionnelle. majeur au changement pour de nombreuses organisations* » ⁽¹²⁵⁰⁾. Elle contribuerait à expliquer pourquoi les 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 annoncé le déploiement de suites collaboratives en ligne d'éditeurs non-européens dans les établissements** espaces numériques de travail fournis par les collectivités. Le ministère n'est cependant pas en mesure d'obliger 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 a reconduit pour quatre ans l'accord-cadre qui le lie à Microsoft pour l'utilisation des logiciels et solutions pour un million de postes de travail et de serveurs au sein du ministère, des organismes de recherche, des universités pour un montant maximal de 152 millions d'euros ⁽¹²⁵¹⁾, dont 2,4 millions par an pour les services centraux. Dans les établissements scolaires, les enseignants et les élèves sont, pour leur part, équipés par les collectivités. Ce privilégier des logiciels français ou européens.

Au-delà des utilisateurs, l'adhérence culturelle serait particulièrement forte parmi les parents

M. Nicolas Vivant, directeur de la stratégie et de la culture numériques de la commune de Paris, explique que la résistance au changement provient du service informatique : « *Le passage au logiciel libre implique que le service informatique doit s'adapter, et il n'en a pas toujours la compétence. Imaginez une équipe de techniciens et toutes les autres travaillent sous Windows. Si vous arrivez et déclarez que Windows n'est plus la plateforme sous Linux, un déséquilibre se crée. La personne auparavant marginalisée se trouve soudain valorisée. Le service se sentent en difficulté par rapport au projet. La résistance, et je ne l'ai pas observée ailleurs, nous l'échangeons beaucoup entre communes, provient davantage du service informatique que des utilisateurs.* »

Cette dépendance serait entretenue par la **mainmise des hyperscalers sur les offres de formation** comme dans le privé. Selon M. Henri Verdier, « *leur formation continue est assurée par quelques grands éditeurs bien qu'ils ne connaissent même pas l'existence d'alternatives. Le principal enjeu consiste à reconquérir les utilisateurs de manière autonome, de chercher et d'expérimenter de nouvelles solutions. Cela suppose aussi une formation continue* » ⁽¹²⁵³⁾.

Enfin, dans un écosystème dominé par quelques solutions reconnues, il peut être difficile pour les collectivités de faire un choix différent dont il faudra assumer seul la responsabilité en cas d'échec, comme le général de Scaleway : « *Il y a vingt ans, on disait « Nobody got fired for choosing IBM ». Je pense que cet adage en remplaçant IBM par AWS* » ⁽¹²⁵⁴⁾.

D. LA PLATEFORME DES DONNÉES DE SANTÉ : UNE DOUBLE ÉMANCIPATION DE MICROSOFT

Le cas de l'hébergement de la Plateforme des données de santé (PDS), anciennement dénommée Plateforme de données de santé (PDS), Azure est emblématique d'un écosystème qui favorise l'enfermement dans des solutions américaines.

travaux de contrôle postérieurs, qui ont démontré l'existence d'alternatives crédibles, pour certains. La commission d'enquête sénatoriale sur la commande publique a noté que l'offre Santéos, certifiée de sécurité et de performance, même si le déploiement aurait pris entre cinq et huit mois supplémentaires, était adéquat. La Cour des comptes a pour sa part regretté que l'offre du Centre d'accès sécurisé aux données (CASD) davantage au motif qu'elle n'était pas encore arrivée au terme de la procédure de certification, qu'elle était partiellement interfacée avec le SNDS ; qu'elle était autorisée par la Cnil à travailler sur des données de santé mobilisable sans appel d'offres au titre d'un contrat public-public de coopération ou d'une quasi-convention. La réponse aux exigences de la PDS a été confirmée *a posteriori* par l'obtention de la qualification de confiance après la signature du contrat avec Microsoft Azure, puis par la reconnaissance de ses fonctionnalités par la PDS en 2023 pour le projet européen d'entrepôt multicentrique de données de santé (EMC2) ⁽²⁶⁰⁾.

Le manque de considération accordée à ces solutions révèle les limites de l'étude comparative et l'absence d'alternative à Microsoft Azure. Les travaux de la commission d'enquête sénatoriale ont été réalisées auprès de l'écosystème « *n'ont en réalité consisté qu'en de simples échanges téléphoniques et de courriels, transparent et complet de dialogue et d'information qui aurait permis d'obtenir un véritable avis des acteurs disponibles sur le marché* ».

M. Michel Paulin, qui était alors directeur général d'OVH, abonde en ce sens : « *Il a été indiqué qu'il n'y avait pas de solution alternative. Mais il n'y a eu ni appel d'offres, ni mise en concurrence, ni faits factuels sur la souveraineté comme l'indice de résilience numérique, quand il n'y a pas de concurrence, il n'y a pas de solution alternative ?* » Aussi la PDS constitue-t-elle selon lui « ***l'exemple concret d'un vice de procédure*** » ***la conclusion qu'il n'y avait pas d'alternative, alors qu'en réalité, la solution avait déjà été choisie***.

La commission d'enquête s'est interrogée sur le rôle qu'avait joué dans ce choix d'hébergement **est intervenu en appui de la Drees dès la phase de préfiguration de la plateforme afin d'en définir les contours**.

Le directeur général de Capgemini, M. Aïman Ezzat, a reconnu que son cabinet avait exercé un rôle de conseil pour structurer le projet et les équipes ⁽²⁶⁰⁾. M. Laurent Vilboeuf, auditionné en tant qu'expert, a déclaré avoir constaté une forte pénétration des cabinets de conseil, pour un coût estimé à 10 millions d'euros. *« Les cabinets ont fourni un appui à la conception et à l'organisation, sous les instructions de la PDS. Capgemini, étaient intégrés aux équipes pour aider à la construction et au pilotage, à l'élaboration des réunions. Au début, les cabinets ont été fortement sollicités pour la construction de la plateforme, à raison de dix personnes par mois. »*. La circulation de documents issus du Health Data Hub présentant des signatures, selon lui, le rôle de « *coproduction* » assumé par les consultants ⁽²⁶¹⁾.

Si M. Ezzat atteste que « *les décisions sont toujours prises par les clients* », qui restent des *considérations non pas seulement techniques ou technologiques, mais aussi budgétaires, réglementaires*, la formalisation de certaines spécifications a directement contribué à orienter le choix technologique du marché réalisées par la Drees pour la PDS. La rapporteure souligne qu'un tel rôle de coordination 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'information de santé, auxquelles était proposé Microsoft Azure, et avait conclu un partenariat stratégique avec Microsoft pour la mise en œuvre 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 sur la maîtrise des données de santé des citoyens, risques qui avaient été largement occultés au cours de la mise en œuvre.

La Cnil a eu à se prononcer sur les modalités d'hébergement de la PDS dans le cadre de sa mission de protection des données. Elle a relevé que les dispositions contractuelles conclues avec Microsoft permettaient que les données de santé soient transférées aux États-Unis, ce qui était contraire à la réglementation.

reçues ». La conduite de chaque projet valide nécessite en effet que la Cnam réalise un 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 secondaire des données de santé », le gouvernement a prévu une **solution intercalaire**, à savoir la migration sur une infrastructure reposant sur une technologie Oracle au sein de la PDS. Une procédure de mise en œuvre de cette solution a été lancée le 1^{er} juillet 2025.

La ministre de la santé, Mme Stéphanie Rist, a finalement annoncé le 6 février 2026 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 l'offre a été soumise, de façon volontaire, par la PDS, elle a émis de très fortes réserves au regard de l'évolution de la solution. M. Laurent Vilboeuf, « *la Dinum a interpellé [la PDS] à propos des possibilités de l'informatique et a permis de conclure qu'il était possible de procéder à une migration vers une solution cible dans des délais raisonnables* » ^([263]).

La bascule de la PDS vers un opérateur de cloud français envoie un signal fort quant à la maturité des solutions souveraines solides, capables de répondre pleinement aux demandes de grandes entités publiques. L'analyse l'aboutissement de ce processus comme « *la rencontre entre les besoins particulièrement exigeants de la PDS et l'offre aujourd'hui disponible* » ^([264]). Alors que la PDS a réalisé plusieurs études, en 2019, 2020, 2021, l'adéquation de ses exigences aux solutions existantes, Mme Ghariani a déclaré avoir observé, notamment, « *de nouvelles offres sur le marché, mais aussi, au sein de ces offres, de nouvelles fonctionnalités, de nouveaux accès, les systèmes de gestion des clés et de chiffrement, ou encore la brique Kubernetes* », des offres « *et présentent des niveaux de service et de configuration qui nous permettent de mettre en œuvre nos projets* ». Les huit fournisseurs de cloud qui ont présenté une offre auraient eux-mêmes reconnu une évolution significative de leur offre.

Cette décision atteste également d'un rééquilibrage des critères de choix, marquant une prise en compte des considérations de performance et de délai sur les exigences de souveraineté. Bien qu'aucune offre n'ait répondu à 350 exigences formalisées dans l'appel d'offres, la PDS a estimé qu'il serait possible de mettre en œuvre des solutions de contournement raisonnables en termes de délai et de sécurité. Cette stratégie apparaît pleinement dans les comptes, qui rappelait dans son rapport de septembre 2025 que « *le parfait exercice des missions de la PDS nécessite nécessairement aligner les spécifications des systèmes d'information sur le plus haut niveau technologique disponible. La performance à court terme peut constituer un double écueil : par la mise en cause de la souveraineté des données 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 les hyperscalers qui génèrent plusieurs centaines de milliards en Europe, évidemment que non, nous ne pouvons pas le faire demain. Mais ce n'est absolument pas le sujet. Le sujet, aujourd'hui, est de savoir comment nous pouvons garantir des données sensibles pour l'ensemble des opérateurs et des clients.* » ^([265])

L'expression des besoins, qui a pu être consultée par la rapporteure, témoigne d'une prise en compte de la maîtrise des données. Outre l'obligation faite aux prestataires privés de garantir la protection des données des personnes publiques d'États tiers non autorisé par le droit de l'Union européenne ou d'un État membre, conformément à l'article 17 de la RGPD, la PDS s'est attachée à évaluer leur résilience en cas de rupture de service, ou *kill switch*. Cette problématique est particulièrement prégnante s'agissant des clouds dits hybrides, opérés par des prestataires européens ou américains, tels que Bleu et S3NS. Une série de questions complémentaires visait ainsi à vérifier le maintien en conditions opérationnelles et en bonnes conditions de sécurité de la plateforme en cas de panne du fournisseur ne relevant pas de la juridiction de l'Union européenne, à garantir que le support opérationnel et juridique européen, ou encore à limiter leur dépendance à des fournisseurs extra-européens.

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 taille des administrations. Faute de disposer des effectifs nécessaires, celles-ci sont parfois contraintes de se tourner vers des prestataires externes pour 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 *cours des trente dernières années, l'État a externalisé les compétences de développement logiciel. Comment réinternaliser ces compétences pour que, lorsqu'une ville, une entreprise ou un ministère ait besoin de personnes capables de « soulever le capot » et de comprendre comment il fonctionne. Le processus est une « prolétarianisation » : on nous a retiré le savoir sur le fonctionnement du logiciel. On nous parle de « dématérialisation » alors qu'il s'agit de quelque chose de très territorialisé et physique. Il va falloir reprendre la main sur les connaissances du fonctionnement du numérique si nous souhaitons que des collectivités, des entreprises puissent basculer vers le libre. » ([268])*

Alors même que l'externalisation excessive des compétences numériques de l'État et les retards dans les progrès demeurent très limités. Cela tient notamment à une gouvernance des ressources humaines numériques fragmentée. Bien que rattachée au Premier ministre et au ministre de l'action et des comptes publics, « la DSI est interministérielle, comme le remarque Henri Verdier. Sa mission consiste à animer un réseau interministériel de référentiel général de sécurité ou celui relatif à l'accessibilité, mais elle n'intervient ni dans le pilotage des budgets. » ([269])

1. Une répartition très inégale des ressources humaines numériques qui reflète des stratégies divergentes

La commission d'enquête a constaté que les taux d'externalisation restent élevés, avec ce qui traduit l'absence de gouvernance unifiée des ressources humaines numériques.

La commission d'enquête s'est attachée à mesurer le niveau de dépendance aux prestataires numériques en consultant les DSI et en demandant à chacune de renseigner les effectifs de leur DSI et le nombre de prestations réalisées. Les chiffres ci-dessous doivent cependant être lus avec prudence, les ministères n'ayant pas tous retenu les mêmes modalités de comptabilisation des ressources humaines et recourant à l'externalisation selon des modalités variées, de l'intégration de prestataires à l'externalisation complète de certaines missions à une entreprise de services numériques, alors évalués. Les taux globaux offrent une première analyse, ils n'apportent pas la finesse nécessaire pour apprécier la dépendance à l'externalisation pour des fonctions critiques ou un projet numérique donné.

Les taux d'externalisation des compétences renseignés par les DSI sollicitées varient dans une large mesure, allant de 0 % à 80 % sur certaines fonctions. « En interministériel, il a été admis qu'un taux dépassant 60 % est préoccupant. À 80 %, la situation n'était plus maîtrisable », a indiqué Audran Le Baron, directeur du numérique pour le

Éducation nationale	2 195	centrale et 23 % en déconcentré)	17 % (36 % en centrale et 12 % en déconcentré)
Intérieur	2 100 hors police et gendarmerie 700 à la DTNUM		Non renseigné 332 prestataires présents sur site pour contribuer à la gestion des SI 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

Le ministère de l'intérieur, la DGFIP et le ministère de l'éducation nationale fonctionnaires avec une spécialisation dans le numérique. Pour M. Mathieu Weill, « *cette considérable pour ces organisations : le fait qu'elles disposent des compétences nécessaires en dépendances.* » ⁽²⁷¹⁾

L'internalisation des compétences est, en effet, au fondement de la stratégie de maîtrise comme l'a expliqué son directeur, le général Marc Boget : « *Mon premier principe est de ne jamais nous recourons ponctuellement à des prestataires extérieurs, c'est toujours sous la direction d'un n tout moment, de changer d'industriel sans fragiliser l'institution.* » ⁽²⁷²⁾. Dans ce but, la gendarmerie, ans, une filière de gendarmes spécialisés en « systèmes d'information et de communication », qu rares nécessaires pour assurer en interne la gestion des postes de travail, l'architecture logicielle et de ses data centers. Le taux d'externalisation de l'Anfsi demeure ainsi limité à 20 %, avec 448 agents.

Les gendarmes recrutés par cette voie spécialisée sont amenés à alterner au cours de leur car techniques, selon un modèle de polyvalence qui « *permet à nos officiers et sous-officiers de conce réalités opérationnelles* », fait valoir le général Marc Boget. Ces possibilités de mobilité contribuent filière : « *Un aspect fondamental de notre stratégie d'internalisation réside dans le refus d'une filière ne rejoindra pas la gendarmerie pour y exercer les mêmes missions que dans le secteur privé, où le qui motive ces personnels et garantit leur fidélité, c'est la perspective d'une carrière alternant des f modèle, qui offre à la fois du sens et une visibilité sur la trajectoire professionnelle, est notre meille alors même que ces profils sont très courtisés par le marché* » ⁽²⁷⁴⁾. L'ouverture du concours universitaires, et la réalisation de formations en partenariat avec de grandes écoles d'ingénieur visent

La DGFIP dispose d'un modèle similaire. Sur 95 000 agents, la direction compte 5 000 int interne ses systèmes d'information : des équipes dédiées prennent en charge l'ensemble des mé

600 prestataires pour les évolutions de ses différents produits. De même, les effectifs numériques de la gendarmerie, demeurent trop limités au regard du nombre de projets, comme l'a expliqué Mathieu V. *chargée de tout ce qui n'est pas police et gendarmerie, compte environ 700 emplois ; ils couvrent développement, etc. Nous avons 150 à 200 projets en cours ; vous imaginez bien que le taux d'externalisation est très élevé, partie développement »* ^([277]).

D'autres administrations ont engagé des efforts pour retrouver une maîtrise interne, comme le ministère de la Santé en son sein d'une usine logicielle. Jusqu'en 2020, l'ensemble des développements était piloté par des compétences internes. L'usine logicielle *« reste en grande partie constituée de prestataires externes (et de ressources) »*.

Afin de réduire sa vulnérabilité et sa dépendance aux fournisseurs de solution, l'AP-HP a développé des compétences internes sur des briques considérées comme critiques ou pour lesquelles des manques de solutions ont été identifiées. Elle *« investit fortement dans des briques d'interopérabilité (EAI/bus développé en propre) et une expertise sur le fond (standards européens règlement EHDS, HL7 FHIR, etc.) permettant de réduire la dépendance (...)». Elle réalise des développements en propre pour une partie réduite du parc applicatif (environ 10 %), celle de se baser sur des éditeurs, en assurant sa capacité, dans la mesure du possible, d'en changer. La maîtrise interne représente un métier assez lointain de celui de l'AP-HP (qui assure déjà largement ceux d'hébergeur), mais s'avère parfois utile pour la réduction de la dépendance, ou pour palier des lacunes. Elle fournit deux exemples dans lesquels le choix de développer des solutions en interne s'est révélé pertinent : le premier, pour lequel les coûts sont moindres que pour une solution externe, et la création de solutions internes (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, pour les CAFs ou ceux à destination des allocataires et des partenaires. Dans un contexte de trajectoire de dépendances technologiques constitue un enjeu majeur pour la résilience, la sécurité et la souveraineté, la réduction des dépendances est au cœur de nos préoccupations, nous diversifions notre portefeuille de solutions, la maîtrise des situations de dépendance excessive vis-à-vis d'un prestataire unique (vendor lock-in) »*. La Cnam est développée par des ressources internes accompagnées d'entreprises de services numériques. La Cnav, pour laquelle *« les développements internes et la maintenance associée représentent 4 fois le coût des prestations hors poste de travail [102 millions contre 25,5 millions]. Que ce soit pour des développements professionnels ou pour des métiers, ceux-ci sont réalisés par des ressources internes avec le cas échéant une extension de compétences. Les ressources internes sont des profils d'analyse fonctionnelle pour la conception, et des concepteurs-développeurs pour les aspects techniques sont celles validées et recensées au catalogue technologique de la Cnav »* ^([280]).

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 de forte dépendance d'externalisation.

Le **ministère de la justice** a souligné, dans ses réponses écrites, qu'il disposait d'effectifs dédiés à l'informatique pour 0,8 % de ses personnels, contre 3,1 % en moyenne.

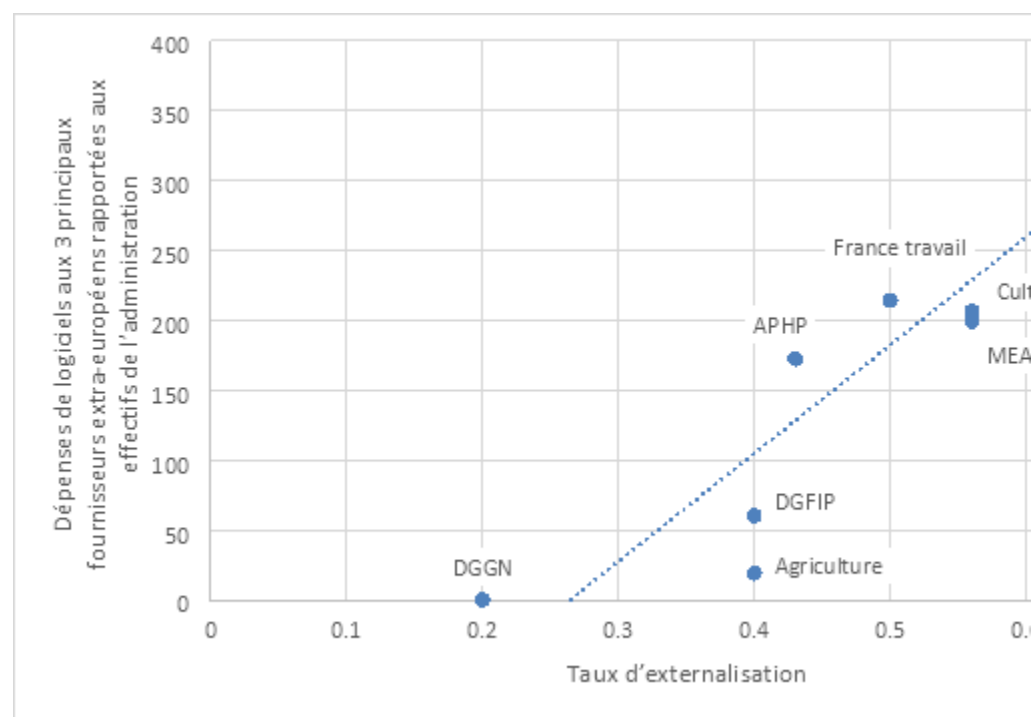
Faute de disposer des compétences internes nécessaires, le ministère a un recours important à des prestataires informatiques, pour un coût autour de 200 millions d'euros par an, correspondant à 1 500 ETP, à côté de 666 ETP du ministère, dont moins d'une vingtaine de développeurs. L'infogérance des SI métiers et des SI liés à l'environnement de travail, hébergés sur site, font également l'objet d'infogérances systématiques. **d'externalisation pouvait atteindre 90 % sur certains projets, avec parfois même une fonction de prestataire.** S'il est depuis redescendu, grâce à la campagne interministérielle de réinternalisation de 2024, il demeure au-dessus du seuil de 60 % recommandé.

La rapporteure souligne que le manque de compétences internes questionne la faisabilité des

De fait, le manque de compétences numériques des administrations contribue à expliquer le succès des « packagées » proposées par les grandes entreprises numériques, plutôt que de déployer des solutions qui devraient assurer elles-mêmes l'exploitation, l'intégration et le développement. « *Face au manque de compétences numériques des administrations publiques, ces grandes sociétés ont compris qu'il fallait cesser de vendre le logiciel et proposer des services. Les administrations publiques paieraient pour que cela fonctionne* », relève Renaud Chaput, directeur technique chez Orange.

Le croisement du taux d'externalisation de différentes administrations avec le budget qu'elles consacrent aux solutions états-uniennes dominantes du marché tend à montrer l'existence d'une **corrélation claire entre le budget des administrations et sa dépendance à des acteurs extra-européens**. Pour évaluer le niveau de dépendance des administrations aux solutions américaines, la commission d'enquête s'est fondée sur les dépenses moyennes licences logiciels extra-européens par agent, estimées à partir des réponses écrites et de l'effectif des entités ⁽²⁸⁴⁾.

DÉPENDANCE DES ADMINISTRATIONS À L'ÉGARD DE FOURNISSEURS DE LOGICIELS EXTRA-EUROPEENS ET 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'année 2019.

**Le ministère de l'éducation nationale n'a pas été retenu dans le périmètre car les personnels enseignants sont équipés par les collectivités locales et les caisses de sécurité sociale, n'ont pas non plus été traités 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 privilégie les solutions dont la gestion et le développement sont internes. Ce critère favorise parfois le choix de solutions d'éditeurs ayant un service intégré et défavorise le recours à des solutions open source, même si elles sont utilisées dès que possible* » ⁽²⁸⁵⁾.

De même, c'est le déficit de ressources internes qui aurait motivé le choix du ministère de l'intérieur pour son cloud interne sur la solution de VMware, plutôt que sur des technologies libres. Selon l'association VMware, le cloud interne a permis au ministère « *d'opérer un cloud interne avec une économie de moyens humains et matériels sans commune mesure avec ceux qu'il faut employer pour faire fonctionner un cloud sur des technologies libres* ». Cela rejoint la question des compétences internes : c'est précisément le manque de possibilités internes suffisantes, en nombre comme en expertise, que nous avons recouru à ces technologies.

L'État semble, de fait, s'être dessaisi des compétences de développement et de conception de logiciels. Cette culture, très répandue parmi les DSI, tant dans le secteur privé que dans le secteur public, a conduit à une externalisation croissante des compétences numériques.

De fait, **les administrations qui bénéficient d'importantes compétences internes, telles celles qui ont mis en œuvre les stratégies les plus ambitieuses en matière de réduction des dépenses**, 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 numérique les plus critiques pour que l'État retrouve la maîtrise de son activité numérique** **3 500 postes supplémentaires d'ici 2028 sur le périmètre des ministères civils**, notamment en matière de 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 priorités de la stratégie numérique de l'État** dans la feuille de route de 2023 de la Dinum. Elle a été inscrite dans le « DRH du numérique de l'État » avec l'objectif de recruter et fidéliser des talents dans le numérique et ces compétences rares.

Par une circulaire du 13 février 2023, la Première ministre Elisabeth Borne a fixé des limites aux prestations intellectuelles informatiques : « *Un grand projet dont le pilotage ou la réalisation est considéré à risque, être suivi de manière plus approfondie et faire l'objet d'un recrutement d'une équipe 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 un plein (ETP) dans les lettres plafond du projet de loi de finances pour 2024. M. Audran Le Baron, directeur du numérique, a salué « *une vague de réinternalisation de 60 ETP qui s'est avérée cruciale pour ramener les taux de nos projets à des niveaux soutenables* » ^{(295)]}.

Le ministère de la justice a bénéficié, dans ce cadre, de 40 ETP supplémentaires sur des fonctions qui lui ont permis de retrouver une certaine maîtrise. Plus aucun projet ne dépasse désormais le taux d'externalisation. L'architecture d'ouvrage est systématiquement internalisée. Le ministère demeure cependant toujours au-dessus du seuil de 80 %.

La loi d'orientation et de programmation du ministère de l'intérieur (Lopmi) du 24 janvier 2023 prévoit la création de postes numériques, incluant un volet cybersécurité et des postes en services déconcentrés, ainsi que la création de postes à l'Anfsi. Le directeur de la transformation numérique, M. Mathieu Weill, a indiqué que 100 postes ont été créés. *La trajectoire a dû être révisée pour tenir compte des contingences budgétaires, le ministère de l'intérieur a réinternalisé les postes-clés du numérique. Une trentaine de créations de postes sont encore prévues pour la réinternalisation, en dépit de différentes contraintes, notamment celles liées au plafonnement des dépenses. Nous voulons maîtriser nos dépendances et réduire nos vulnérabilités.* » ^{(296)]}

La vague de réinternalisation aurait permis de réaliser une **économie nette de 18,3 milliards d'euros** interministérielle du numérique ^{(297)]}.

Ces efforts n'ont cependant pas été poursuivis les années suivantes, et demeurent bien en deca de ce que le CGE. Ils n'ont, par ailleurs, pas été ciblés sur les ministères les plus vulnérables. Ainsi, les ministères ont 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 numérique engagée en 2024. C'est notamment le cas de M. Audran Le Baron qui a déclaré « *la vague interministérielle, pour obtenir des dispositifs de réinternalisation de compétences et donc la création de postes* » faisant valoir que certains des systèmes cœur de métier du ministère présentent encore des faiblesses.

préservation de la souveraineté au rang des priorités de la transformation numérique. Elle dispose d'action : un rôle de prescription visant à orienter les choix technologiques vers des solutions d'animation interministérielle, en favorisant le partage d'expérience et la coordination ; et le d mutualisées au niveau interministériel afin de proposer des alternatives souveraines.

Cette stratégie se heurte néanmoins à une gouvernance numérique éclatée entre les d positionnement institutionnel de la Dinum. Placée sous l'autorité conjointe du Premier ministre publics, elle n'a pas d'autorité hiérarchique sur les directions du numérique, qui dépendent de c manière autonome. Comme le confirme Mme Julia Mouzon, déléguée du comité stratégique de filiè de confiance, « *la Dinum, ou même le Premier ministre lorsqu'il édicte des circulaires sur la comm la plupart des cas, n'imposent pas. Sur toutes les questions de sécurité et d'alignement stratégique s pluralité d'objectifs et d'outils, où chacun va créer, utiliser et choisir ses propres solutions.* » « *dispose* », résume Michel Paulin, président du CSF ^([301]).

1. Des exigences de souveraineté aisément contournées

a. Un dispositif d'audit des grands projets numériques de l'État qui devrait permettre d'app

Le principal pouvoir de contrôle dont dispose la Dinum à l'égard des ministères repo projets numériques de l'État. Conformément à l'article 3 du décret du 25 octobre 2019 r **communication de l'État et à la direction interministérielle du numérique**, les projets numéri montant prévisionnel supérieur à 9 millions d'euros doivent être soumis pour avis conforme au direc d'émettre son avis, la Dinum consulte l'Anssi et la direction du budget sur les enjeux de cybersécurité

En tant que responsable des systèmes d'information de l'État, le Premier ministre conserve, *avec son bras armé qu'est la Dinum* » : il peut saisir la Dinum d'une demande d'évaluation sur ministères et des organismes placés sous leur tutelle sur la base de l'article 4 du décret du 25 octobre solliciter un tel audit. Cette procédure est néanmoins peu mobilisée, avec moins de quatre saisines p comptes ^([302]).

À l'origine, cet audit ne prenait pas directement en compte les enjeux de souverain *s'assurer que, lorsqu'on investit dans un tel projet, il respecte son budget et son calendrier et qu* après plusieurs dérives de grands projets numériques, a indiqué Stéphanie Schaer ^([303]). Par la suite, **la procédure d'avis conforme le contrôle de la doctrine Cloud au centre**, et notamment le respect 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 ou le renforcement de dépendances technologiques, comme l'a expliqué la directrice intermini *avons sur les grands projets nous amène à discuter technique avec les équipes pour identifier ce d'architecture. Notre avis peut être favorable, mais avec des recommandations ou des réserves qui avant la passation du marché et l'engagement des crédits* » ^([304]). Cela a conduit la direction à ale techniques disponibles lorsqu'une dépendance était identifiée de longue date, par exemple à Oracle. **de se prononcer sur le choix des attributaires des marchés**, puisqu'elle intervient en amont : « *s'organise avec les métiers concernés, c'est-à-dire la structure d'achat, mais pas sur les acteurs en pas encore connus* », précise Stéphanie Schaer ^([305]).

b. En pratique, un impact trop limité

La procédure d'audit n'a pas pu être pleinement mise au service du renforcement de la sou 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 p

fonctions clés de direction et d'architecture étaient encore assurées en externe, « *depossession de fonctions clés de direction et d'architecture* ». Cela aurait dû, en principe, conduire à la suspension du projet tant que les conditions de *pilotage du projet* ». Cela aurait dû, en principe, conduire à la suspension du projet tant que les conditions

Le ministère a pourtant choisi de poursuivre les développements. Au moment de la troisième réunion de la commission de suivi, le 20 janvier 2024, 31,9 millions d'euros, soit 72 % du budget total d'investissement. Dans un dernier avis rendu le 20 janvier 2024, la commission de suivi a déclaré que l'avancement du projet ne lui permettait plus de se prononcer. Elle relevait néanmoins des progrès réalisés : le taux d'externalisation redescendu à 70 %, la reprise de la majeure partie des fonctions clés, et le choix d'un prestataire français, 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 dans le cadre 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 pour le traitement des données sensibles des agents du ministère, malgré la non-conformité à la doctrine Cloud au centre, le directeur général de l'éducation nationale a déclaré que cette décision avait été prise de façon concertée « *après une analyse au plus haut niveau de la conformité de la Dinum au titre de l'article 3 du décret de 2019 et [ayant] été visé par la Cnil et l'Anssi* ».

Or non seulement l'Anssi et la Cnil ont émis un avis négatif, mais la Dinum n'a pas non plus validé le projet Virtuo. Ayant été saisie seulement en mars 2024, alors que le projet était déjà finalisé et devait être mis en œuvre le 2 avril 2024, la directrice interministérielle du numérique a estimé, dans son avis du 18 avril 2024, que le projet « *challenge les options prises* » et qu'en conséquence, « *ce projet Virtuo ne relève plus de la procédure d'avis conforme* ».

Si le ministère considère désormais que ses systèmes d'information de ressources humaines ne présentent pas une sensibilité particulière au sens de l'article 31 de la loi Sren et ne doivent donc pas être hébergés sur le territoire français, **démontre l'insuffisance de la procédure d'avis conforme pour assurer le respect par les ministères de la loi relative aux données sensibles.** La rapporteure constate l'absence de corde de rappel lorsque les ministères contournent la procédure d'avis conforme.

Plus généralement, on peut s'étonner de la **latitude dont disposent les ministères pour appliquer la loi relative aux données sensibles dont dépend l'obligation de recourir à un cloud de confiance.** À titre de comparaison, le centre national de traitement des données relatives aux ressources humaines (CISIRH) des ministères économiques et financiers a retenu un cadre de confiance pour des données pourtant similaires : « *compte tenu des données à caractère personnel traitées dans les outils concernés, les éventuels besoins de technologie cloud s'appuient systématiquement sur le cadre SecNumCloud défini par le décret n° 2016-1601 des centres de l'État, notamment Nubo* ».

c. Un récent renforcement du dispositif d'audit, qui conserve des angles morts

Par un décret et un arrêté du 18 mars 2026 ^(l309l), le Premier ministre a profondément révisé la procédure d'audit afin de l'adapter aux nouvelles pratiques. Le seuil à partir duquel un projet doit être soumis à la procédure d'audit a été abaissé afin de l'ajuster à l'évolution du coût des projets numériques. Un **seuil spécifique de 2 millions d'euros pour les projets à suites collaboratives ou de logiciels à la demande ayant recours à un service commercial d'hébergement** a été introduit. Selon Stéphanie Schaer, « *à la généralisation des solutions d'hébergement en nuage et témoignent de la mise en œuvre de 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 a été confortée par l'introduction de l'alinéa suivant à l'article 3 du décret de 2019 : « *L'examen du directeur général de l'éducation nationale doit s'assurer que les conditions de réussite du projet sont réunies et que les référentiels introduits par la circulaire n° 2016-1601 sont appliqués, notamment en matière de sécurisation des données et d'hébergement des données sensibles.* » L'alinéa a été introduit par l'article 31 de la loi visant à sécuriser et à réguler l'espace numérique, ainsi qu'en matière de préservation de l'indépendance des systèmes d'information et de communication concernés, en cohérence avec la loi n° 2016-917 du 7 octobre 2016 susvisée. »

En parallèle, la Dinum a publié en février 2026 un **vade-mecum relatif à la sensibilité des données**.

Cet effort de mutualisation se heurte néanmoins aux résistances des ministères et, malgré 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. Les deux offres de services développées par le ministère de l'intérieur, le cloud Pi, et le ministère des Armées, le cloud Nubo, ont pour vocation de répondre 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 loi sur la sécurité informatique, ce qui leur confère un statut équivalent aux offres commerciales certifiées SecNumCloud, comme l'a assuré M. Tomasz Blanc : *« notre cloud Nubo, nous intégrons les règles de sécurité technique de ce référentiel, auxquelles nous soumettons tous les systèmes d'information de l'État (PSSI-E). En matière de sécurité, le cloud Nubo se situe au même niveau que les offres SecNumCloud »* ^([311]).

Les clouds Pi et Nubo disposent de capacités similaires, comptant chacun plus de 13 000 machines virtuelles. Ils offrent de nombreux choix technologiques : Pi repose sur un partenariat avec Red Hat, pour le déploiement de la solution OpenStack, fondé sur le déploiement interne de solutions open source, en particulier OpenStack, opérées directement par les ministères. Nubo est soumise à des contraintes sur les horaires non ouvrés, la disponibilité des SI vingt-quatre heures sur vingt-quatre, la continuité de l'action publique. Pi est également seul à proposer un service de diffusion restreinte, en interne.

La Cour des comptes relève cependant, dans son rapport sur les enjeux de souveraineté des données, daté de septembre 2025, que les clouds interministériels *« restent peu utilisés, non seulement par les services de l'État, mais aussi par les autres administrations »* ^([313]).

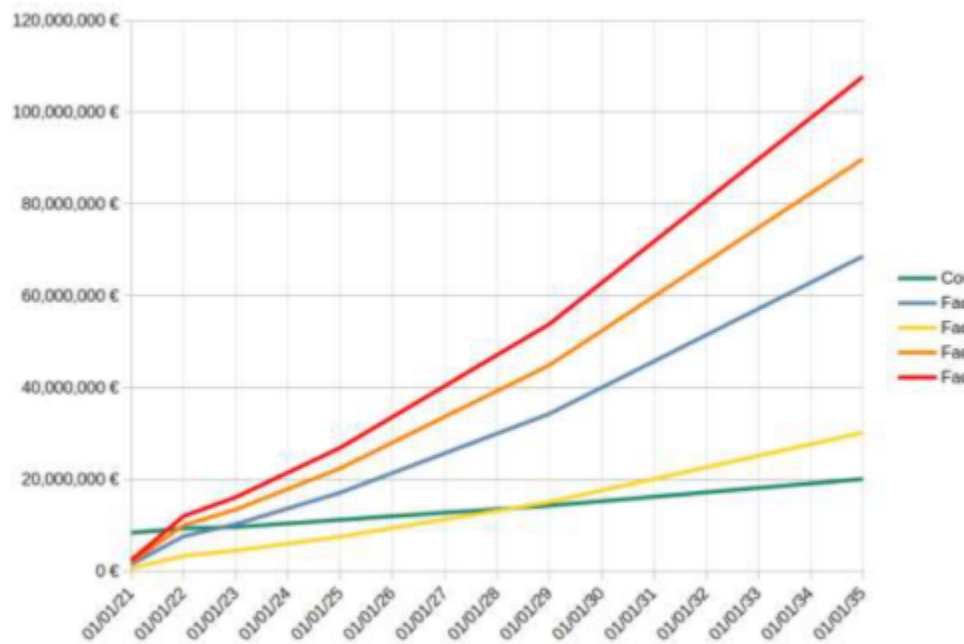
La Dinum a reconnu que, si l'usage des clouds interministériels progressait en volume, il resterait limité par l'ouverture interministérielle demeurant limitée. La consommation sur Nubo a atteint 13,4 millions de données en 2025, soit quatre fois plus qu'en 2020, mais M. Tomasz Blanc concède qu'*« une importante marge de progression reste à parcourir pour une généralisée »*. Nubo ne couvre encore qu'une part limitée des SI de l'État, même la DGFIP n'y héberge que ses données interministérielles demeure également très limitée : la DGFIP représente 91 % de la consommation sur Nubo, la part interministérielle seulement 5 % – il s'agit essentiellement de la Dinum, pour ProConnect, et du ministère de la culture ^([314]).

Si selon la Dinum, la situation serait comparable pour le cloud Pi – l'utilisation interne représente la majeure partie de la consommation –, selon le ministère de l'intérieur, 15 % de la capacité est aujourd'hui consommée par le ministère ^([315]).

Cette situation s'explique par les résistances de grandes administrations, qui *« ne peuvent pas être contraintes de partager leurs données et développent chacune leur propre cloud interne »* ^([316]). En contradiction avec la doctrine Cloud au centre, l'éducation nationale, le ministère de la transition écologique ou le ministère de l'agriculture continuent de développer leurs propres infrastructures cloud sur site, au lieu de s'engager dans la consolidation du cloud interne. Les réponses écrites, des choix qui *« fragmentent les efforts, limitent les économies d'échelle et compliquent l'exploitation de clouds robustes, dont la construction reste par nature complexe, coûteuse et exigeante »*. 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 décisions d'hébergement sont arbitrées au niveau des directions du numérique de chaque ministère, ce qui perpétue la doctrine Cloud au centre. En parallèle, le pilotage des deux clouds interministériels Nubo et Pi reste limité à la DGFIP, ce qui ne garantit pas la prise en compte des besoins des autres administrations utilisant le cloud. Les réunions trimestrielles associant les référents cloud de chaque ministère, qui se limitent à des échanges de bonnes pratiques, ne suffisent pas à assurer une véritable gouvernance interministérielle.

Le déploiement des clouds Nubo et Pi se heurterait également à une « tarification interne »



Source : Dinum, d'après DGFIP.

La rapporteure prend acte de la relance des travaux interministériels pour faire évoluer le m les nouveaux tarifs reflètent mieux les coûts de revient, afin de favoriser l'engagement de toutes les a

Certains ministères consultés mettent également en avant des limites en matière de fon regrette ainsi que « *les couches de services managés actuellement proposés ne couvrent pas l'ensem collaboratifs de grande ampleur; ce qui impliquerait des développements et des charges complémen opérationnelles objectives* » qui exigeraient de mobiliser « *des capacités d'exploitation renforcées humaine pour assurer le maintien en conditions opérationnelles, le support et l'intégration dans un s*

Si les clouds interministériels offrent des services comparables aux offres commerciales Sec demeure en effet inférieure à celle des offres des *hyperscalers*. La Dinum a confirmé que des progrès de type PaaS, de bases de données managées, d'orchestration de conteneurs, ou de gestion fine des io

Pour y remédier, la feuille de route des deux clouds prévoit néanmoins des investissements c l'intégration de cartes graphiques GPU pour accompagner des services d'IA. Ces progrès devraient la migration de certains ministères, notamment l'hébergement des SI du ministère de la justice sur le c *offres sont tout à fait utilisables par d'autres ministères, y compris dans un contexte d'attention tr* selon la DSI du ministère de l'intérieur ^([320]).

En parallèle, des travaux ont été engagés pour rapprocher les deux clouds interminist d'économies d'échelle. La Cour des comptes recommandait de « *définir la trajectoire de converg rendre plus performants et augmenter significativement leur utilisation mutualisée par l'ensemble* confirmé à la commission d'enquête que les ministères travaillaient à renforcer l'interopérabilité et 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

D'autres produits numériques sont développés et opérés directement par la Dinum. Depuis industriels français, le Réseau interministériel de l'État, un réseau unifié de communications électri l'État sur l'ensemble du territoire national et compte désormais un million d'utilisateurs. Elle assure numérique FranceConnect ou la plateforme data.gouv.fr.

La feuille de route de 2023 a confié explicitement à la direction la mission de structurer un

Les services de La Suite, en particulier, semblent correspondre aux attentes et peuvent constituer des dépendances aux logiciels propriétaires américains, d'après les réponses écrites des administrations. La gendarmerie nationale a salué des produits qui « *sont novateurs et bénéficient d'un important travail auprès de la direction nationale* », tandis que la Cnam atteste que FranceTransfert, Tchapp et Grist sont « *des agents du ministère* ». La gendarmerie nationale s'est emparée des briques Fichiers, Docs et Grist. La solution performante et sécurisée de collaboration avec des interlocuteurs internes et externes à l'administration. Tchapp répondent très bien à nos besoins en remplacement de Zoom actuellement déployé sur nos plateformes. La gendarmerie nationale attend également beaucoup de l'outil Visio, qui pourrait se substituer à la solution américaine. Les ministères auditionnés – Inrae, CEA, CNRS et Inserm – ont également annoncé avoir migré sur Visio, ou sur Teams ou de Zoom. La Suite pourrait également offrir une alternative à Office 365, étudiée notamment par la gendarmerie nationale.

Le gouvernement accompagne désormais cette diffusion de façon volontariste. Une circulaire publiée le 25 juillet 2025, a appelé à **déployer Tchapp** au sein de la sphère publique et des cabinets ministériels. La confidentialité des communications électroniques des agents publics. Puis, une seconde circulaire du 15 août 2025, a appelé à **de Visio** à l'ensemble des services de l'État, en remplacement des solutions de visioconférence. La publication de la circulaire sur la doctrine de l'État pour les achats publics numériques, en février 2025, a défini une stratégie consistant à promouvoir, au sein des administrations, un usage exclusif du « cœur de métier » FranceTransfert. Ce choix répond, pour la directrice interministérielle du numérique, au « *besoin de garantir la continuité de l'État grâce à des outils présents dans tous les ministères, avec un service sans faille en situation de gestion de crise* » ⁽³²⁵⁾.

La réussite de cette migration suppose que la puissance publique démontre sa capacité à déployer des outils numériques souverains, en garantissant leur fiabilité, leur performance et leur résilience.

Les fonctionnalités de La Suite doivent encore être améliorées, pour couvrir l'ensemble des besoins et se substituer totalement aux solutions propriétaires. À défaut, le risque est d'entraîner « *une dispersion des données* », met en garde une DSI ministérielle. Par exemple, le déploiement de Visio en remplacement des systèmes de visioconférence des salles de réunion, et aucune solution n'est encore proposée. Les défis sont néanmoins inhérents à la stratégie adoptée par la Dinum : « *en appliquant des méthodes de type agile, dans un premier temps la recherche d'impact et d'adhésion des utilisateurs en remettant l'industrialisation des besoins à des phases ultérieures* », explique la direction du numérique du ministère de la justice.

Le déploiement de La Suite auprès de plus de deux millions d'agents publics implique une planification rigoureuse. Il ne pourra réussir qu'avec des moyens humains et financiers adaptés. Si le ministère de l'intérieur a déployé plusieurs outils collaboratifs de la Dinum, concentrant 32 % des utilisateurs de Tchapp en octobre 2024 et Docs en raison du manque de capacité de passage à l'échelle de ces solutions – par exemple, l'outil Docs pour plus de 1 000 participants, besoin essentiel pour le réseau des préfetures et services territoriaux. Mais, à cet égard, qu'« *il faut que la puissance publique accompagne la Dinum pour qu'elle soit plus performante et puisse offrir un support pour le nombre d'utilisateurs ciblés.* » ⁽³²⁶⁾

Les ministères consultés ont tous souligné l'importance de définir une feuille de route claire et de la respecter dans la durée. L'industrialisation des produits et leur déploiement auprès de l'ensemble des administrations. Le changement que cela suppose, n'est possible qu'à la condition que la Dinum assure la fiabilité et la pérennité des solutions. Les économistes et financiers insistent ainsi sur « *la nécessité d'une projection plus lointaine de la stratégie à long terme, car s'il est sans doute facile de faire preuve d'agilité au niveau interministériel pour suivre les évolutions du numérique, en revanche, au niveau ministériel ou directionnel, le déploiement des outils et l'accompagnement des utilisateurs sont des délais incompressibles pour en permettre la bonne appropriation.* » ⁽³²⁷⁾

La politique d'outillage conduite par la Dinum a en effet pu manquer de continuité par exemple, la plateforme collaborative Osmose au profit de Resana, acté en mars 2024, n'ont pas pu être corrigés. La plateforme collaborative Osmose au profit de Resana, acté en mars 2024, n'ont pas pu être corrigés. La plateforme collaborative Osmose au profit de Resana, acté en mars 2024, n'ont pas pu être corrigés.

organisation ont néanmoins été marquées par une certaine confusion : alors que le Premier ministre Dinum et de la direction interministérielle de la transformation publique (DITP), il semblerait autonomie et assurera la prise en charge de la transformation numérique des démarches et des rapporteure sur les nouveaux leviers dont bénéficierait l’Ariane pour faire respecter la doctrine numérique n’a pas apporté de réponse précise. Il a renvoyé à la mission de préfiguration qui a été confiée à Arnaud.

– 1 –

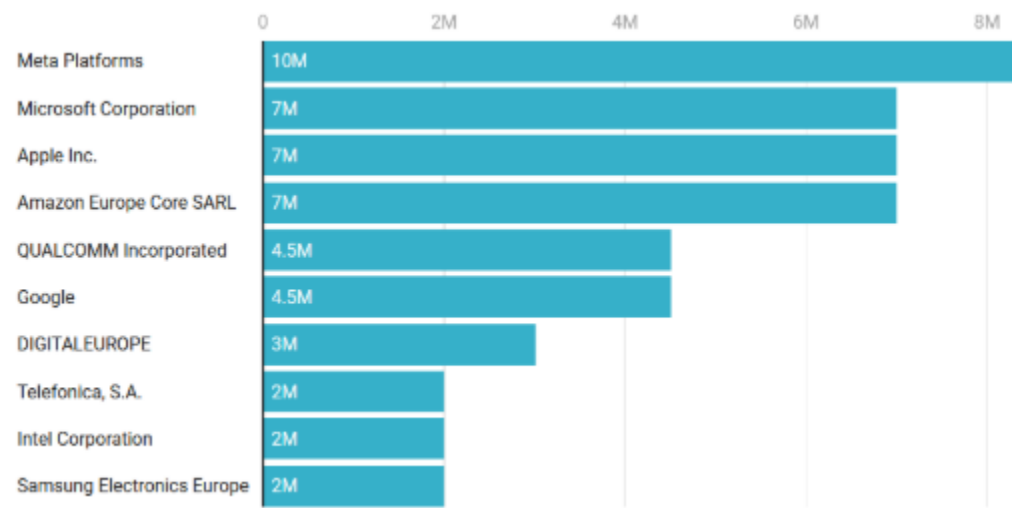
CHAPITRE 9 – LE LOBBYING : GRÂCE À DES MOYENS MASSIFS, LE COMBAT EN PASSE D’ÉCHEC À LA RÉGULATION

A. UN LOBBYING FÉROCE

La puissance du lobbying des grandes entreprises numériques extra-européennes a été soulignée et auditionnées.

Les Big Tech déploient des moyens humains et financiers considérables au service de l’industrie. Selon le registre européen de transparence, les ONG *Corporate Europe Observatory* et *LobbyControl* ont montré que les entreprises tech qui dépensaient étaient à l’origine de 49 millions d’euros de dépenses de lobbying auprès des institutions européennes pour les seuls Gafam^{(330)]}. À titre de comparaison, les dix entreprises qui ont dépensé le plus en lobbying dans la finance et de l’automobile n’atteignent que 42 millions. Ces montants ne cessent de croître, et devraient atteindre 100 millions en 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 intérêts auprès des institutions européennes qui leur offre un accès illimité au Parlement européen^{(331)]}.

NOMBRE DE LOBBYISTES DÉCLARÉS PAR LES GRANDES ENTREPRISES NUMÉRIQUES EXTRA-EUROPÉENNES

auditionné Meta plus de soixante fois afin de recueillir son avis sur la pertinence de cette législation et le contrôle des algorithmes. À ma connaissance, aucune association de logiciels libres n'a été conviée, pas que mes collègues ici présents disposent d'un lobbyiste à temps plein à Bruxelles. » M. Pierre Moyens entre un logiciel libre, qui n'a que peu de porte-parole, et un lobbying des éditeurs de logiciels : « nous jouons à armes totalement inégales » ^([334]).

Le lobbying des firmes états-uniennes s'exerce également auprès du gouvernement et des parlementaires. Leur a consacré la Haute autorité pour la transparence de la vie publique (HATVP), Google, Microsoft et Facebook entre 2020 et 2024, **533 fiches d'activités** témoignant des actions d'influence qu'elles ont entreprises auprès des autorités françaises ^([335]).

Ces initiatives visent, en majorité, à contrecarrer la régulation du secteur du numérique. Ils sont particulièrement actifs lors de la transposition du DSA et du DMA par la loi Sren de 2024, afin de dissocier des contraintes supplémentaires. Google, Microsoft, Amazon et Facebook ont sollicité directement l'Autorité de l'audiovisuelle et numérique (Arcom), l'Autorité de la concurrence ou l'Arcep. *Corporate Europe Observatory* note une intensification du lobbying en faveur du détricotage des réglementations européennes au tournant de la présidence de Trump ^([336]).

Les géants du numérique peuvent compter sur le soutien complet de l'administration fédérale américaine face au lobbying et aux menaces des États-Unis que M. Henri d'Agrain, attribue l'échec des négociations européennes 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 législations extraterritoriales. Le 25 mai 2023, les principales associations représentant les entreprises, notamment la Computer and Communications Industry Association (CCIA) et la Business Software Alliance, ont sollicité l'administration Biden pour exprimer leur opposition à ce dispositif européen, qu'elles considéraient comme une menace à la sécurité nationale américaine. En septembre 2023, le secrétaire d'État américain Antony Blinken a informé la Commission et aux chancelleries européennes, indiquant que l'adoption de l'EUCS en l'état pourrait nuire aux relations économiques et sécuritaires transatlantiques.

« À l'automne 2023, la Commission européenne décide alors de renvoyer le schéma à l'Agence européenne de la sécurité des données. Lorsqu'il réapparaît en mars 2024, il est expurgé de l'ensemble des critères d'immunité aux législations nationales. La Commission justifie cette décision par une analyse de son service juridique, soutenant qu'un schéma basé sur la Security Act ne pourrait contenir que des critères dits « techniques », c'est-à-dire technologiques.

« C'est ainsi qu'a émergé dans le CSA 2 une distinction artificielle entre risques techniques et risques systémiques du point de vue des utilisateurs, n'a aucun sens. Qu'un risque soit qualifié de technique ou non, cela ne change rien à l'intégrité ou la disponibilité des données et des traitements associés, il constitue un risque de sécurité.

« En Allemagne, cette évolution s'est traduite par un revirement politique rapide. Les associations allemandes, notamment pour l'industrie automobile très exposée au marché américain, ont pesé lourdement. Un communiqué trilatéral entre la France, l'Italie et l'Allemagne affirmait encore la volonté de travailler à une certification de sécurité intégrant des critères d'immunité extraterritoriale. Un mois plus tard, la position allemande a changé.

« À cela se sont ajoutées les réticences d'autres États, tels que les Pays-Bas, exprimant la volonté de rester alignés sur l'américain et aux garanties de sécurité américaines. Ce faisceau de pressions et de lobbying a finalement conduit à l'abandon d'immunité dans le schéma européen de certification. Telle est, en tout cas, l'analyse que j'en fais aujourd'hui. » ^([337])

Grâce à leur pénétration des cercles juridiques, les Big Tech sont également en mesure d'influencer la législation dans un sens qui leur est favorable. « Dans l'univers de la protection de la vie privée, le simple fait d'être présent dans les discussions est une victoire en soi. »

B. L'OMNIBUS NUMÉRIQUE : UN RECUL DE LA RÉGULATION EUROPÉENNE QUI DONNE S

La Commission européenne a présenté, le 19 novembre 2025, un paquet législatif visant à m et le règlement sur l'intelligence artificielle. Il s'inscrit dans l'agenda de simplification porté par la avec l'objectif revendiqué de supprimer les lourdeurs administratives qui entravent la croissance e sur le volet de l'intelligence artificielle étant déjà très avancées ^([340]), les travaux de la commis proposition de règlement dit omnibus numérique ^([341]), qui inclut notamment des modifications impo

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 p modifications ciblées du règlement (UE) 2016/679 à des fins de clarification et de simplification protection des données* », il ressort des travaux de la commission d'enquête que les amender simplification, remettant en cause l'équilibre même du RGPD. Selon M. Pierrick Clément, avocat p simplification, en tant que mécanisme juridique, consiste à faciliter l'application des normes p harmonisation des procédures ou une réduction des redondances. En revanche, redéfinir des conc aux garanties fondamentales ne relève pas de la simplification, mais bien d'un choix de dérégulation

Dans l'avis conjoint qu'ils ont adopté sur la proposition omnibus le 10 février 2026, le C protection des données ont souligné que « *certaines modifications proposées suscitent d'impor avoir une incidence négative sur le niveau de protection dont bénéficient les personnes, créer une i l'application de la législation en matière de protection des données* » ^([342]).

a. Une grave entaille à la définition des données personnelles

L'omnibus numérique vise à modifier la définition même des données à caractère p pseudonymisées. Alors que l'article 4, paragraphe 1, du RGPD dispose que toute information c identifiée ou identifiable constitue une donnée à caractère personnel, il est proposé d'ajouter le relatives à une personne physique ne sont pas nécessairement des données à caractère personne simple fait qu'une autre entité peut identifier cette personne physique. Les informations ne revêtent p donnée lorsque ladite entité ne peut identifier la personne physique à laquelle elles se rapportent, susceptibles d'être utilisés par cette entité. Ces informations ne se muent pas en informations à simple fait qu'un destinataire ultérieur éventuel dispose de moyens raisonnablement susceptibles p physique à laquelle les informations se rapportent. » ^([343])

La Commission européenne prétend qu'il s'agit d'une simple codification de l'arrêt S M. Yvo Volman, directeur des données à la direction générale des réseaux de communication, du cor 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 app Alors que la jurisprudence de la Cour avait jusqu'ici tendu à assimiler les données pseudonymisées a établi pour la première fois que des données pseudonymisées pouvaient être considérées comme no peut avoir accès aux informations identifiantes, ni transmettre les données à un tiers capable de le fa que « *des données pseudonymisées ne doivent pas être considérées comme constituant, en toute hypo à caractère personnel aux fins de l'application du règlement 2018/1725, dans la mesure où la pseuo de l'espèce, effectivement empêcher des personnes autres que le responsable du traitement d'identi que, pour elles, celle-ci n'est pas ou n'est plus identifiable* ». En l'espèce, le comité de régulation u Deloitte sous forme pseudonymisée, des commentaires communiqués par ses clients sur sa dernière

comme anonyme, et donc être exclue du champ du RGPD, s'il apparaît que celui qui la détient raisonnablement être utilisés » pour établir le lien entre les données et la personne. Par opportunité, la Commission propose d'ajouter à la définition de données personnelles, y compris des règles qui ne sont pas si simples, **les responsables de traitement de données risquent de traiter des données personnelles comme des données anonymes, donc de ne pas soumettre leur traitement au RGPD. Ils ne partagent pas leur appréciation. Surtout, ils priveront les utilisateurs des garanties nécessaires, y compris des tiers étrangers.** » ([348])

Dans leur avis conjoint, les autorités européennes de protection des données font également « invitent instamment les législateurs à ne pas adopter les modifications proposées à la définition de données personnelles qu'elles vont bien au-delà d'une modification ciblée ou technique du RGPD. En outre, elles vont bien au-delà de la jurisprudence de la CJUE, et elles aboutiraient à une réduction significative des garanties nécessaires aux personnes concernées » ([349]).

M. Julien Rossi confirme le **risque que l'exclusion des données pseudonymisées du champ du RGPD ne prenne pas en compte des situations pourtant sensibles** : « cette redéfinition pourrait conduire à ignorer des situations comportant ni le nom de la personne, ni son adresse, ni son numéro de téléphone, ni son adresse IP, ni son adresse e-mail, ni son exemple de données composées uniquement de points de géolocalisation horodatés. Si l'on sait que, dans un lieu donné, 90 % de ses horaires ouvrés dans un autre lieu donné, et une part significative de ses ventes le vendredi, dans un lieu de culte précis, il devient relativement aisé de reconstituer un fichier d'identification des personnes, ne s'agit formellement que de données pseudonymes, puisque le nom de la personne n'apparaît pas. Cela peut faire courir un risque réel, y compris physique, aux personnes concernées, notamment dans des contextes de surveillance, pour cette raison que certains collègues, en particulier Szilvia Lestyán, évoquent le phénomène d'« anonymisation », afin de souligner que des données présentées comme anonymes ou pseudonymes peuvent être liées aux personnes concernées. » ([350])

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** pouvant également soutenir l'innovation, dont le développement technologique et la diffusion des connaissances scientifiques existantes ou appliquent les connaissances existantes de manière à promouvoir l'accroissement des connaissances et du bien-être généraux de la société et respectent les normes éthiques et de protection des personnes concernées. Cela n'exclut pas que la recherche puisse également viser à promouvoir un intérêt commercial.

Cela aurait pour conséquence d'étendre les possibilités de déroger aux droits des personnes concernées. La recherche scientifique bénéficie en effet d'un certain nombre d'exceptions : elle peut justifier le traitement de données personnelles sans dispenser de l'obligation de fournir des informations quand les données personnelles n'ont pas été collectées à des fins de recherche et que cela exige des efforts disproportionnés ; elle permet de limiter le droit des personnes à accéder à leurs données personnelles, à y accéder, ou à en demander la rectification ou l'effacement.

L'omnibus tend également à **limiter le droit d'accès aux données personnelles, consacré par l'article 12, paragraphe 1** du règlement, en modifiant l'article 12, paragraphe 5 pour autoriser le responsable de traitement à refuser de donner accès à ses données personnelles, ou à exiger le paiement de frais raisonnables en contrepartie, lorsque la personne concernée ne peut pas accéder à ses données personnelles en vertu du présent règlement à des fins autres que la protection de ses données ». La charge de la preuve sera alors sur le responsable de traitement n'ayant plus à démontrer « le caractère manifestement infondé ou excessif de la demande d'accès » ou « 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 au responsable de traitement de refuser les demandes qui auraient des finalités économiques, politiques ou juridiques. Ces dernières sont pourtant des finalités légitimes, l'a expliqué M. Max Schrems : « Dans le monde du travail, par exemple, il arrive que des personnes demandent à accéder à leurs données personnelles pour se faire payer leurs heures supplémentaires ; elles invoquent le droit d'accès à leurs données. On entend monter la volonté que de telles requêtes ne puissent être faites qu'à des fins de protection des 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'article 6, paragraphe 1, point f) du RGPD. Le CEPD a confirmé, dans son avis du 17 décembre 2020, que l'article 6, paragraphe 1, point f) du RGPD pouvait bien être invoqué pour le traitement de données personnelles par des systèmes d'IA. L'avis du CEPD sur l'application de l'article 6, paragraphe 1, point f) du RGPD à l'IA souligne que 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 d'avance ;
- le traitement doit être nécessaire à l'entraînement du modèle, sans qu'il soit possible d'atteindre le même objectif 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 concernées, au cas par cas. Le responsable de traitement devra mettre en place des garanties limitant ces risques, telles que la pseudonymisation des données personnelles collectées, ou des dispositifs permettant aux personnes concernées d'exercer leurs droits d'accès ou d'effacement.

Or, l'omnibus ne fait aucune référence à cette triple exigence de proportionnalité. La séquence des considérations de l'omnibus sur les modèles d'IA paraît à cet égard bien trop large pour pouvoir constituer un intérêt légitime au sens de l'article 6, paragraphe 1, point f) du RGPD.

L'article 88 *quater* prévoit que le traitement des données personnelles par les systèmes d'IA doit être conforme aux principes de minimisation des données, la non-divulgaration des données conservées de façon résiduelle, et le droit d'accès, de rectification et d'effacement au traitement de leurs données personnelles.

Ces garanties ne sont cependant citées qu'à titre d'exemple et ne sont pas définies de façon exhaustive. L'omnibus **œuvre risque par ailleurs de se heurter aux difficultés techniques souvent invoquées par les personnes concernées pour ne pas donner suite aux demandes.** Afin d'être en mesure d'exercer leurs droits, les personnes concernées doivent être en mesure d'utiliser de leurs données personnelles et disposer d'un délai suffisant pour s'opposer au traitement de leurs données. Or, relève le CEPD ⁽³⁵⁷⁾. Or, en pratique, les informations de contact sont souvent manquantes et l'identification d'une personne relative à une personne est complexe ⁽³⁵⁸⁾. Les droits de rectification, d'effacement et d'opposition sont donc difficiles à exercer sur les systèmes d'IA sur une nouvelle base de données.

Les mesures prises pour limiter la divulgation ou la « régurgitation » des données personnelles par les systèmes d'IA ont été illustrées par M. Max Schrems : « Une de nos affaires en cours concerne par exemple un ressortissant de l'UE qui a été victime d'un attentat. L'OpenAI prétend qu'il a assassiné ses enfants, maltraité sa femme et commis toute une série d'actes de violence. Nous demandons à OpenAI de corriger ces informations produites par son algorithme, l'entreprise refuse de le faire. De nombreuses personnes témoignent de cas similaires. (...). Que des compagnies de la sorte puissent prétendre n'avoir aucun moyen de corriger ces erreurs ou de traiter le problème est affligeant. C'est pourquoi nous sommes dotés des principes qui figurent dans le RGPD. » ⁽³⁵⁹⁾

La reconnaissance explicite d'une présomption d'intérêt légitime pour les modèles d'IA n'est pas prévue par le RGPD. Selon l'association Noyb, cela revient à consacrer une sorte de « *présumé d'intérêt légitime* » autorisant les sociétés à déroger largement à l'obligation de recueillir un consentement libre et éclairé. L'avis du CEPD sur l'application de l'article 6, paragraphe 1, point f) du RGPD à l'IA souligne que la nécessité soit d'obtenir le consentement d'un nombre suffisant d'utilisateurs pour entraîner le modèle ou de permettre aux entreprises d'utiliser simplement les données de tout le monde tout en offrant une option de retrait (opt-out). **La proposition de la Commission tend à faire peser la charge de la gestion minutieuse des données personnelles des 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 à l'article 9 du RGPD ⁽³⁶⁰⁾. Cela recouvre notamment les données qui révèlent l'origine ethnique, les opinions politiques, religieuses, l'orientation sexuelle, des données biométriques, ou encore les données de santé. Ac

donné lieu à quarante-huit sanctions et à 953 millions d'euros d'amende. En tout cas, c'est une préo

La rapporteure relève qu'il en résulterait également une **perte de recettes significative pour d'amendes prononcées par la Cnil depuis 2020, 903 millions l'ont été à l'encontre de grandes France, et qui relèveraient donc des autorités luxembourgeoise, irlandaise ou néerlandaise si la**

L'omnibus prévoit, en outre, de larges exceptions à l'obligation de recueil du consentement pour accéder aux informations stockées dans les équipements terminaux. Il sera ainsi possible d'*agrégées sur l'utilisation d'un service en ligne afin de mesurer l'audience de ce service* », ou « *main* fourni par le responsable du traitement et demandé par la personne concernée ou l'équipement service ».

Pourtant, les traitements visant à mesurer l'audience sont loin d'être neutres, comme l'a *proposition omnibus semble considérer que ces pratiques auraient peu d'impact sur la vie privée* travaux montrent que certains de ces services collectent un volume considérable de données *gr* services qui suit, de fait, chaque clic de souris, chaque mouvement, chaque interaction sur internet *de données collectées est totalement disproportionné par rapport à la finalité affichée. Nous estim* posent un problème d'autant plus grave qu'elles sont fréquemment combinées et fusionnées *d* antérieurs, nous avons observé des techniques de fusion permettant de relier deux identifiants *dis* étudiés, 40 % recouraient à ce type de méthode. Le projet actuel affaiblit donc, selon nous, la protec CEPD partage ces inquiétudes et a recommandé de limiter le champ de l'exception à la colle d'évaluer la performance d'un site sans être directement reliées à des individus.

S'agissant de la dérogation dont bénéficierait l'accès aux données personnelles dans le termi Noyb de « *permettre des recherches étendues et massives dans les données stockées localement sur appareils similaires* ». Si aucune exigence de proportionnalité ne s'appliquait, il serait, par exemple analyse l'intégralité de l'ordinateur des joueurs pour s'assurer que ceux-ci n'ont pas installé de logici

Enfin, l'omnibus entend lutter contre la fatigue des cookies en exigeant que l'utilis **consentement au moyen d'un « bouton à simple clic ou par un moyen équivalent »**. Il est *d* navigateurs fournissent des **moyens techniques permettant aux personnes de donner ou d** **automatisée et lisible par machines.**

Si ces dispositions sont intéressantes et répondent à un réel besoin, elles soulèvent là encore que le mécanisme permettant de refuser les cookies en un seul clic ne suffira pas à protéger les uti non traitées par l'omnibus. **Quant au traitement automatique du consentement, il sera essentiel être renseignés avec la granularité nécessaire**, en distinguant les finalités de traitement, et en utilisateurs pourraient sinon être amenés à accepter par défaut l'ensemble des cookies pour ne pas s des sites web qui appliquent ce mécanisme. M. Thomas Dautieu, directeur de l'accompagnement ju « *Si vous dites non à tout, ça marche. Mais si vous souhaitez par exemple accepter les cookies seule les sites marchands, ça marche moins bien : c'est tout ou rien.* » ^([364]) La Cnil a engagé des discussi 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 au profit des grandes plateformes

Alors que l'omnibus numérique visait à simplifier le droit de la protection des données *d* pesant sur les petites entreprises et de favoriser l'innovation en Europe, il ressort des travaux modifications proposées risquent, au contraire, d'accroître la complexité juridique et de consolider extra-européens. La perplexité exprimée par M. Robin Berjon, informaticien et directeur de l'ag l'ensemble des personnes auditionnées : « *Pour ce qui est de l'omnibus, le texte est tellement mau*

Alors que l'objectif était d'assouplir l'obligation de fournir des informations, la dérogation aux sept critères, dont certains très vagues, qui pourraient faire l'objet d'interprétations divergentes. Le document de travail accompagnant la proposition, que cette « *simplification des exigences en matière de données pour les PME qui ne mènent pas d'activités de traitement à forte intensité de données ou à haut risque, telles que les boulangers, car elles seraient dispensées de l'obligation de rédiger des avis de confidentialité* ». Seules les PME puissent bénéficier de cet allègement, puisqu'elles n'en vérifieront pas les conditions : elles ont un hébergeur web, fournisseur de messagerie électronique, logiciels de comptabilité) et transmettent certaines données. Certains sont situés dans des pays tiers ^([366]).

De même, **l'omnibus risque de complexifier le cadre applicable aux traceurs.** Il est prévu dans l'omnibus permettant le traitement de données personnelles ; l'accès aux données non personnelles stockées dans le cadre de la directive e-privacy. Les représentants du Comité européen de la protection des données ont fait part de leur inquiétude qu'une telle scission compromette la bonne application des règles et la détermination de ce qui sera pas la même selon que les données sont personnelles ou non, ce qui pourrait être difficile à déterminer. De surcroît, l'effet incohérent de soumettre l'accès aux données personnelles à des conditions moins strictes que pour les données personnelles.

Le même constat s'impose pour le changement de définition des données personnelles. Cnil : « *De mon point de vue, ce serait tout sauf de la simplification : ce qui serait une donnée à caractère personnel pour l'un, pourrait être une donnée anonyme pour l'autre. Des données identiques prendraient ainsi un double visage. Les autorités devraient porter une appréciation sur leur capacité à identifier ou non les personnes derrière les données. Cette appréciation serait subjective : à partir de quel degré d'effort estime-t-on que l'identification n'est plus possible ? Plus, cette appréciation devrait évoluer avec les technologies.* » ^([367])

La démarche de la Commission européenne tendant à codifier les arrêts de la CJUE en matière de protection des données suscite également des interrogations. Comme l'ont fait observer les représentants de la Cour est juridiquement applicable sans qu'il soit nécessaire de l'inscrire explicitement dans le règlement. C'est fait l'objet de lignes directrices ou d'opinions du CEPD, que les autorités sont tenues d'appliquer. L'omnibus précise que les amendements proposés par l'omnibus. C'est notamment le cas de la définition de l'application du RGPD aux modèles d'IA ^([369]), de l'intérêt légitime ^([370]), ou encore de la pseudonymisation. Sur l'intérêt légitime pour traiter des données personnelles aux fins d'entraîner un modèle d'IA était prévu. La codification n'apporte à cet égard aucune clarification puisque c'est aux autorités ou aux juridictions nationales que l'exigence de proportionnalité est bien remplie.

Au-delà de l'omnibus numérique, **c'est toute l'approche par les risques sur laquelle repose la réglementation.** M. Max Schrems : « *En effet, ce que le législateur européen appelle « approche fondée sur l'analyse des risques », c'est en fait une approche par les risques. Elles sont ainsi comme des enfants dans un magasin de bonbons, où on leur dit combien de sucre il est souhaitable et raisonnable de consommer. De telles normes juridiques ne protègent personne. Les avocats les critiquent beaucoup car elles leur rendent difficile d'indiquer à leur clients le niveau de risque qu'ils acceptent. J'aime dire que ces lois numériques européennes sont comme les autoroutes allemandes, où chaque conducteur choisit son propre niveau de risque qu'il estime correct pour lui. Mais on pourrait choisir une autre approche, d'ailleurs, la majorité des pays européens, en limitant la vitesse – à 30 kilomètres à l'heure devant les écoles, et ainsi de suite. Ces limitations rendent le risque gérable, avec des lignes rouges claires.* » ^([372])

b. Un « énorme cadeau » aux Big Tech

La Commission européenne prétend que « *les PME et autres petits opérateurs bénéficieraient des modifications proposées.* » ^([373])

Cet argument est battu en brèche par M. Max Schrems : « On entend souvent que les lois numériques européennes sont comme les autoroutes allemandes, où chaque conducteur choisit son propre niveau de risque qu'il estime correct pour lui. Mais on pourrait choisir une autre approche, d'ailleurs, la majorité des pays européens, en limitant la vitesse – à 30 kilomètres à l'heure devant les écoles, et ainsi de suite. Ces limitations rendent le risque gérable, avec des lignes rouges claires. » ^([372])

monde bénéficiera de cette économie numérique fondée sur les données. Or nous savons, notamment comme Lina Khan, qu'**accroître la circulation des données favorise les grands acteurs et crée un** proposé aujourd'hui était adopté en l'état, ce serait un **énorme cadeau fait à Google et à Meta**, qui de données encore plus facilement. À l'inverse, les entreprises européennes ne pourraient plus tirer et aux données qu'elles collectent elles-mêmes pour leurs propres besoins. » ^([375]). **La proposition** l'**empreinte du lobbying des grandes plateformes extra-européennes**. Une étude conduite par (CEO) et Lobby Control ^([376]) révèle que **de nombreux amendements proposés par la Com** **demandes formulées par les Gafam**. Le tableau ci-dessous met en regard les propositions d'ar européenne ou à des États membres par ces entreprises ou leurs groupes d'intérêt et les modifications numériques.

COMPARAISON DES MODIFICATIONS AU RGPD PROPOSÉES PAR L'OMNIBUS NUMÉRIQUE AVEC LES CONT

	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 : « 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 : 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 b) refuser de donner suite à ces demandes. »	Google a proposé au gouvernement allemand l'amendement suivant : « 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 : 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 b) refuser de donner suite à ces demandes. » (2)
Utilisation des données personnelles pour entraîner des modèles d'IA	Ajouter un article 88 quater : « 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) Digital Europe a appelé la Commission à « renforcer 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)
	Ajouter un article 88 bis « Traitement des	Google : « La simplification la plus efficace consiste à supprimer l'article 5 (3) de la

- (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 confirmé qu'aucune étude d'impact n'avait été réalisée pour évaluer les conséquences des modifications. s'expliquerait notamment par le choix du véhicule législatif, un règlement omnibus, censé être des modifications de fond. Le calendrier a en outre été marqué par une certaine précipitation, liée à l'agenda de la Commission européenne à son agenda de simplification.

La consultation de l'appel à contributions diffusé par la Commission européenne le 16 septembre 2025 n'a pas prévu d'inclure le RGPD dans le paquet législatif sur la simplification numérique ⁽³⁷⁷⁾. En effet, la DG Consommateurs (DG Just) indiquait, dans son rapport annuel de 2025 sur la simplification, que le programme de travail de l'année 2026 serait notamment consacré à « l'identification d'éventuels amendements ».

Les amendements proposés au RGPD constituent donc « des ajouts de dernière minute », souligne M. Max Schrems ⁽³⁷⁸⁾.

Leur élaboration dénote un manifeste manque de préparation : sur les 200 pages de la proposition de législation ⁽³⁷⁹⁾, seules 10 concernent les modifications apportées au RGPD. La Commission ne fournit aucun élément précis pour appuyer l'idée selon laquelle ces amendements « renforceraient la compétitivité des nouvelles technologies », ou « apporteraient des avantages réglementaires directs grâce à une réduction des risques, ainsi qu'à un environnement plus propice à l'innovation et au développement durable ». « pas possible d'étayer ces affirmations par des chiffres précis ». De façon paradoxale, la Commission met en évidence que **96 % des organisations sondées ont estimé que les avantages liés aux innovations de la vie privée l'emportaient sur les coûts.**

La mauvaise qualité juridique de l'omnibus numérique traduirait également une précipitation chargée du sujet, selon M. Max Schrems : « le principal problème est que l'unité de la Commission dans ses propositions de directive ne dispose tout simplement pas du personnel et de l'expertise nécessaires pour partager pas forcément les options politiques de l'équipe précédente, en tant qu'avocat, force est de constater qu'elle n'est pas forcément compétente. L'équipe actuelle, elle, n'est pas forcément en mesure de produire des textes juridiques de qualité. eux-mêmes hésitent à souscrire à ses propositions, car ils ne voient pas bien comment elles pourraient être mises en œuvre ».

Aussi la rapporteure appelle-t-elle le gouvernement à s'opposer avec fermeté, au sein du Sénat, aux modifications du RGPD qui risqueraient d'affaiblir la protection des droits fondamentaux. Le Sénat a également adopté une proposition de résolution européenne en ce sens le 13 mai 2026. Les dispositions proposées par la Commission est à cet égard encourageant.

numérique. Or la dépense militaire américaine s'élève à 1 000 milliards de dollars, tandis que la n... Les ordres de grandeur, les masses financières et l'écosystème de financement aux États-Unis n'ont p...

M. Robin Berjon dresse le même constat ^([381]) : « En matière de dépendances structur... situation dans laquelle nous nous trouvons n'est pas le fruit du hasard. Elle ne résulte pas d'une q... des Américains, mais d'un choix politique fait au début des années 1990 et assumé depuis par toutes

« Au début des années 1990, les États-Unis se sont rendu compte que leurs investissements... justifiés, du fait de la fin de la guerre froide, et ont décidé de les réorienter vers le secteur de la tec... Valley. Ces investissements très significatifs, qui s'élèvent à plusieurs centaines de milliards, ont... visant à permettre aux sociétés informatiques de se développer sans entraves nationales ou interna... gouvernance de l'internet. »

M. Yann Lechelle souligne en particulier l'impact du Small Business Act ^([382]) : « En effet, [en réalité dès 1953] un protectionnisme intelligent à travers ce Small Business Act, qui a perm... acteurs locaux devenus ensuite des entreprises majeures. Par exemple, la Defense Advanced Res... massivement, par la commande et non par la subvention, des projets à l'origine de l'émergence de... bénéficié de budgets fédéraux considérables ».

Ainsi que l'indique la Small Business Administration ^([383]), l'agence fédérale américaine en... le gouvernement des États-Unis est le plus grand consommateur du monde et a l'obligation légale... moins 23 % des achats fédéraux chaque année.

La première source de financement des entreprise américaines, dans leur phase de dév... commande publique. Les montants consacrés sont considérables, ainsi que le décrit Mme Maya... marchés publics américains aux acteurs étrangers est de l'ordre de 30 %, tandis que celui des m... dynamique structurelle dans laquelle non seulement les États-Unis investissent plus d'argent dans... davantage. S'ajoutent à cela d'autres initiatives américaines, telles que le Buy American A... 94 milliards pour favoriser des acteurs américains, ou le Chips and Science Act, qui inclut... conducteurs et représente 50 milliards de dépenses directes – soit l'équivalent du plan France 2030... États-Unis dans le soutien public à la recherche et à l'industrie. »

Ce protectionnisme américain est également souligné par M. Yann Lechelle : « Les Ét... protectionnisme intelligent à travers ce Small Business Act, qui a permis de rediriger les flux public... des entreprises majeures. Par exemple, la Defense Advanced Research Projects Agency (Darpa) a j... non par la subvention, des projets à l'origine de l'émergence des hyperscalers, Google ayant pa... 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 déplo... marché de plus de trois cents millions de consommateurs.

Un marché unifié permet, d'une part, de générer rapidement des revenus importants. Com... commissaire européen au marché intérieur ^([385]) : « Les créateurs des Gafa se sont positionnés pour... grâce à l'interconnexion, à l'internet, apparue au début des années 2000. Et si ces géants sont a... n'est pas parce que nous sommes plus idiots que les autres, mais parce que, eux, ils avaient accès... unique. Les États-Unis, c'est un marché de 330 millions de consommateurs ; nous, on était vingt-se... tentatives de régulation – souvent orthogonales d'un pays européen à l'autre, d'ailleurs –, dix-huit l...

D'autre part, un marché unifié est synonyme d'économies d'échelle dans les investiss...

entreprises, celles que je connais et que je représente, il est indispensable d'aboutir enfin à ce marché » dont nous parlons depuis quinze ou vingt ans, sans jamais réellement le concrétiser. Il s'agit d'acteurs nationaux, mais d'identifier les grands opérateurs européens de cloud sur lesquels il conviendrait d'investir 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 capables de financer le développement d'entreprises qui « brûlent du cash » (*cash-burn*) pour financer une croissance et s'imposer face à la concurrence selon le principe du « *winner takes it all* ». C'est le fondement même du succès.

D'une part, l'épargne disponible est abondante et drainée vers le financement de la tech. « *Le capital-risque financé par des investissements considérables, dans un pays capable d'émettre autant de titres qu'il en faut, peut en créer lorsqu'il en manque* » ^([388]). Selon Cédric O, « *La puissance financière américaine vient du fait que Fidelity consacre seulement 1 % ou 2 % de ses actifs au capital-risque, ça représente des montants énormes* ».

D'autre part, les marchés financiers sont structurés pour ces opérations, et sont soutenus par des acteurs capables de mener à bien des financements de taille très importante.

M. Arnaud Caudoux ^([390]), directeur général adjoint de BPIFrance, explique de façon très précise comment les levées de fonds reposent sur des mécanismes croisés d'échanges de titres entre entreprises et investisseurs qui s'autoalimentent : « *C'est le premier élément de différence entre les États-Unis et l'Europe aujourd'hui. C'est la capacité à lever du capital-risque. Cette taille vient de deux choses : la disponibilité des capitaux à s'investir dans le capital-risque, et la capacité des investisseurs américains et les endowments des universités, que nous n'avons pas à la même échelle en Europe à vendre les entreprises.* »

« *Effectivement, les fonds américains ont une capacité à vendre les entreprises à de très grandes entreprises européennes, ce qui est une vertu importante que notre capacité à vendre nos entreprises à de grandes entreprises européennes ne possède pas. C'est vertueux d'un côté et vicieux de l'autre. Est-ce à cause des dividendes ? Il me semble que c'est d'abord à cause de la capacité à lever du capital-risque. Beaucoup de ces rachats se font en titres, et donc avoir une valorisation très importante permet de lever des fonds sur une valeur importante en échangeant des actions. La question clé numéro un, c'est la valeur d'une entreprise, la capacité à prendre du risque, et la capacité du marché actions à évaluer l'opportunité de ces acquisitions. Il y a une capacité à lever des fonds pour acheter des actions pour juger de la bonne valeur d'une entreprise et de l'opportunité de l'achat d'une start-up. Ce phénomène est relevé par M. Arthur Mensch : « Les start-up vendent, dans un premier temps, aux investisseurs américains, dans sa version venture capitalist, fonctionne de façon circulaire – puis aux autres entreprises européennes qui rachètent rapidement. Une fois qu'elles sont ainsi passées à l'échelle, elles exportent vers l'Europe, et rachètent les quelques boîtes qui ont développé des compétences, ce qui leur permet de se consolider sur le marché ».* »

Mme Maya Noël décrit elle aussi la nécessité de disposer d'acteurs couvrant toutes les étapes du cycle de vie d'une entreprise dans notre modèle économique, les acteurs qui financent les fonds d'investissement en capital-risque ont besoin d'acteurs capables de leur faire sortir leur argent – dans les dix ans. Il faut donc que quelqu'un d'autre, disposant d'un capital-risque, prenne le relais pour accompagner la poursuite de la croissance de l'entreprise. Or nous ne disposons pas d'acteurs privés du financement capables de prendre le relais. Les acteurs américains sont les seuls capables de lever l'investissement ». L'écosystème de la tech américaine est désormais très complet : un soutien de la commande publique, un marché largement unifié sur lequel les entreprises peuvent se déployer rapidement, la capacité de prendre des risques pour financer des entreprises innovantes, les succès passés contribuant à créer un environnement très favorable.

B. LA COMMANDE PUBLIQUE : UN INSTRUMENT ENCORE MAL MOBILISÉ

Le seul cadre dans lequel une préférence européenne est généralisée est celui des marchés publics, dans lesquels la logique est inversée. Le recours à des prestataires européens est le principe, l'exclusion l'exception. L'article L. 2353-1 du code de la commande publique dispose ainsi que « *les marchés publics sont exemptés de l'accord sur les marchés ou d'un autre accord international équivalent auquel l'Union européenne est partie, des opérateurs économiques d'États membres de l'Union européenne. L'acheteur peut toutefois exclure des opérateurs économiques d'un pays tiers à l'Union européenne à participer à une procédure de passation. La décision d'exclusion tient compte des impératifs de sécurité de l'information et d'approvisionnement, la préservation des intérêts économiques, l'intérêt de développer la base industrielle et technologique de défense européenne, les objectifs de coopération d'avantages mutuels et les exigences de réciprocité.* »

Dans certains cas, des critères objectifs peuvent être mobilisés pour justifier le recours à des prestataires non-européens. L'éducation nationale souligne que « *des clauses d'immunité au droit non-européen à portée extraterritoriale ont été introduites dans des marchés récents de services à hébergement externalisé, sans contestation devant le juge administratif. L'existence du cadre de protection des données à caractère personnel (Data Privacy Framework) en vigueur le 10 juillet 2023 et qui, contrairement aux deux accords précédents (Safe Harbor et Privacy Shield), est reconnue par la justice de l'Union européenne (arrêts Schrems), rend juridiquement délicate l'exclusion d'un prestataire en raison d'incompatibilité au RGPD. L'article 31 de la loi SREN vient certes sécuriser le recours à des services cloud de SecNumCloud pour les SI traitant de données "d'une sensibilité particulière", mais il est limité à des marchés à 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, un véritable tremplin pour elles. Ainsi que l'ont montré les chiffres de Numeum, le tissu économique des fournisseurs est composé de peu de grandes entreprises. La participation des PME et de ETI aux achats publics devrait donc être encouragée pour 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 l'Observatoire des relations entre start-ups et grands comptes, contient des indications chiffrées sur l'évolution des achats des administrations et des grands groupes auprès des start-ups.

Au rang des satisfactions, les achats publics auprès des start-up ont fortement augmenté, passant de 1,7 à 2,3 milliards d'euros. Ce montant est désormais comparable à celui des achats passés par les 39 entreprises du périmètre de la direction des achats de l'État, la hausse est de près de 50 %. On note donc un effort significatif.

ÉVOLUTION DES ACHATS AUPRÈS DES START-UP ENTRE 2022 ET 2023

	2022	2023	Pro
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'il est faible : 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, 20 % comptent pour moins de 20 % de leur activité pour 73 % d'entre elles. Parmi les administrations, les collectivités territoriales qui sont les plus actives, avec 44 % des acheteurs. Les ministères ne comptent que pour 12 % ;
- pour les contrats signés avec des administrations, la part des contrats de moins de 5 000 € est de 60 % ;

techniquement. Elles sont en effet dotées d'une forte agilité, c'est-à-dire d'une capacité de prise de décision de manière extrêmement rapide, ainsi que d'une forte ingénierie en recherche et développement, ce qui les différencie ainsi de beaucoup d'acteurs majeurs du marché. »

La commande publique pourrait donc davantage recourir à des entreprises innovantes, puisées dans la base de données 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'innovation, via des subventions. La commande publique vise quant à elle à répondre aux besoins de la puissance publique. 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 moyenne pour mener des projets de grande ampleur et donner des garanties de stabilité sur le long terme. Les financements publics jouent ce rôle : contribuer à solvabiliser les entreprises dont la technologie est jugée très prometteuse, de leur permettre de faire de 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 l'Armement, à travers la direction générale des entreprises (DGE) pour préparer le tissu industriel en amont. Le ministère de l'Armement échange avec la DGE sur les besoins clés et les entreprises présentant les plus avancées technologiques, et contribue éventuellement aux financements via des prises de participation ou d'autres moyens, notamment via des contrats-cadres ⁽⁴⁰¹⁾. *« Dans le domaine du numérique, comme dans tous les autres domaines écologiques, le ministère des armées entretient des échanges réguliers avec la Direction générale des entreprises. Parmi les organismes publics impliqués dans la politique industrielle, les relations avec les entreprises et le tissu industriel sont très importantes. Ces échanges, assurés notamment par la direction de l'industrie de défense de la Direction générale des entreprises, permettent d'entretenir la vision du paysage industriel français, à optimiser les dispositifs de soutien industriel sur le long terme, à renforcer la performance et la résilience des filières critiques. Par ailleurs, ces échanges contribuent à la commande publique et à la juste utilisation des moyens de l'Etat, tout en tenant compte des spécificités des besoins de la défense, comme des autres acteurs étatiques de la souveraineté.*

« Afin de structurer sa relation avec la base de ses fournisseurs actuels et potentiels (entreprises de la défense et numérique (CND) s'appuie sur les fédérations et organisations professionnelles et associatives (GIFAS10, GICAN11, Hexatrust, Collège Défense et Numérique), ainsi que sur les pôles de compétences (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 et les startups innovantes, de mieux connaître l'organisation et les besoins du numérique de défense ainsi que les capacités de l'Etat, et, le cas échéant, de se regrouper pour y répondre. À cet effet, le CND organise des webinaires de sensibilisation au profit de ces entreprises, ainsi qu'un évènement annuel, le Séminaire du numérique de défense, qui rassemble 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 Direction nationale du numérique (DNUM) du ministère de l'Europe et des Affaires étrangères (MEAE) et la DGE sont actuellement très fortes. Une interaction a eu lieu en novembre 2025 dans le cadre de la mission sur l'évolution des capacités d'innovation de la DGE.*

« Lors de cet échange, le MEAE a souligné la criticité de ses infrastructures, notamment en matière de cybersécurité, de délégataire de service pour le classifié à l'étranger par l'OSIIC, et dans un contexte de diffusion restreinte de l'information interne. Nous avons également rappelé que, malgré la taille relativement modeste de nos locaux technologiques, nous sommes comme un opérateur critique pour l'État. Nous avons mis en garde contre une mutualisation qui pourrait nuire aux systèmes d'information mis à disposition sur l'ensemble de nos emprises à l'étranger et du niveau de la sécurité nationale. »

généralement fondé sur un abonnement annuel. Or, avec 900 000 professeurs, les chiffres ont tendu

Enfin, la question s'est posée, de manière assez vive, pour les projets faisant l'objet d'un plus emblématique est celui des suites collaboratives.

En 2023, trois lauréats sont sélectionnés pour le développement de suites collaboratives « Développement de suites bureautiques ». L'objectif est ainsi de se positionner comme des alternatives à Office 365 et Google Workspace. Le montant total des aides attribuées aux trois consortiums s'élève à 1,5 million de euros, dont un tiers de subventions et un tiers d'avances remboursables. À ce jour, le taux de décaissement est de 76 %, ce qui représente 1,1 million de euros des trois projets. Ainsi que l'indique BPIFrance ⁽⁴⁰³⁾, « globalement, l'avancement technique est satisfaisant, les 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 et celles développées par la Dinum a inévitablement été évoquée lors des différentes auditions de la commission d'enquête parlementaire sur la souveraineté numérique chez les acteurs de la filière. M. Alain Garnier, président de Jamespot, résume le point de vue des acteurs des alternatives souveraines aux produits collaboratifs de Microsoft ⁽⁴⁰⁴⁾ : « Je ne peux passer sous silence la véritable politique industrielle en lançant un appel à projets France 2030, bien doté, pour les suites collaboratives. Trois ont été désignés : Wimi, Jamespot et Interstis. Cependant, alors que cette politique industrielle était très ambitieuse, elle a fait de cap en développant une offre étatique unifiée, nommée LaSuite. Cette initiative a entraîné une réelle perte de visibilité sur l'articulation des offres et d'importantes frictions, qui n'ont été que des ajustements ministériels successifs. Pourquoi passer d'un modèle de soutien à un écosystème de filière, qui a fait de la France 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 le développement de solutions à de grandes échelles ;
- d'autre part, ils reprochent à cette dernière de capter une partie du marché que les éditeurs souhaitent croître leur offre : « L'enjeu n'est pas de chasser Microsoft de France ou d'Europe, mais de rééquilibrer le marché des outils collaboratifs, mais aussi dans d'autres domaines, par exemple la gestion de l'identité ou les services de cloud. 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 la stratégie de M. Henri Verdier, initiateur de cette stratégie lorsqu'il dirigeait la Dinsic. « Mon objectif était de réinventer les méthodes agiles, des politiques publiques fondées sur la donnée (data-driven policies), le développement de ressources humaines capables d'attirer une plus grande diversité culturelle et des profils rares et les maintiens – que lorsqu'une organisation ne sait plus produire elle-même, elle ne sait plus acheter. Les factures vingt fois trop chères, simplement parce que les achats avaient été réalisés à l'aveugle (sans stratégie). Lui-même. À un moment donné, la faiblesse insigne de l'État constitue en elle-même un problème. » (405)

M. Henri Verdier signale également l'écart de coût entre les solutions que l'État est capable de développer et les solutions commerciales des acteurs privés : « L'État n'a pas vocation à se substituer au secteur privé et il n'est pas, par exemple, un opérateur de cloud. En revanche, dans certaines situations, il faut être capable de faire des choses que le secteur privé ne peut pas faire, comme la messagerie instantanée Tchao, que j'ai contribué à lancer. Ce service, réservé aux fonctionnaires, est financé par agent public. Il compte 400 000 utilisateurs hebdomadaires sur un potentiel de deux millions de utilisateurs d'une messagerie. On peut considérer qu'il s'agit d'un succès raisonnable. À l'époque où je dirigeais la Dinsic, c'était 20 euros par an et par agent public. Face à un tel écart, il me paraît légitime que l'État envisage, 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 l'économie du pays en soutenant les entreprises françaises – je parle en connaissance de cause pour avoir vu les aider à réussir dans la compétition internationale, non les placer dans une situation protégée, à

« S'agissant des outils de la DINUM, même si des progrès sont évidemment possibles sur la qualité de différents produits est de bonne qualité, et répond à un vrai besoin, tout en assurant un très bon interministériel de l'État, FranceConnect pour l'authentification des usagers sur les services en ligne simplifiés, Sur d'autres produits plus émergents, la couverture des besoins et le niveau de qualité sont bien compris que c'est normal, car en appliquant des méthodes de type « lean start-up » la DINUM fait de la recherche d'impact et d'adhésion des utilisateurs en remettant l'industrialisation et la complétude à l'avenir. Un des intérêts principaux des logiciels interministériels est la capacité pour les services ministériels, ce qui permet une économie globale à l'échelle de l'État mais repose sur la fiabilité et la confiance qu'elle peut donner. ».

Aux dires des éditeurs de logiciels indépendants, le déploiement des outils de la Dinum aura un impact positif. Il ne faut tout de même pas occulter le fait que les financements publics alloués aux trois consortiums s'élèvent à 11,7 millions de subventions. Le président de Jamespot a indiqué que sa société tirait 40 % de ses revenus de ces acteurs tels que la Cnam.

Le soutien à des projets et des entreprises innovantes comporte une part de risques, et il convient de sélectionner les projets qui auront été financés. L'attribution de subventions à des acteurs émergents ne doit pas être guidée par les besoins des administrations devant primer.

La rapporteure constate que l'État soutient de manière volontariste et pour des sommes importantes. Elle souligne la nécessité dès lors d'une politique ouvrant davantage le marché de la commande publique à l'ensemble des solutions bénéficiant d'aides publiques. En effet, la commande publique ne représente qu'une partie 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 D'ÉCHEC

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, rendait public son rapport sur le futur de la compétitivité de l'Europe ⁽⁴⁰⁸⁾. Ce rapport pointait du doigt deux freins essentiels : le manque de capitaux à l'échelle européenne et la part insuffisante des fonds de pension, représentant seulement 10 % des actifs, contre 30 % aux États-Unis. Cette situation conduisait à faire reposer le financement de l'innovation majoritairement sur des actifs risqués et contraints par les règles prudentielles.

De façon convergente, les représentants des institutions publiques chargées du financement de la recherche à financer des opérations pour la phase dite de *scale-up*, c'est-à-dire celle durant laquelle les besoins dépassent les 10 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 est bien documenté, dont les causes sont multiples. Pour y remédier, nous sommes convaincus de la nécessité d'un front sur la mobilisation prudentielle des capitaux et sur l'orientation des investissements privés. L'initiative Tibi a déjà produit d'excellents résultats et nous entrons désormais dans une phase d'accompagnement. Le lancement d'un fonds par la Commission. En France, si l'amorçage et le stade A sont relativement faciles, les difficultés apparaissent lors des phases de croissance, aux stades B et C. C'est précisément sur ce stade que car cette faille de marché influence directement les choix stratégiques des entreprises, et singulièrement

Pour M. Benjamin Delozier, chef du service des politiques écologiques et sectorielles à la direction générale de le financement, je partage le constat selon lequel les principales difficultés de nos start-up technologiques se concentrent sur le late stage, malgré le dynamisme de notre écosystème entrepreneurial. Pour y remédier, Tibi, coordonnée par la direction générale du Trésor depuis 2020, mobilise l'épargne des investisseurs

LISTE DES INTRODUCTIONS EN BOURSE (IPO) RÉALISÉES SUR EURONEXT PARIS DEPUIS LE 1^{ER} JANVIER 2020

CLOUD

Société	Activité de l'entreprise	Date	Capitalisation boursière (M€)	Montant de l'opération (M€)
Lighton	Développement de logiciels et de modèles d'intelligence artificielle générative	Novembre 2024	62	
Planisware	Fourniture de solutions SaaS pour le management de projet	Avril 2024	1 100	
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	
OVH	Fournisseur de services cloud	Octobre 2021	3 488	
Exclusive networks	Solutions de cybersécurité et de cloud	Septembre 2021	1 830	
Spartoo	Plateforme de vente en ligne d'habillement	Juillet 2021	119	
AMA corporation	Plateforme vidéo, photo et audio pour travailleurs en mobilité	Juillet 2021	146	
namR	Plateforme de données sur les infrastructures et les bâtiments	Juin 2021	38	
Obiz	Plateformes web pour le marketing	Mai 2021	31	
Alchimie	Plateforme de streaming de vidéos à la demande par abonnement	Novembre 2020	71	
Energisme	Plateforme SaaS pour la gestion des consommations d'énergie	Juillet 2020	28	
Nacon	Jeux vidéo	Mars 2020	458	
Munic	Acquisition et traitement de données des véhicules automobiles	Février 2020	61	

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 France et en Europe. La revente à des investisseurs étrangers et la cotation sur un indice américain sont devenues des étapes incontournables pour toute entreprise de la tech qui réussit.

L'exemple le plus emblématique en est le changement de domiciliation de Criteo pour l'octobre 2025. Criteo réalise aujourd'hui 1,8 milliard d'euros de chiffre d'affaires, soit à elle seule 8 % du chiffre d'affaires du secteur de la publicité en France, selon le recensement réalisé par Numeum. Ainsi que l'explique la société, la domiciliation au Luxembourg est une étape clé pour Criteo, car elle lui permet de préparer le futur d'organiser un transfert vers les États-Unis, et ainsi d'accéder à des financements très importants. *La domiciliation au Luxembourg est une étape clé dans le parcours de Criteo visant à tirer pleinement parti des avantages de notre introduction en bourse. Cette décision stratégique initialement prise par nos fondateurs afin de soutenir la croissance à long terme de Criteo est devenue une réalité. Aujourd'hui, devenue une société cotée en bourse, le passage du marché boursier américain a considérablement*

minoritaire aux côtés de fonds étrangers, souvent américains. Dans ce cadre, elle joue un rôle d'équilibre entre les fondateurs ou les dirigeants de la société et ces actionnaires majoritaires. Elle négocie une 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* » rapporteure : « *Nous avons avec nous quelques sociétés de VC (venture capital), qui représenteraient ce que nous aurions été ravis de prendre des Européens, mais il n'y en avait pas ! On y perd sur le plan économique sur investissement dans Mistral reparti aux États-Unis, par le biais des fonds américains. Quant à la présence partielle en Europe, car les Américains lèvent dans le monde entier. Donc on perd du retour, pas de dommage mais c'est comme ça* ».

M. Charles-Antoine Beyney, directeur général de DataOne donne à la commission une réponse au rachat ⁽⁴¹¹⁾ : « *Quelle garantie puis-je apporter que le projet restera 100 % français ? Je vais répondre que non. Parce que BSO n'est pas une association à but non lucratif. Pour le dire très clairement, si nous n'avons pas de refinancement ou un schéma d'investissement fort en Europe, les États-Uniens continueront à nous acheter pendant cinquante ans. Si j'ai vendu à Equinix, c'est parce que cette société m'a présenté la meilleure offre financière, aussi parce que la meilleure offre était américaine* ».

Dans les imaginaires et les motivations profondes des entrepreneurs de la tech, le développement 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 cannibaliser les concurrents, pour devenir une « licorne » ou une « décacorne », voire une « pédocorne » et 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 transition énergétique et numérique, chargée de l'intelligence artificielle et du numérique présentait devant la commission la politique constante lancée depuis désormais plus de quinze ans, qui conduisait à faire de la France un terreau de création de start-up.

« *Collectivement, (...) nous ne sommes pas restés les bras croisés face à ces dépendances technologiques. Les travaux de mes prédécesseurs. De longue date, le combat est mené pour soutenir le développement de la France. Dès 2010 fut lancé le premier programme d'investissements d'avenir. En 2013 ont été créées BPIFrance et France 2030. BPIFrance connaît une forte accélération depuis 2017, avec des stratégies sectorielles ambitieuses : la Stratégie nationale pour l'intelligence artificielle en 2018, à la suite du rapport Villani, la stratégie nationale pour le cloud en 2021, pour la stratégie nationale quantique lancée par le Président de la République en 2021 et, bien sûr, le plan France 2030 de 54 milliards d'euros d'argent public* ». (...).

« *En parallèle, notre fiscalité encourage l'entrepreneuriat et l'innovation avec le crédit d'impôt pour le soutien à la recherche et développement et d'attractivité du pays, ainsi qu'avec des dispositifs spécifiques pour la jeune entreprise innovante (JEI), cher à votre collègue Paul Midy, dont je salue l'engagement auprès de la France* ».

« *La France est le leader européen en matière d'innovations de rupture, avec des pépites dans l'intelligence artificielle ou les biotech. C'est le résultat d'un effort de long terme, qu'il convient de maintenir* ».

En France, le continuum de financement de l'innovation apparaît relativement bien structuré, de la recherche et à la maturation technologique, les fonds d'amorçage et de capital-risque *early-stage* aidés par des acteurs non financiers (incubation, accélération, mise en réseau). Ce continuum est particulièrement visible grâce aux dispositifs publics permettant de réduire le risque scientifique et technologique via l'attribution de subventions et d'investissements en fonds propres. **L'aide aux entreprises du numérique se déploie à travers France Numérique** pour le compte de l'État. BPIFrance chiffre les aides à l'innovation dans le domaine du numérique (hors « santé numérique ») à 1,1 milliard d'euros en 2025, dont 470 millions d'aides régionales et 630 millions d'aides nationales.

Genesis	Genesis développe des modèles d'IA appliqués à la robotique et autonomes, notamment en s'appuyant sur un moteur de simulation. La technologie vise à doter les machines de capacités de raisonnement et d'interaction avec le monde réel.
Altrove	Altrove conçoit des modèles d'IA et développe des capacités de synthèse vocale pour identifier des nouveaux matériaux et réduire leur cycle de développement. La société vise à développer des matériaux alternatifs à des matériaux actuels 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 d'informations à grande échelle, à destination de clients privés et publics (en particulier régaliens et militaires) dans le domaine de l'investigation, de la recherche et l'analyse de grandes quantités de données, de la cybersécurité, de la gestion de crise, de l'open source intelligence (« 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 acteurs majeurs nationaux dans le domaine du logiciel.
Doctolib	Doctolib développe des logiciels à destination des professions médicales pour faciliter la prise de rendez-vous des patients afin d'optimiser la prise de rendez-vous et la gestion des informations des patients.
CHR Groupe	CHR Groupe édite des solutions SaaS pour les professionnels de la restauration, notamment les métiers de bouche. Le groupe opère principalement via ePack Hygiène (gestion de la traçabilité sanitaire) et Adoria (gestion des achats, stocks et pilotage multi-sites).
Ciril Group	Ciril Group édite plusieurs logiciels utilisés par les collectivités territoriales pour la gestion des déchets.
Septeo	Septeo développe des logiciels à destination de plusieurs secteurs, notamment les professions réglementées telles que les avocats ou les notaires. Les produits 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. de diagnostic) : informatisés, gestion administrative des patients, imagerie, biologie, etc. Elle est à la fois éditeur, intégrateur et hébergeur de données de santé. Elle mène un développement produit innovant, permettant une efficacité accrue de la prise de décision, une intégration et interopérabilité des outils, une sécurité renforcée pour les données sensibles, autour d'un hébergement dans des infrastructures certifiées HDS.
Cybersécurité	
Sekoia	Plateforme étendue de détection et de réponse aux cyberattaques de dernière génération, auto-apprenante, s'interfaçant avec toutes les solutions de cybersécurité existantes pour une détection de tous types de menaces dont les signaux faibles.
Yes We Hack	Leader européen des plateformes de <i>bug bounty</i> mettant en relation des entreprises avec des hackers éthiques afin d'identifier des failles dans les systèmes d'information et 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 1,2 milliard 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 à fort potentiel de leur financement. Une accélération du financement est en cours dans le domaine de l'intelligence artificielle. *« dans le cadre de son plan stratégique 2026-2030, Bpifrance prévoit de déployer 10 Md€ pour soutenir l'IA : des infrastructures aux applications, en passant par les modèles de fondation responsables »*. *« L'objectif est de créer l'écosystème de financement de l'innovation en IA à tous les niveaux : en accompagnant les fonds d'investissement et leurs investissements vers l'IA, en favorisant l'émergence de fonds sectoriels couvrant toute la chaîne de valeur, en créant des fonds européens et mondiaux qui affichent un fort intérêt pour le marché français. L'objectif est également de créer des fonds partenaires. Bpifrance soutiendra également le développement de projets stratégiques en fondant des fonds de capital-risque, des modèles de fondation, tout en investissant dans les infrastructures clés de l'IA : semi-conducteurs, cloud, données, applicatives et composants spécialisés »* ⁽⁴¹⁴⁾. Le financement public joue également un rôle important dans lequel l'État investit. Ces sociétés peuvent également bénéficier du soutien de l'appareil d'État à travers la diplomatie économique (visites d'État dans d'autres pays, sommet Choose France, etc.). La question des participations demandées par l'État actionnaire lorsqu'il prend des participations dans le numérique.

remboursement de leurs créances. *Votre rapporteure considère que cette séquence engage la res*
successifs et appelle une évolution de la doctrine d'intervention de l'État dans un con
géopolitiques. » ([417])

Deux exemples peuvent ainsi être donnés dans le portefeuille de BPIFrance de l'insuffisance

– Mistral AI : cette entreprise est désormais placée au centre de la stratégie de déploiement
elle est décrite comme la seule véritable alternative aux géants américains et chinois dans le dom
développe des outils critiques pour les administrations. Pourtant, l'État n'a assorti sa prise de particip

– Chaps Vision : cette société a été choisie tout récemment par l'État comme alternative à Pa
si l'actionnaire majoritaire cède ses parts, BPIFrance ne dispose d'un droit de veto que pour les
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 fragilis
industrielle. L'effort de l'État pour soutenir les entreprises innovantes est à signaler, que ce soit dire
indirectement à travers l'appui à la constitution de fonds de financement. Mais quelles sont les c
développée sur des fonds publics ou grâce à des commandes publiques, ou a tout simplement bénéf
aux délégations présidentielles, appui dans les instructions administratives, etc.), décide de s'expatrie

Enfin, le soutien aux entreprises innovantes, que ce soit via des subventions ou des pri
d'orienter les choix techniques des sociétés soutenues, de façon à favoriser la diffusion des te
interopérables.

**Recommandation n° 11 : Flécher une partie des fonds France 2030 et du dispositif French 120 à destin
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 c
géants de la tech n'ont jamais été aussi puissants, l'Europe et la France ne semblent pas prendre la
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
actes de l'Union européenne. Le constat est désormais partagé, mais aucune initiative ne témoigne d'

Les politiques de soutien à l'innovation menées par l'Union européenne sont insuffisan
financièrement dans leurs investissements par le pacte de stabilité et de croissance et sont égale
réglementation sur les aides d'État. Les financements européens ne prennent pas le relais des aides
Draghi, « *le soutien de l'UE aux investissements publics et privés est limité par la taille du budget*
ainsi que par une attitude trop prudente à l'égard des risques. Le budget annuel de l'UE est peu éle
de 1 % du PIB de l'Union, tandis que les budgets des États membres en représentent collectivement

S'agissant de la mise en œuvre d'une préférence nationale dans les achats publics, la Com
d'un texte sur les achats publics au second semestre 2026. La référence à une préférence européenne
sont encore incertains : « *Dans ses orientations politiques, la présidente de la Commission, Ursula v*
législation relative aux marchés publics. Elle a souligné que cette révision « permettra de privilégie
publics de certains secteurs stratégiques ». Lors de son discours sur l'État de l'Union de 2025, l
promis d'« *introduire un critère « made in Europe » dans les marchés publics* ». ([418])

Il reste cependant une incertitude sur ce que recouvrira ce critère « *made in Europe* ».

« Des alliances européennes sont possibles, notamment autour d'un dispositif équivalent à Small Business Act européen existe théoriquement, mais il n'est pas fonctionnel. » ([419])

En conclusion, le modèle de financement des entreprises est un levier fort de différenciation. Un constat qui a été établi maintes fois, les lignes de la réglementation européenne bougent à un rythme qui nous oblige à nous interroger : pourquoi ? Expliquer que nous soyons encore la seule région du monde à nous appliquer à nous-mêmes des règles de 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 de créer des licornes. Cette politique souffre de deux défauts : d'une part, l'ambition de copier le modèle américain comporte des défauts. Ainsi, au prétexte de créer de nouveaux géants européens, il faudrait affaiblir la réglementation. Les prises de participation ne s'accompagnent pas de contreparties suffisantes, ce qui laisse grandes ouvertes des portes désormais stratégiques à des investisseurs extra-européens.

– 1 –

CHAPITRE 11 – LE DÉPLOIEMENT DE L'IA : LE RISQUE D'UNE PERTE DÉFINITIVE DE TOUTE

A. LES CONSÉQUENCES ÉCONOMIQUES

Comme le soulignait M. Arthur Mensch devant la commission d'enquête, « la situation est préoccupante. L'intelligence artificielle, il y a des destructions d'emplois – en tout cas, des modifications très rapides. Il y a ensuite des conflits d'usage de l'électricité – tout le monde en veut, mais il n'y en a pas assez. Une explosion du déficit commercial qui, dans le domaine des services, sera multiplié par cinq dans les prochaines années, comme celle-ci est révolutionnaire. Il faut la prendre en compte, en parler davantage et avoir un point de vue clair. Cela implique pour l'économie, pour la société et pour les équilibres géopolitiques. Si on ne le fait pas, on risque de prendre de mauvaises décisions – une situation que l'on ne voudrait pas voir advenir. » ([420])

En créant cette commission d'enquête, l'Assemblée nationale montrait que ce sujet était une priorité de la représentation nationale. Il était clair que l'examen des conséquences économiques de la dépendance à l'IA trouvait son prolongement logique dans la réflexion sur les conséquences économiques de nouvelles technologies, de l'intelligence artificielle générative. La rapporteure a souhaité réaliser cet examen selon une approche la plus globale possible. Les questions doivent ainsi être traitées :

– Quelles sont les perspectives réelles de l'intelligence artificielle ? Assistes-t-on réellement à une révolution de l'économie, ou bien à un changement du même type que ceux connus par le passé (bulle internet des années 2000) ?

– Que montrent les premiers travaux économiques sur les conséquences de l'IA sur l'emploi ?

1. Révolution ou évolution ? Bulle ou pas bulle ?

Il est impossible de répondre avec certitude à la question sur la magnitude de la transformation induite par l'IA sur l'économie mondiale. Une question dérivée de celle-ci est l'adéquation des valorisations des entreprises à leurs revenus futurs qu'elles généreront. En d'autres termes, existe-t-il une bulle sur l'intelligence artificielle ?



L'entreprise Anthropic a ainsi vu son chiffre d'affaires dépasser les 45 milliards de dollars et OpenAI a réalisé un chiffre d'affaires de 40,4 milliards d'euros en 2025. Anthropic a ainsi levé 65 millions de dollars lors de son opération de valorisation la société à 965 millions de dollars ([423]).

Dans son rapport sur la stabilité financière mondiale, datant d'avril 2026, le Fonds monétaire international (FMI) considère que les investissements des *hyperscalers*, bien que très importants, s'appuient sur des revenus. « Pour les principaux hyperscalers, la croissance des bénéfices a suivi le rythme de la trésorerie disponibles se maintenant à des niveaux élevés. À l'avenir, les bénéfices et les réserves s'avéreront insuffisants compte tenu des dépenses d'investissement liées à l'IA estimées à 3 400 milliards de dollars par an. Ces dépenses exerceront des pressions sur leur bilan dans les années à venir. En prévision de ces dépenses futures de 100 milliards de dollars par le biais d'émissions obligataires depuis janvier 2025 (...). Cela dit, l'ampleur des dépenses d'investissement (capex) en IA sur le marché des titres ne sera pas excessive. La qualité de crédit moyenne des hyperscalers est solide compte tenu de la robustesse de leur situation financière à générer d'importants flux de trésorerie disponibles. Par conséquent, même si le rythme des émissions d'obligations restera 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 à l'échelle des valorisations et des investissements astronomiques des géants américains de la tech. La poursuite des investissements des sociétés d'intelligence artificielle repose sur une potentielle croissance exponentielle **correspondant aux attentes des investisseurs**. Or des doutes importants existent à ce sujet, qu'ils soient liés à la disponibilité de data centers ou des raccords électriques, disponibilité des puces) ou à la demande (délais de livraison des entreprises). L'horizon temporel de retour sur investissement pourrait donc être plus faible et plus incertain.

Dans son *Technology report*, publié en septembre 2025, la société de conseil Bain souligne que pour répondre à l'IA sont multipliés par 4,5 chaque année, ce qui est deux fois supérieur à l'augmentation de l'efficacité énergétique. Pour répondre à ces besoins, une capacité de production électrique supplémentaire de 200 gigawatts sera nécessaire aux États-Unis. Cela représente un investissement estimé à 500 milliards de dollars par an. Si, malgré de tels investissements en maintenant des ratios de solvabilité suffisants, les hyperscalers devaient lever 2 000 milliards de dollars.

Pour estimer les potentiels revenus générés par la monétisation de l'IA, la société de conseil Bain propose :

- 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 par an, ce qui est bien inférieur au scénario maximaliste des revenus possibles des entreprises d'intelligence artificielle. Y compris dans un tel scénario, les revenus ne seraient pas suffisants pour financer l'ensemble des investissements nouveaux – sans même prendre en compte le renouvellement du matériel. L'écart entre le revenu et les besoins de financement s'élèverait donc à 2 790 milliards de dollars.

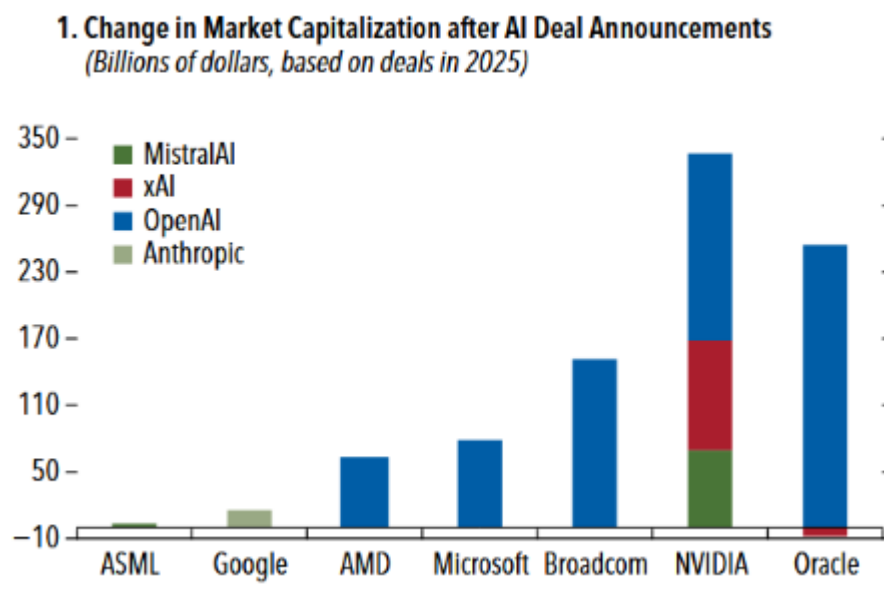
produits phares, Sora. Destiné à la génération de vidéos par intelligence artificielle, il avait entraîné une hausse de 100 % de sa capitalisation boursière. Ainsi que le rapporte Mediapart, citant le Wall Street Journal « *Sora coûtait en moyenne 1 million de dollars par vidéo générée, qu'un peu plus de 2 millions de dollars.* » ([426])

De l'autre, après une phase d'enthousiasme pour un produit nouveau, de nombreuses entreprises ont commencé à regretter l'IA au regard de l'envolée des factures de tokens. Ainsi, alors que les coûts liés à l'IA chez Uber ont augmenté de 100 %, un article de *Next* rapporte que le directeur des opérations, Andrew Macdonald, considère qu'« *il est devenu très coûteux de développer des applications liées à l'usage de l'IA générative. Invité du podcast Rapid Response, il a expliqué qu'une consommation excessive de tokens mène nécessairement à une augmentation proportionnelle des fonctions utiles pour le consommateur.* » ([427]) Praveen Neppalli Naga, directeur technique de la plateforme VTC, s'était étonné chez *The Information* que les coûts de l'IA aient augmenté de 100 % en l'année en seulement quatre mois. »

Une étude menée par des chercheurs du Massachusetts Institute of Technology ([428]), basée sur une enquête auprès de 100 entreprises d'entreprise, montre que 95 % des entreprises ayant investies dans l'IA générative sont « *coincées* » dans un cycle de dépenses sans bénéficier d'aucun retour sur investissement. Des résultats confirmés par lors des différentes conférences sur l'IA, il est communément admis qu'il n'existait aucune étude macroéconomique mesurant le niveau de dépense et 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 l'écosystème de l'IA artificielle », composé d'Amazon, AMD, Alphabet (Google), Intel, Microsoft, Nvidia et Oracle. Ces dernières sociétés appartenant à ce cercle ont vu leur capitalisation boursière augmenter de 40 milliards de dollars, contre une augmentation moyenne de 7 points. « *Depuis 2025, les mécanismes de financement circulaire se sont généralisés. Dans le cadre de ces mécanismes, les développeurs d'IA, les fabricants de puces et les investisseurs jouent simultanément le rôle de clients, d'investisseurs et de bailleurs de fonds. La structure de ce financement crée des liens étroits entre les entreprises cotées en bourse (par exemple, Nvidia, Oracle) et celles non cotées liées à l'IA (par exemple, les startups). Ces liens étroits entraînent des niveaux de vulnérabilité financière variables et des modèles économiques divers. Ces liens étroits entre entreprises concernées peuvent chacune se prévaloir de prévisions de chiffre d'affaires gonflées, au détriment de leurs cours et de leur valorisation. Le graphique ci-dessous montre la hausse des capitalisations boursières d'accords croisés.*



Source : Fonds monétaire international.

Second risque, les dépréciations brutales d'actifs liées à l'obsolescence technique. Les entreprises ont des dépréciations comptables au regard de la rapidité de l'évolution technologique. Le FMI souligne que les entreprises ont des dépréciations comptables au regard de la rapidité de l'évolution technologique. Le FMI souligne que les entreprises ont des dépréciations comptables au regard de la rapidité de l'évolution technologique.

ou de créer de nouveaux emplois ? M. Aïman Ezzat, directeur général de Capgemini, a témoigné et dirige ^([433]) : « *Nous devons nous adapter en permanence aux évolutions technologiques comme au passé. Nous envisageons effectivement environ 2 400 suppressions de poste. Ce ne sont pas 2 400 licenciements ou départs volontaires. C'est lié à des évolutions. Ainsi, le contrôle qualité des logiciels était très intensif, avec l'intelligence artificielle, il est de plus en plus automatisé. Il est évident que les besoins ne sont plus les mêmes. Nous évoluons, nous évoluons les compétences de nos collaborateurs, ou nous proposons des départs volontaires, par exemple, pour des personnes dans ce domaine précis. Il y a un grand plan d'investissement dans les compétences lié à la transformation numérique.* »

Durant les travaux de la commission d'enquête, plusieurs groupes ont annoncé des suppressions de postes et la généralisation de l'IA. Le secteur bancaire a été particulièrement touché : 1 800 emplois supprimés dans le monde pour BNP Paribas ^([434]), jusqu'à 20 000 postes chez HSBC d'ici cinq ans ^([435]).

De la même manière, le secteur de la presse est fortement affecté : 400 postes supprimés par *Libération*, *L'Est Républicain*, *Les dernières nouvelles d'Alsace*, etc.), 261 postes supprimés par *Prisma*, etc.), et 19 postes de rédacteurs supprimés au sein du groupe Infopro Digital (*Le Moniteur*, etc.) ^([436]).

Qu'en est-il de l'impact économique de l'intelligence artificielle ? Les travaux économiques sur l'impact de l'intelligence artificielle ne sont encore qu'à leurs débuts. Toutefois, certaines études présentent d'ores et déjà des résultats.

La commission de l'intelligence artificielle, installée par Mme Elisabeth Borne en 2023, a confié à Mme Anne Bouverot, en a réalisé une première synthèse dans son rapport de mars 2024 ^([437]). Pour elle, l'intelligence artificielle est d'automatiser certaines tâches, ce qui crée deux effets contradictoires sur l'activité : d'une part, elle remplace l'humain et réduit ainsi l'activité. De l'autre, elle augmente la productivité des individus, ce qui crée de nouveaux produits, à la condition que les gains économiques bénéficient effectivement au consommateur et ne soient pas captés par des monopoles. Ainsi que l'indique le rapport de Philippe Aghion, « *pour comprendre l'effet d'un choc technologique sur le marché du travail, il faut donc comprendre qui de ces deux effets l'emporte. Pour cela, deux approches sont possibles. Premièrement, en étudiant directement les effets de l'adoption de l'IA au sein des entreprises ou de la production. Deuxièmement, en étudiant les effets de l'IA sur les différentes tâches composant l'économie.* »

Deux articles récents, de l'Insee ^([438]) et de la direction générale du Trésor ^([439]), effectuent 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 a réalisé une comparaison entre 312 entreprises ayant adopté l'intelligence artificielle (non générative) et 897 entreprises n'ayant pas adopté l'IA. Elle constate que *l'emploi total dans les premières augmente davantage que dans les secondes, alors que ces deux groupes ont des caractéristiques similaires. L'effet résulte principalement de la création de nouveaux emplois, plutôt qu'un maintien ou une augmentation de l'emploi existant. En particulier, certains échelons au sein de l'entreprise ou certains métiers risquent de subir des réductions, notamment dans les fonctions administratives ou le marketing.* » ^([440])

La rapporteure note trois éléments sur ce travail de comparaison. Tout d'abord, ce travail est préliminaire car l'usage de l'IA est encore peu généralisé. On peut donc supposer que cette étude porte sur des secteurs très exposés à l'IA. 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 les entreprises ^([441]), constate que « *l'usage de l'IA augmente avec la taille de l'entreprise : 9 % des entreprises de moins de 50 salariés y ont recours, contre 33 % de celles de 250 salariés ou plus. Les entreprises de 50 à 249 salariés concentrent la moitié du chiffre d'affaires total et représentent deux cinquièmes de l'emploi.* »

Une autre étude, publiée par Xiang Hui, Oren Reshef et Luofeng Zhou en août 2023 ^([445]), a constaté un effet négatif sur l'emploi et la rémunération des travailleurs américains indépendants recrutés sur des plateformes de travailleurs *freelance* pour des missions de courte durée, en particulier pour la rédaction de textes. La rémunération sur la plateforme diminue de 2 % chaque mois et les revenus touchés par les travailleurs indépendants de longue date expérimentés sont tout aussi touchés. Selon les auteurs, ces résultats suggèrent que l'utilisation de l'IA tend 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 Statistique de l'OCDE, se base sur une enquête réalisée auprès de 5 300 travailleurs et 2 000 entreprises dans sept pays (Autriche, Canada, France, Allemagne, Irlande, États-Unis et Royaume-Unis) ^([446]). Elle constate que l'IA n'avait entraîné aucun changement en matière d'emploi au sein de leur entreprise, le nombre d'emplois a dépassé celui des employeurs ayant signalé une augmentation. Dans les entreprises ayant adopté l'IA, 15 % du secteur financier et 15 % des employés du secteur manufacturier déclarent connaître quelqu'un dans leur entreprise victime de la cause du déploiement d'outils d'intelligence artificielle. 29 % et 24 % ont déclaré connaître quelqu'un qui a perdu son emploi à cause de l'IA. Ces baisses pourraient indiquer que l'IA a automatisé davantage d'emplois qu'elle n'en a créés. Les données sur l'ampleur des pertes et des gains d'emplois – les gains pourraient concerner un nombre limité de postes en proportions plus grandes.

Enfin, la note de conjoncture de l'Insee précitée revient sur les impacts de l'essor de l'intelligence artificielle. Elle reconnaît un lien possible entre le développement de l'IA et la baisse de l'emploi des jeunes. Elle précise : *« précisément, les ajustements liés à l'IA pourraient, à court terme, se concentrer moins sur l'emploi des jeunes, en particulier sur les positions d'entrée dans certains métiers (fonctions support, administratif, commercial, etc.), et pénaliser fortement les jeunes. (...) »*

« En France, une analyse semblable est possible à partir des séries d'emploi par âge dans les services d'information, de l'édition et des activités des sièges sociaux et conseil en gestion (...) ». L'emploi concentré sur les jeunes : au quatrième trimestre 2025, l'emploi salarié des 15-29 ans (hors agriculture) a baissé de 7,4 % dans les activités informatiques, de 5,8 % dans l'édition, et de 3,7 % dans les activités de conseil en gestion 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. Globalement en ralentissement en France et d'autre part, ces secteurs peuvent être concernés par une baisse. Les indicateurs d'activité continuent d'être correctement orientés dans des secteurs qui connaissent une baisse d'effectifs depuis 20 ans : le retournement paraît ainsi brutal et plutôt concomitant de l'arrivée de cette IA. (...) »

b. Quelle est la proportion de tâches de l'économie pour lesquelles les travailleurs sont susceptibles d'être remplacés par l'IA ?

En complément de l'approche examinant *ex post* les effets de l'adoption de l'IA sur l'activité, quantifier, pour chaque métier, *ex ante*, les effets potentiels de l'IA via un « indice d'exposition » à l'IA et ses effets potentiels sur l'économie.

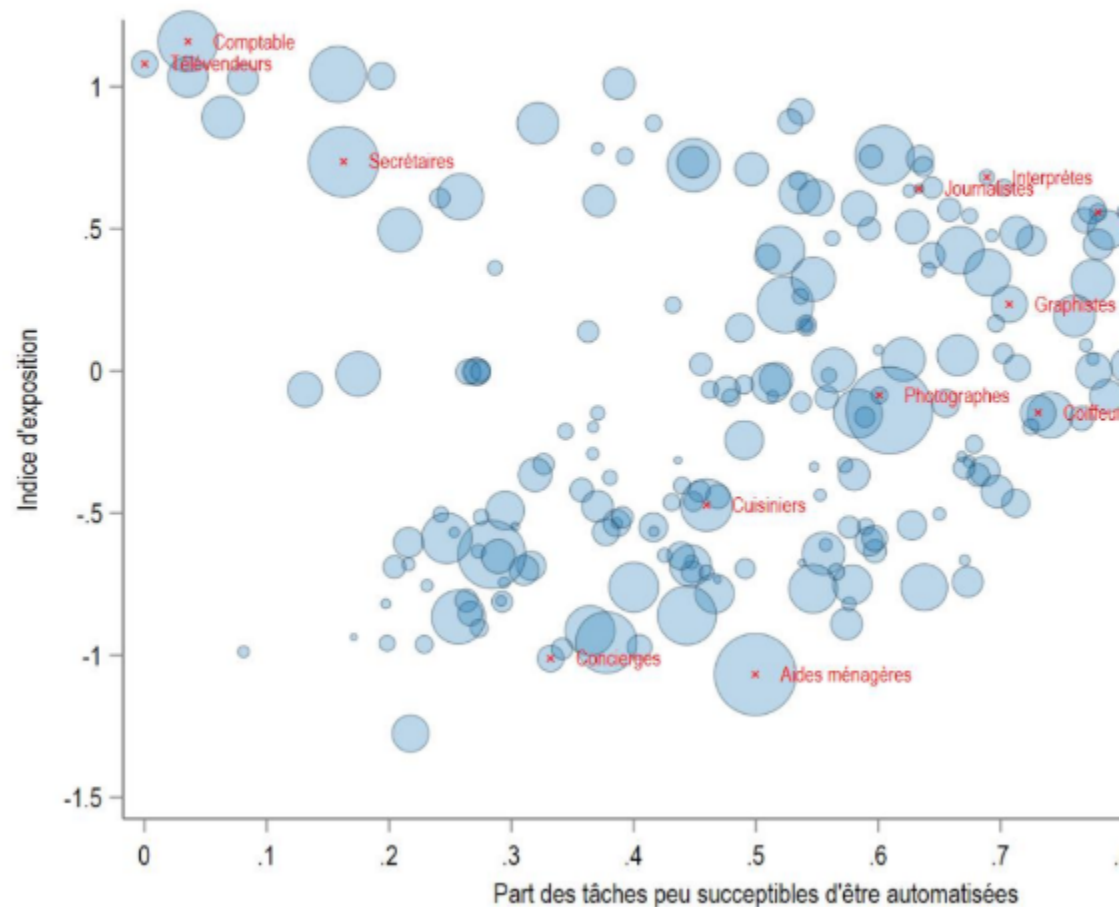
Il est intéressant de comparer les travaux publiés au cas de l'entreprise Mistral AI. Son dirigeant déclare : *« n'y a pas encore beaucoup d'études macroéconomiques parce qu'on manque de recul : la délégation de la journée n'est possible que depuis six mois. Je le disais, avec 10 % de notre masse salariale consacrée à l'IA, nous avons fait un gain de productivité de facteur 2 par rapport à il y a six mois. Ce n'est pas une étude, mais ça parle d'un gain de productivité pour un coût représentant 10 % à 20 % des opex (dépenses d'exploitation) par tête de monde. »*

« Certes, la productivité ne sera pas multipliée par deux partout ; chez nous c'est assez facile, car la tâche physique de notre activité, l'utilisation des agents suscite peu de frictions. Dans l'industrie lourde, ça sera plus compliqué. (...) »

Le rapport conclut que le développement de l'IA comporte un risque de remplacement d'emploi, mais qu'il comporte également des opportunités en termes de productivité et de complément du travail humain.

Une note d'Antonin Bergeaud de janvier 2024 ^([448]), publiée pour le Laboratoire de l'innovation, a réalisé un travail similaire sur des données françaises, afin de dresser un panorama des effets attendus de l'IA, définies par la nomenclature du ministère du travail.

FIGURE 1 : POSITIONNEMENT DE CHAQUE FAP DANS UN REPERE EXPOSITION (AXE DES ORDONNÉES) / TÂCHES DIFFICILE À AUTOMATISER (AXE DES ABSCISSES). LA TAILLE DE CHAQUE CERCLE EST PROPORTIONNELLE À L'EMPLOI TOTAL DANS LA FAP EN FRANCE EN 2020.



Le graphique positionne ces familles professionnelles sur deux axes : l'exposition à l'IA et la part des tâches difficiles à automatiser. Les professions comme les juristes, les médecins ou les architectes, évolueront fortement avec l'apparition d'applications basées sur l'IA, mais elles conserveront néanmoins une part importante de tâches non substituables. Enfin, et de façon assez inattendue, les cuisiniers, les concierges ou les aides ménagères, sont peu susceptibles d'être fortement exposés.

Enfin, l'Observatoire des emplois menacés et émergents a mené une étude sur les effets de l'IA à partir d'une analyse fine des tâches au sein de 923 professions. « *L'étude met en évidence une rupture dans la logique d'automatisation : l'intelligence artificielle ne prolonge pas les vagues précédentes d'automatisation en déplaçant leur centre de gravité vers les tâches cognitives, complexes et non répétitives. Son impact se concentre d'abord au niveau des tâches, puis se répercute de manière inégale sur les métiers, les familles professionnelles et les secteurs d'activité.* »

« Dans le scénario central étudié portant sur le déploiement de l'intelligence artificielle à l'échelle nationale, la France franchit le seuil de 30 % de tâches automatisables, que l'étude retient comme un seuil de transformation structurelle. Cela signifie sa disparition. Les professions les plus exposées se concentrent dans les univers à forte intensité technologique : ingénierie, informatique, fonctions administratives, finance, droit ou encore certains métiers de la santé. Les professions les moins exposées sont celles qui nécessitent une forte interaction humaine, comme les métiers de la santé, les métiers de l'éducation ou les métiers de la culture. »

0,25 et 0,3 point aux États-Unis, à comparer avec le taux de croissance qui est de 1 point de point de dernières années. Il s'agit donc d'une contribution significative, mais toutefois inférieure à celle qu'en 1995-2005 grâce aux nouvelles technologies.

La direction générale du Trésor rassemble les estimations des effets de l'IA sur l'emploi agrégé

Tableau 1 : Panel des estimations des effets de l'IA sur le niveau d'emploi agrégé		
Références	Réaction de l'emploi	Zone géographique
Hartley <i>et al.</i> (2025) ^a	0	États-Unis 2010-2023
Teeselink (2025) ^b	–	Royaume-Uni 2021-2025
Lebastard <i>et al.</i> (2026) ^c	0/+	Europe 2025
Baslandze <i>et al.</i> (2026) ^d	0	États-Unis 2025
Yotzov <i>et al.</i> (2026) ^e	0	États-Unis, Royaume-Uni, Allemagne et Australie 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 (hausse des prix, hausse du pouvoir d'achat, redéploiement de la demande vers d'autres secteurs), qui compte pour la substitution.* » En l'occurrence, les effets sont nuls ou proches d'être nuls dans quatre études sur cinq, 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'IA générative dans l'économie, et de disposer de premières évaluations de leurs effets. Du fait des limites (disponibilité des données, difficulté à construire des modèles fournissant une vision complète de l'impact de l'IA sur l'adoption de l'IA, quatre réserves doivent être signalées.

Premièrement, les travaux réalisés examinent les chances de disparition de tâches existantes. Ils ne peuvent donc pas tenir compte des tâches qui pourraient être créées à la suite du développement du domaine de l'IA. Comme l'indique le rapport de la commission de l'intelligence artificielle, « *d'imaginer que le métier de data scientist puisse prendre une telle place au début de la révolution numérique, ou que le métier de dépanneur en électroménager puisse exister avant l'adoption massive de l'électricité domestique.* » De la même manière, il est à ce stade difficile d'identifier toute l'ampleur des tâches automatisables lors des futures évaluations, que cela représentera *in fine* pour l'employeur.

Deuxièmement, ces travaux reposent sur une estimation de la probabilité de remplacement des tâches, aujourd'hui très subjective. Les études expérimentales se concentrent sur des tâches simples et bien ciblées, dans la recherche concernant l'impact de l'IA sur les tâches complexes, courantes dans les entreprises. En raison de l'importance prise par le sujet de l'impact de l'intelligence artificielle sur l'emploi, les travaux économiques ont développé des méthodes de classification des professions. Une note de travail de l'OCDE, datant du 26 mai 2026 (OCDE, 2026), mesure de l'exposition à l'IA en adoptant une approche complète des compétences requises par les professions. Les compétences sont prises en compte, réparties en trois groupes (compétences cognitives, sociales et techniques). Cet indicateur n'est pas comme une mesure directe de l'adoption de l'IA dans les différentes professions, mais reflète des probabilités de déploiement. Utiliser un panel plus complet fait apparaître que l'exposition potentielle concerne les métiers dont les tâches sont plus standardisées et codifiables, tandis que des lacunes importantes existent pour l'interaction sociale, la résolution de problèmes et de nombreuses autres tâches nécessitant une incarnation humaine. L'exposition, par leur degré d'exposition, mais aussi par les capacités qui déterminent cette exposition.

des considérations de communication financière. Ainsi, 59 % des entreprises américaines admettent d'embaucher, 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, l'État, les partenaires sociaux, France Travail, l'Insee et des experts indépendants.
Une telle cellule aurait vocation à rassembler l'État, les partenaires sociaux, France Travail, l'Insee et des experts indépendants pour identifier les risques et les opportunités 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

Dans l'estimation des impacts de l'IA pour l'économie française, il convient également d'évaluer si l'économie française est-elle bien positionnée ? Quels sont les risques et les opportunités, eu égard des caractéristiques de l'économie française par le déploiement ?

La rapporteure a noté deux phénomènes qui pourraient être source de vulnérabilité : un déclin de la croissance de la valeur ajoutée par des entreprises extra-européennes.

a. Les gains économiques sont-ils réels ?

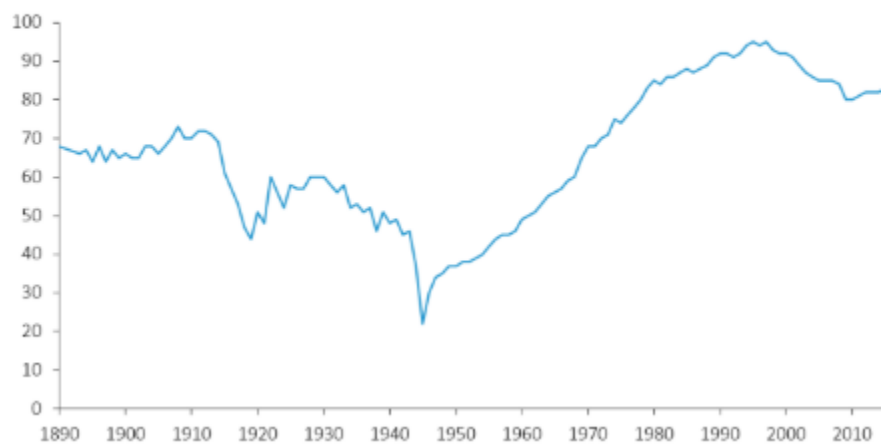
Le lien entre développement technologique et croissance des différentes zones économiques est bien établi. L'adoption des technologies numériques est notamment pointée du doigt pour expliquer la croissance des États-Unis. Par exemple, Robert Gordon et Hassan Sayed ⁽⁴⁵³⁾ montrent que la hausse de la productivité fut tirée par les industries fortement intensives en technologies numériques, et par le secteur de la construction. Par comparaison, dans dix pays de l'Union européenne, la croissance a connu un ralentissement entre 1990 et 2000, lié aux investissements en télécommunications, ainsi qu'à des difficultés à capter les facteurs d'efficacité. Après 2005, les économies des deux côtés de l'Atlantique connaissent toutes les deux un ralentissement de la croissance, 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 augmenté de 95 % en 1945 à 1995, cette croissance a ensuite connu un ralentissement plus marqué, n'atteignant que 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 est la divergence de la croissance de la productivité. L'Europe semble actuellement prendre encore plus de retard. La principale raison pour laquelle la productivité de l'Europe est inférieure à celle des États-Unis au milieu des années 1990 a été l'incapacité de l'Europe à tirer parti de la productivité de la technologie de l'information — tant en ce qui concerne la création de nouvelles entreprises technologiques que la diffusion de la technologie existante. »

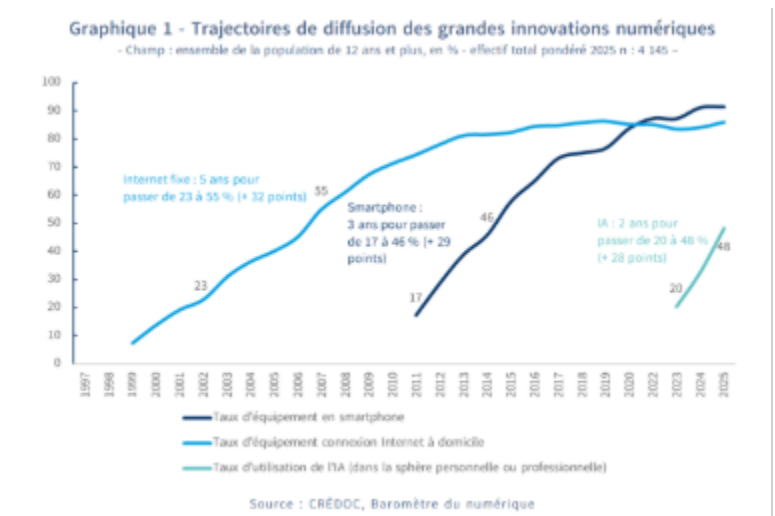
nous dépendons majoritairement d'acteurs américains ?

b. Une captation de valeur par les hyperscalers, qui renforceront leur domination

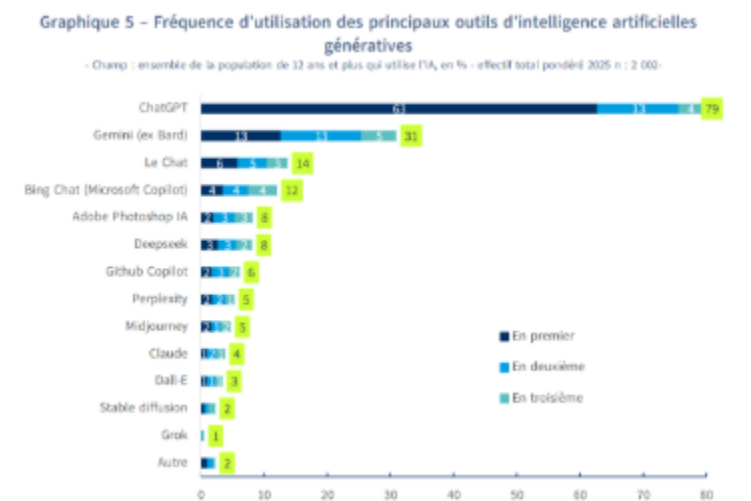
Avec le déploiement des outils d'IA, les schémas qui ont prévalu lors de l'installation des reproduire. La rapidité et la facilité de déploiement est privilégiée au choix de solutions européennes situations d'enfermement inévitables.

S'agissant des **outils à destination des particuliers, tout d'abord, l'offre américaine domine la** **génération.**

Selon le Baromètre du numérique publié par l'Arcep, le Conseil général de l'économie, l'Arcep des territoires ^([455]), la diffusion des outils d'IA au sein de la population est très rapide, davantage que les smartphones. 48 % des Français de plus de 12 ans utilisent aujourd'hui ce type d'outils, ce qui rep



ChatGPT est utilisé par 79 % des Français utilisant l'IA – soit 22 millions d'utilisateurs d'o contre seulement 14 % pour Le Chat de Mistral IA – 4 millions d'utilisateurs.



L'usage des technologies numériques états-uniennes est donc d'ores et déjà généralisé dans le

S'agissant des **outils à destination des professionnels, le déploiement d'outils d'IA non-structurelles importantes.** Dans un article publié en septembre 2025 dans la revue du National Bureau of Economic Research, Susan Athey et Fiona Scott Morton développent un modèle économique pour tenter de décomposer l'activité induits par une captation de valeur des entreprises proposant les modèles d'IA. Cet article suppose que le remplacement des tâches réalisées préalablement par des salariés est

les mêmes conditions ». Elles bénéficient également d'avantages liés à leur intégration verticale et co

Enfin, elles déploient nativement leurs propres outils d'IA dans leurs écosystèmes de pr
déploie ses propres modèles et ceux de son partenaire OpenAI dans la fonction « Copilot » afin d'a
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
des éléments d'analyse de l'Autorité de la concurrence, puisqu'elle décrit exactement les mêmes ph
la chaîne pour son concurrent : *« La concurrence dans le cloud n'est pas alimentée par d'anciens l*
jamais été aussi évident qu'aujourd'hui. Dans ce nouveau paradigme de cloud computing piloté
d'avantages uniques : un marché plus important et un chiffre d'affaires annuel supérieur à Micro
empreinte mondiale massive de centres de données qui fournit du calcul à la demande ; le plus gran
continu par les services grand public les plus utilisés au monde ; Deep Mind, un laboratoire de recr
des années ; et une capacité inégalée à atteindre les consommateurs via Android et Chrome. Ce s
l'avenir de l'informatique en nuage que les logiciels comme Windows Server » ⁽¹⁴⁶⁰⁾. Plus que toute
mieux placés pour bénéficier du boom de l'intelligence artificielle : par leur accès aux données et a
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
aujourd'hui. L'éclatement d'une bulle est tout à fait possible, si les revenus tardent à se matérialiser
à suivre le rythme du numérique. Mais le déploiement de l'intelligence artificielle générative aura q
la population active, à moyen et long terme. Les enjeux systémiques pour la France sont de quatre or

- identifier les limites physiques au déploiement de l'IA, qu'elles soient technologiques ou c
- 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
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 a
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
impossible de prédire le résultat des actions. C'est en particulier le cas de l'IA agentique, dont l'obj
dans la mise en œuvre d'actions ayant des conséquences concrètes. Ainsi que le relève Mme M
agentique et de son intégration dans les systèmes d'exploitation, qu'elle soit mise en œuvre
l'intermédiaire de dispositifs qui incitent les utilisateurs à accorder à ces agents des permissions ex
à l'ensemble de leurs données, notre inquiétude est, évidemment, très vive. Voilà en effet plusieurs
face à ces évolutions nouvelles. Nous observons en effet une pression croissante en faveur d'une
toujours davantage de contrôle sur nos vies et à agir de manière autonome, alors même que le pa
directe avec les exigences de cybersécurité et de protection de la vie privée. Le terme même d'
technique, désigne en réalité un système qui remplit deux fonctions. D'une part, pour pouvoir agi
univers, à votre environnement, à votre contexte, autrement dit à vos données, de sorte qu'une m
soudainement accessible. Ces données sont, très vraisemblablement, transmises ailleurs, car la puis

2. Le sujet critique de la cybersécurité

Le 12 juin 2026, le gouvernement américain exigeait d'Anthropic la suspension de l'accès à Mythos 5 ^([462]). Cette décision met en lumière les impacts globaux que pourrait avoir le déploiement

Le cas d'une fermeture de l'accès des modèles aux non-États-Uniens crée un déséquilibre flou. On constate que la sécurité de l'ensemble de nos systèmes d'information dépend de la décision unilatérale de l'accès à ses modèles pour l'ensemble de ses clients, y compris États-Uniens. Mais au-delà du choc de cet épisode, il faut en réalité considérer Mythos comme le premier de la catégorie des modèles frontière cyber, « *Mythos doit donc être dé-mythifié* » : *prendre le modèle moins pour ce qu'il est et ce qu'il révèle des grandes lignes de force qui refaçonnent le paysage de la cybersécurité sous sa manifestation du phénomène à un instant T, mais dans la pente de la courbe. Il faut appréhender Mythos comme le dernier signal en date d'une accélération très forte des modèles* » ^([463]). Mythos sera une référence aux performances qui ne cesseront de s'améliorer.

Devant la commission d'enquête, M. Vincent Strubel, directeur général de l'Anssi, dressait un constat sur l'accès à Mythos. *Comme la plupart des observateurs, nous l'analysons à partir de témoignages et d'une prudence. Ce qui en ressort, au-delà du discours porté par Anthropic, c'est moins une rupture qu'une évolution déjà engagée. L'évolution était prévisible et elle va se poursuivre. En cela, Mythos ne constitue pas durablement le paysage car d'autres acteurs atteignent déjà des niveaux comparables, et les progrès sont loin. Nous sommes face à une dynamique d'amélioration continue, dont l'accélération impose d'être vigilant en termes de rupture ponctuelle.*

« *Dans ce contexte, l'intelligence artificielle devient effectivement de plus en plus apte à identifier des failles de code permettant de les exploiter. Cela ne signifie pas qu'un modèle comme Mythos soit aujourd'hui capable de mener une cyberattaque de bout en bout, mais il peut fournir à un attaquant humain des éléments crédibles pour leur exploitation. La conduite complète de l'attaque, avec la compréhension de l'infrastructure cible, revient en revanche du ressort humain. Il s'agit d'une évolution significative et la réponse à votre deuxième question est d'intégrer ces évolutions dans nos logiques de certification et, plus largement, dans la production logicielle, en difficulté face aux vulnérabilités puisque des dizaines de milliers sont découvertes chaque année dans des logiciels, mais sur des systèmes déjà en circulation, et elles peuvent être exploitées très rapidement. Des correctifs, que la plupart des organisations ne parviennent pas à absorber dans les délais, même si les services de défense en profondeur permettent d'en atténuer les effets, mais elles ne dispensent pas de traiter les vulnérabilités des logiciels.* »

Ce constat appelle plusieurs commentaires. Tout d'abord, il convient de préciser que Mythos est un modèle de bout en bout pour des systèmes mal protégés. C'est ce qui ressort de l'évaluation du modèle effectuée par le centre de recherche du ministère des sciences, de l'innovation et des technologies britannique ^([464]) : « *Le modèle d'entraînement cyber montre qu'il est au moins capable d'attaquer de manière autonome des systèmes non défendus et vulnérables, pour lesquels l'accès au réseau a été obtenu (...) Nos tests démontrent que les systèmes présentant une posture de sécurité faible, et il est probable que d'autres modèles dotés de capacités similaires*

À mesure que les performances des modèles s'amélioreront, ces derniers seront en mesure de mener de mieux en mieux protégés, y compris ceux sur lesquels repose le fonctionnement d'infrastructure critique. Les nouvelles pourront être mises à disposition dans des échelles de temps très rapides, ne laissant que peu de corrections nécessaires.

Selon le Campus cyber, « *les dirigeants d'organisations doivent se préparer à une vague (d'ici 2027) de découverte massive de zero days mises au jour par l'IA, avec un effet de purge - en*

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 l'intelligence artificielle. En effet, les infrastructures physiques sont une composante essentielle du fonctionnement des modèles. Le Sommet de l'IA à Paris en février 2025, voulu par le Président de la République, annonce 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 soutenue par la politique de captation de la capacité électrique par certains acteurs ?

– la localisation physique des data centers est-elle un moyen de retrouver un contrôle sur la souveraineté numérique et des 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 que pour l'inférence, peut s'effectuer de façon distribuée, en recourant à un réseau de câbles interconnectés et de data centers. 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 du lieu d'utilisation crée un délai de latence de quelques millisecondes qui peut pénaliser certaines applications. Cela concerne notamment les assistants vocaux ou encore des usages industriels associant des capteurs à des commandes. La localisation géographique, et pas nécessairement l'implantation sur le territoire national (un data center à Amsterdam ou un data center industriel français basé à Dunkerque qu'un data center à Marseille).

Toutefois, la localisation sur le territoire de grandes capacités de traitement de données s'applique à des 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 délocalisée.

– la **construction** (incluant la préparation de site, le génie civil, le montage et les tests) et les **infrastructures** : ces activités sont peu délocalisables. Si elles sont intensives en emploi au moment de la construction, elles le sont moins en phase d'opération. Ainsi que l'indiquait M. Fabrice Coquio, président-directeur général de Datacenter France : *« Ces infrastructures pour le territoire concerné, il s'observe d'abord pendant la phase de construction que les emplois sont nombreux. On emploiera 400 à 450 compagnons pendant deux ans, sans parler des machines que nous sommes en train d'acheter, qui sont françaises ou européennes (...). Contrairement à ce qu'on pense parfois, on pourrait presque dire qu'un data center à Dunkerque n'emploie pas plus de personnes que chacun de nos quatre centres marseillais, 120 à 170 personnes entrent et sortent par tranche de vingt personnes par semaine »*.

« (...) Il est vrai que les data centers restent des infrastructures : ils sont intensifs en emplois. L'estimation du nombre d'emplois directs créés par l'activité des data centers est fournie par AWS : « Dans le cadre de nos dossiers de demandes de permis, chaque 1 000 m² de surface de centre de données crée 10 emplois directs ».

sont des fonds d'investissements internationaux, mobilisant des fonds issus de l'ensemble des pays, proviennent majoritairement d'acteurs extra-européens, limitant ainsi les impacts positifs pour l'économie française.

– qu'en est-il de l'**activité de vente du calcul** à proprement parler ? Il s'agit de la partie prioritaire ajoutée du modèle économique de l'intelligence artificielle, la transformation de l'électron en token. Le data center n'assure pas le retour de cette valeur dans le pays, ni l'utilisation par des clients nationaux. Les clients extra-européens, M. Coquio indiquait ^([474]) : « *Elle est grosso modo de 50 %. C'est le cas en France, dans les pays européens où nous sommes implantés, sauf à Marseille, où la part des clients étrangers est de 80 %*. L'organisation mondiale de la donnée, trois zones métropolitaines – Singapour, Miami et Marseille – à l'échelle géographique, des gateways, c'est-à-dire, des portes d'entrée et de sortie. Si Marseille est devenue un hub, elle croît d'environ 30 % par an, c'est parce qu'elle se situe à l'interface entre, d'un côté, l'hinterland français – Francfort, Londres, Amsterdam –, et, de l'autre, l'Afrique, le Moyen-Orient, l'Inde et l'Asie. Un peu de valeur est connectée à Marseille ! C'est pourquoi les clients étrangers sont surreprésentés dans ce hub (...) Les accords traités concernent l'Inde ».

Selon les modalités de fourniture des services d'IA, la part de valeur localisée en France peut être :

– dans le cas d'un service d'IA fourni par un *hyperscaler* à partir d'un data center localisé en France, la part de valeur en France est nulle ;

– la localisation en France du data center utilisé pour l'inférence (réponse aux requêtes) permet de relocaliser l'activité d'achat d'électricité et de construction-exploitation. Toutefois, si ce data center est localisé hors de France, la 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 de calcul sont localisés en Europe, utilisant ses propres modèles ou des modèles ouverts, et financés au moins en partie par des clients européens.

Concernant les recettes fiscales, les taxes locales et les taxes de fonctionnement (éventuellement de l'État) peuvent être appliquées sur le territoire. S'agissant de l'impôt sur les sociétés, la part revenant dans le pays 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. L'accès au calcul induit nécessairement un accès aux données de l'utilisateur : les données nécessaires pour le réglage du calcul, l'entrée et la sortie. Comme il a été montré dans le chapitre 4, la localisation sur le territoire n'est pas suffisante pour la maîtrise des données, du fait de l'application extraterritoriale du droit. Toutefois, c'est une question de confiance des administrations, des entreprises et des citoyens sur leurs propres données.

La pénétration croissante de cette technologie dans les processus économiques pourrait faire émerger une dépendance au fonctionnement d'un pays, et la localisation territoriale des data centers la seule façon d'assurer une souveraineté numérique.

B. ÉTAT DU DÉPLOIEMENT : DES PROJETS QUI BÉNÉFICIERONT EN GRANDE MAJORITÉ À L'ÉCHELLE NATIONALE

La rapporteure souhaitait réaliser un état des lieux du déploiement des data centers en France, identifier les acteurs et déterminer dans quelle mesure le développement des projets sur notre territoire contribue à notre indépendance. Au contraire, renforce nos dépendances. Pour cela, la commission d'enquête a eu accès aux données de consommation du réseau public de transport d'électricité effectuées par les développeurs de projet ^([475]). Les puissances installées de façon agrégée, afin de ne pas divulguer d'informations commercialement sensibles.

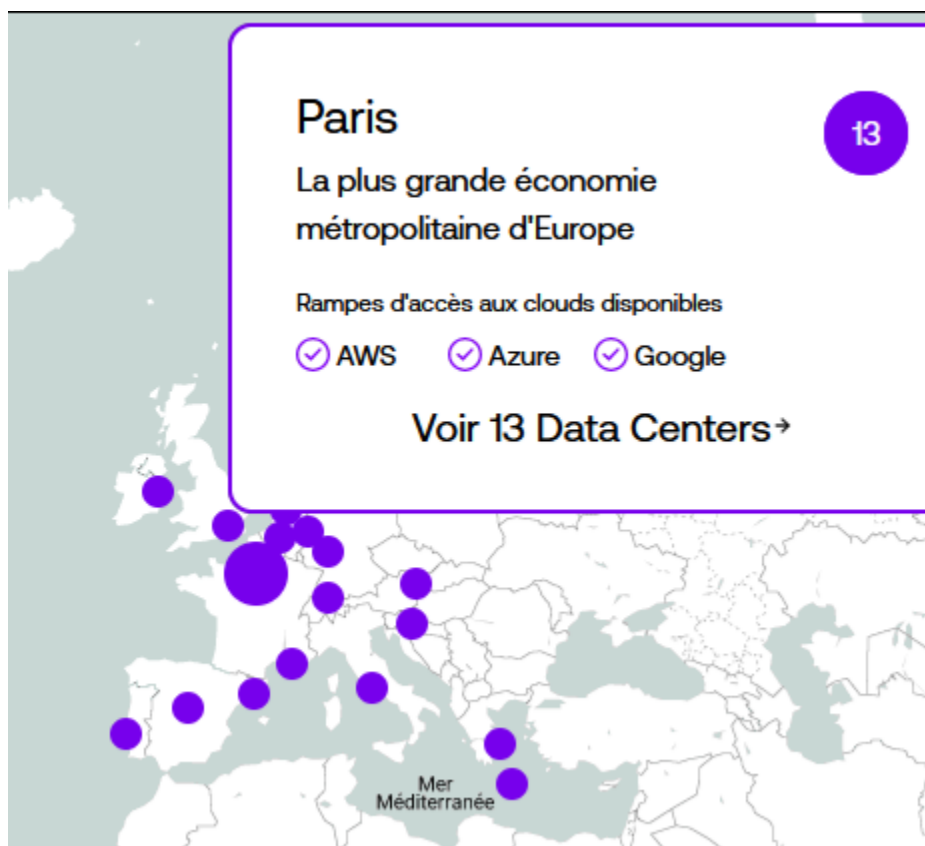
1. Une capacité électrique réservée représentant 24 % de la puissance installée du parc national

États-Unis	
Promoteurs immobiliers et logistiques	
France	
Extra-UE hors États-Unis	
États-Unis	
UE hors France	
Investisseurs internationaux	
Extra-UE hors États-Unis	
France	
UE hors France	
Total général	

Source : RTE.

Au total, les acteurs du secteur (*hyperscalers* et développeurs et exploitants de data centers) ont contractualisé une capacité totale de 5,8 GW. Au sein de ces deux catégories, les acteurs états-uniens et français ont contractualisé 1,3 GW (22 %) et 1,3 GW (9 %).

Concernant les développeurs et exploitants de data centers, comme Digital Realty ou Datacenter Group, ils ne sont pas en mesure de fournir de l'information sur l'utilisation effective de la capacité de calcul, comme cela a été démontré dans les auditions. Les infrastructures de Digital Realty à Marseille sont utilisées entre 60 % à 70 % par des clients extra-européens. Cela illustre bien à quel point les hyperscalers sont structurants dans le portefeuille de l'opérateur ^([478]). L'opérateur est également impliqué dans des affaires en France avec des acteurs non-européens ^([479]), dont 45 % avec des hyperscalers – elle-même a des sociétés Bleu et Tricolore.



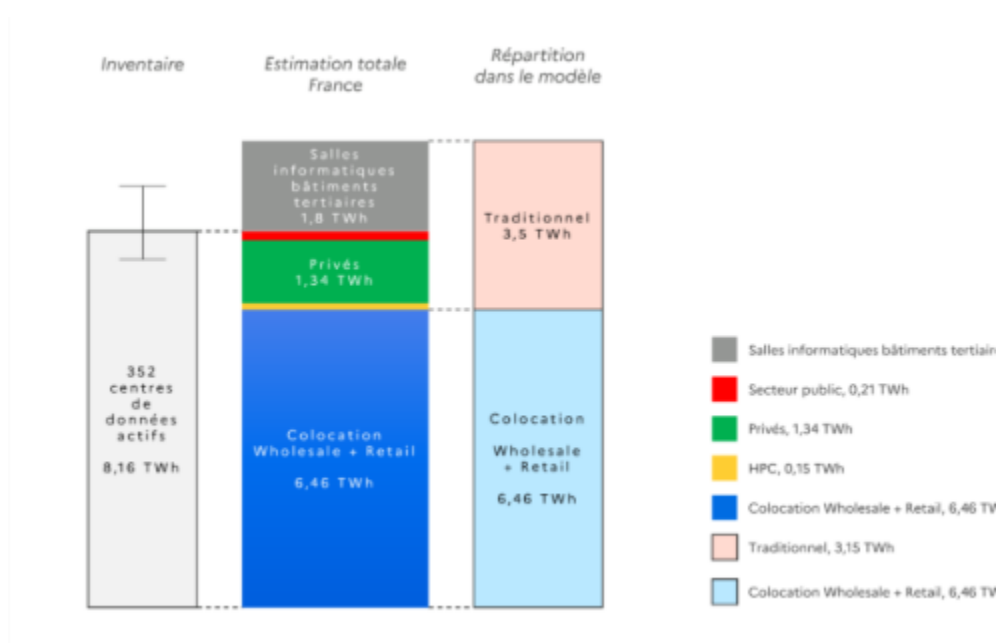
Source : Site internet Digital realty.

En ce qui concerne DataOne, l'audition de cet acteur par la commission d'enquête a révélé des enjeux de souveraineté. Data One construit et entretient les bâtiments, gère les raccordements physiques de l'accès aux données. En revanche, les racks informatiques et les GPU, c'est-à-dire la puissance de calcul, sont fournis par des clients. Dans son projet le plus avancé à Eybens, ce client est Core42, fonds d'investissement émirati. Core42 est un acteur immobilier, spécialisé dans les data centers. Il n'a aucun contrôle sur les acteurs qui utiliseront la puissance de calcul pour faire fonctionner ^([480]) : « Je peux suggérer à notre client de privilégier ce type d'acteurs plutôt que des hyperscalers ».

C. LA TRAJECTOIRE DE DÉVELOPPEMENT DES DATA CENTERS EST-ELLE SOUTENABLE EN FRANCE ?

La tendance actuelle des entreprises en France consiste à basculer leurs usages numériques de leurs locaux, vers des infrastructures de cloud.

Le travail de l'Agence de la transition écologique (Ademe) a permis d'identifier en 2024 8,16 térawattheures (TWh) d'électricité consommée ⁽⁴⁸¹⁾.



Source : ADEME

La consommation des data centers sur sites dédiés augmente régulièrement depuis 2019. Elle est alimentée par le réseau de transport d'électricité opéré par Réseau de transport d'électricité (RTE), 3 TWh sur la consommation électrique française. En outre, une large partie des usages numériques français est aujourd'hui délocalisée à l'étranger.

La forte croissance des projets aura des impacts structurels sur le système électrique français à moyen terme : les volumes d'électricité disponibles (incluant les capacités de production nationales et les importations d'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 permettra pas d'alimenter simultanément, sans conflit d'usage, la décarbonation des secteurs des transports, de l'industrie et du bâtiment, prioritaire, ainsi que le développement du secteur du numérique. Les scénarios prospectifs de RTE prévoient que, par ailleurs, tous les projets de data centers ayant réservé de la capacité ne se concrétiseront vraisemblablement pas. La 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 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 à 15 TWh à 2030, à un taux de concrétisation d'environ 60 % (4,3 GW) pour les projets ayant sécurisé un raccordement au réseau à l'horizon 2030. Elle suppose en outre un développement des data centers raccordés au réseau de distribution de moyenne et basse tension.

– la trajectoire de décarbonation lente correspond quant à elle à une augmentation de la consommation de 10 à 15 TWh à 2030, à un taux de concrétisation d'environ 60 % (4,3 GW) pour les projets ayant sécurisé un raccordement au réseau à l'horizon 2030. Elle suppose en outre un développement des data centers raccordés au réseau de distribution de moyenne et basse tension.

consommée en région Normandie était de 26,5 TWh en 2024.

Au regard des capacités de production électrique nationales, le risque de cannibalisation avoué par RTE tend actuellement à des niveaux élevés (entre 80 et 100 TWh par an), et ces volumes exportés sont nécessaires 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 sont estimées à 50 TWh à l'horizon 2050 en fonction de la concrétisation des projets. Elles sont soumises à des incertitudes liées à la technologie de l'IA générative et à la soutenabilité économique et environnementale des trajectoires.

2. Des problèmes locaux liés à des congestions du réseau, entraînant des conflits avec d'autres usages

Selon RTE, la situation est « *plutôt bien maîtrisée* » concernant la demande de puissance industrielle. La tendance à éviter les zones industrielles – autre source importante de demande potentielle – et à privilégier les grands gestionnaires de foncier industriel comme les autorités portuaires veillent à assurer une allocation efficace des capacités électriques. De plus, les grands sites « fast-track » (cf. *infra*) ont été définis également dans un souci de fluidité.

Cependant, dans certaines zones, les demandes de l'industrie et du numérique sont concurrentielles. M. Fabrice Coquio cite également le cas de la zone industrielle de Fos-sur-Mer : « *Enedis n'est pas satisfait par l'électricité immédiatement disponible sur le réseau, que ce soit en haute tension – pour les usages industriels – Enedis –, ce qui peut causer des encombrements et poser des problèmes d'attribution (...). Cela renvoie à la problématique de la décarbonation de certaines activités – je pense par exemple à la zone industrielle de Fos-sur-Mer – et à la nécessité d'électrification des usages.* »

En vertu de la règle du « premier arrivé, premier servi », ce sont les projets ayant réalisé leur raccordement qui bénéficient des capacités de raccordement existantes et évitent ainsi de devoir dépendre de la construction de nouvelles infrastructures. Les conséquences positives en termes de calendrier de mise à disposition de la connexion, les coûts de raccordement et 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 permet à l'État de donner la priorité à des projets dérogeant ainsi à l'ordre de la file d'attente établi par RTE. À la date donnée, l'ensemble des demandes de raccordement au réseau engendrent, pour au moins un des projets, un délai supérieur à cinq ans, RTE saisit le préfet de la région concernée, qui établit un nouvel ordre de priorité. Pour des data centers : s'il permet de hiérarchiser entre eux des projets industriels, il ne permet pas de prioriser les projets industriels et des projets de data center. En tout état de cause, ce dispositif s'éteindra au printemps 2025, à l'initiative du législateur.

En accord avec la Commission de régulation de l'énergie, RTE a organisé au premier trimestre 2024 une concertation proposant de faire évoluer la logique actuelle de « premier arrivé, premier servi » vers une logique de gestion des capacités. Les modalités concrètes de déclinaison de ce principe doivent maintenant être élaborées en concertation avec les acteurs du secteur. Cela contribuera encore à renforcer la place des *hyperscalers*, dans la mesure où leur avantage concurrentiel est renforcé. Ainsi dans son étude sur les enjeux concurrentiels liés à l'impact énergétique et environnemental des data centers, RTE *a analysé plusieurs comportements susceptibles de soulever des préoccupations au regard des règles de gestion des capacités, des barrières à l'entrée ou à l'expansion pour des acteurs de taille modeste, l'Autorité sera particulièrement vigilante à privilégier des acteurs les plus importants du secteur ne leur permettant de sécuriser des approvisionnements à long terme et des avantages.*

3. Le mix bas carbone français : un mauvais argument pour justifier l'accueil des data centers

a. Ne pas servir d'excuse au développement inconsideré de l'intelligence artificielle

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 « *ouvrir la conversation* » sur le recours à des énergies fossiles pour alimenter les data centers ^([483]).

Les développeurs de projet recourent de façon croissante à des contrats d'achat d'électricité directement auprès de producteurs d'énergie renouvelable, de façon à récupérer des « garanties d'origine » pour façon de justifier un bilan environnemental inattaquable, comme a pu le faire M. Coquio devant la cour de cassation *Digital Realty, la France est pionnière en matière environnementale. Depuis 2014, nous nous y fournissons en énergie verte – c'est également le cas de l'ensemble de nos data centers en Europe depuis 2021* ». Pourtant, les data centers comptabilisent la production renouvelable qu'à la maille mensuelle, et non à la maille horaire, et peuvent consommer de l'électricité carbonée venant du réseau durant certaines heures tout en étant couverts par la production renouvelable. L'impact environnemental des data centers devra donc s'appuyer sur des analyses fondées sur des données à 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 garanties d'origine à une maille horaire.

Ce type d'obligation est d'ores et déjà en vigueur pour les installations de production d'hydrogène. Comme l'indiquent les actes délégués de l'Union européenne relatifs à l'hydrogène renouvelable ^([484]), « *à moins que le système électrique ne soit essentiel de faire correspondre la demande d'électricité pour la production d'hydrogène à une production supplémentaire* ». La production d'hydrogène n'était pas accompagnée d'une production supplémentaire à partir de sources renouvelables. La production supplémentaire d'électricité des électrolyseurs risque d'entraîner une augmentation de la production d'électricité à partir de janvier 2030, tous les producteurs d'hydrogène renouvelable, y compris ceux qui ont signé avec des centres existants, devront avoir une production correspondant à l'électricité qu'ils ont achetée, sur une base horaire. Le déploiement des data centers un atout dans la décarbonation européenne plutôt qu'une menace.

b. La permanence d'autres sujets environnementaux majeurs

L'implantation des data centers en Europe s'accompagne d'obligations minimales en matière d'impacts environnementaux, et bientôt de performances, s'agissant :

– de la récupération de chaleur fatale : depuis 2024, les centres de données d'une puissance supérieure à 1 MW doivent récupérer la chaleur fatale de leurs équipements ; la Commission européenne publiera 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 de consommation d'eau des centres de données dans son enquête « Pour un numérique soutenable ». Depuis 2025, ces obligations s'appliqueront à l'ensemble des centres de données européens issus de la directive 2023/1791 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'impact environnemental (MRAE) d'Île-de-France sur le projet Campus IA, qui est un cas d'école pour les data centers de data center atteignant le gigawatt de puissance installée ^([485]) :

– la consommation de foncier, avec en particulier la destruction de terres agricoles dont les rendements, des conditions pédoclimatiques très favorables à l'ensemble des cultures ». Comme l'a souligné la Seine-et-Marne, lors de l'audition de M. Arthur Mensch, « *ce projet est colossal (...) parce qu'il détruit la Seine-et-Marne de façon importante. Il a déjà fait disparaître les champs de betteraves et de blé qu'on avait en place préventive effectuée actuellement des fouilles* ».

– la pollution atmosphérique liée au fonctionnement des générateurs de secours ; il s'agit de générateurs électrogènes, ce qui représente 4,6 MWth de puissance installée, soit davantage que le parc thermique de la région métropolitaine ^([486]). Dans un document de 2023, la MRAE réalise une synthèse des enjeux identifiés par les data centers. S'agissant des groupes électrogènes, elle met en valeur les risques de pollution en cas de panne.

La première est le soutien public marqué de la présidence de la République dans 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 directer centres. Ces investissements se répartissent de la façon suivante :

Acteur	Pays d'origine	Montant l'investissement annoncé (en Mds d'euros)
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, 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 part de nombreux éléments, MGX a signé un accord avec Microsoft pour l'investissement de 100 milliards de dollars. MGX a également participé aux levées de fonds d'OpenAI ^([491]) et d'Anthropic ^([492]). L'investissement de MGX s'inscrit dans le cadre d'un partenariat dans lequel sont aussi investisseurs BPIFrance et Mistral AI. Campus IA fait suite à un partenariat d'OpenAI aux États-Unis, formalisé en mai 2024 et matérialisé par un accord signé le 6 février 2025, qui vise à développer des infrastructures IA sur le site de Fouju. À l'occasion de Choose France, en juin 2026, une extension a été annoncée.

Lors du même sommet de juin 2026, d'autres projets ont fait l'objet d'annonces additionnelles :

– Brookfield (Canada) porte à 30 milliards d'euros ses investissements dans les infrastructures de données, le développement de nouveaux data centers et d'un écosystème industriel associé ;

– Nebius (Pays-Bas) reconvertit l'ancienne friche Bridgestone de Béthune en site majeur de données. En mars 2026, Nebius signait un accord avec Meta dans lequel cette dernière s'engage à contractualiser des services sur plusieurs sites pour un montant cumulé de 27 milliards de dollars ^([494]) ;

– Phoenix Group (Émirats arabes unis) développe des infrastructures numériques et de données, notamment dans la région lyonnaise ;

– SoftBank Group Corp. (Japon) annonce un vaste programme de centres de données décentralisés pour 100 milliards d'euros d'investissements. Le projet vise le déploiement en France d'infrastructures pouvant atteindre 100 milliards correspondant à un investissement de 75 milliards d'euros, dont 3,1 GW dans les Hauts-de-France et 10 milliards ;

– Verne et Ardian (Royaume-Uni / France) développeront en Île-de-France un campus numérique pour le calcul haute performance.

– simplifier et réduire les délais d’implantation : la DGE a notamment travaillé à l’élargissement 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 accompagnées
Union européenne	25	44 %
<i>Dont Française</i>	<i>21</i>	<i>35 %</i>
Hors Union Européenne	29	51 %
<i>Dont états-uniennes</i>	<i>14</i>	<i>25 %</i>
Indéterminée	3	5 %

Source : Réponse aux questionnaires de la rapporteure.

Soixante-cinq emplacements ont été identifiés par le gouvernement pour faciliter la recherche dans les régions dans lesquelles ces emplacements se situent. « *La task force datacenters, au travers de projets de présenter leurs cahiers des charges aux agences régionales de développement (ARD), travaille en étroite attache avec le porteur si un des sites répertoriés par l’ARD répond aux exigences du cahier des charges du 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 présence d’emprises foncières bien connectées aux grands réseaux de télécommunications. L’implantation des data centers ont été mis en valeur dans une vaste opération de marketing territorial. S’ajoute à ces efforts une perméabilité au lobbying des grandes entreprises du numérique dans les instances gouvernementales. L’implantation de data centers en France sera facilitée grâce à l’article 35 de la loi de simplification. Cette campagne importante du lobby des Big Tech ^([496]), le statut de projet national d’intérêt majeur ne sera pas en disposition, introduite par l’Assemblée nationale à l’initiative de Philippe Latombe, a été supprimée. L’objectif est donc de favoriser les investissements étrangers et non de renforcer la souveraineté européenne du numérique. Le déploiement du gouvernement au déploiement des data centers ne répond pas à l’impératif de souveraineté, et ne répond pas à l’intérêt public.

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 permet de répondre aux besoins des services d’intelligence artificielle. Le risque est l’accaparement de la production électrique nationale principalement par les *hyperscalers* ;

– Aucune hiérarchie n’a été faite entre les différents projets par type d’acteur. **La politique des data centers s’effectue tous azimuts, sans aucune prise en compte du profil des futurs exploitants** comme il a été expliqué plus haut. il conviendrait de favoriser des projets visant à dédier des capacités de production à des acteurs publics ou privés.

QUATRIÈME PARTIE : POUR UN NOUVEAU MODÈLE NUMÉRIQUE EN FI

CHAPITRE 13 – DES ALTERNATIVES ROBUSTES EXISTENT

Depuis des décennies, nous avons laissé s'installer la domination des Gafam sur le monde. Nous dressons 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'existe. Les autres acteurs ne seraient pas au niveau et parce que le numérique et ses effets de réseau exigent une approche globale pour le bien du consommateur.

Or de telles alternatives existent bel et bien, et elles permettent d'envisager des modèles différents de la domination des Gafam, avec une 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 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. La définition de logiciel libre publiée en février 1989 ⁽¹⁴⁹⁷⁾. Pour être qualifié de libre, un logiciel doit réunir quatre conditions : i) liberté 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 et de redistribuer le programme ; iv) liberté d'améliorer le programme et de publier ces améliorations.

Plusieurs types de licences peuvent être associées au logiciel libre. La licence « copyleft » garantit qu'un logiciel dérivé conserve le statut de logiciel libre de l'original. En choisissant une licence copyleft, on assure l'évolution possible de son travail sorte du domaine du libre.

Open source et logiciel libre sont des notions très semblables. Cependant, il est considéré que l'open source a une acception plus large, en désignant l'ensemble de l'approche, c'est-à-dire à la fois son approche technique et son éthique. 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 les vulnérabilités causées par l'adoption de solutions propriétaires.

Premier avantage, le logiciel libre est, par définition, exempt de tout risque de vendor lock-in. Les logiciels libres ont des codes sources ouverts, ce qui permet de vérifier que le code est utilisable sans restrictions, et qu'il peut être copié et adapté.

des exemples flagrants de projets libres qui fonctionnent avec des écosystèmes et une gouvernance particulier ».

Les leaders internationaux mettent en avant leur capacité à offrir une solution sur l'ensemble alternative à cette captation des infrastructures essentielles, comme en atteste l'exemple de Signal. Whittaker, indiquait devant la commission d'enquête : *« Cela étant, cette perspective ne répond pas à la question : se fait-il qu'un dispositif aussi vertueux et nécessaire que Signal ne constitue pas le modèle par défaut ? Cela implique un biais économique structurel et appelle d'autres interrogations, notamment sur les modalités de financement de l'infrastructure réellement indispensable (...) »*.

« Dans les années 1990, les conditions ont été réunies pour permettre à un nombre restreint d'acteurs de contrôler la logique de monopole et nous utilisons aujourd'hui leurs serveurs parce que cela est nécessaire pour disposer, pour notre part, des milliards de dollars annuels requis pour reproduire de telles infrastructures. Nous avons un chiffrement rigoureux qui garantit que, même en recourant aux serveurs de ces entreprises, ce n'est pas nous, puisque seul l'utilisateur détient les clés permettant d'accéder à ses communications sur Signal ». ⁽¹⁴⁾

Quatrième avantage, le logiciel libre est plus résilient puisqu'il ne dépend pas de son propriétaire expose à deux risques importants : le *kill switch*, restriction volontaire de la part de son propriétaire du produit pour des raisons économiques (faillite de l'entreprise, réorientation stratégique, etc.). Le risque de tels scénarios de se produire, ainsi que l'indique le directeur de la stratégie et de la culture numérique de Signal, M. Renaud Chaput, est *« une fois que Linux est installé sur mon serveur, il est à moi. Si demain la fondation coule, j'ai le droit de continuer à l'utiliser. C'est une alternative. Pour GitHub, c'est pareil : si la plateforme venait à disparaître, nous avons des copies de son code. C'est le principe de GitHub : synchroniser des machines en local avec le dépôt. Effectivement, ce n'est pas le même compte ailleurs, mais nous sommes capables de déplacer le code. Ce n'est pas du tout le même niveau de résilience »*.

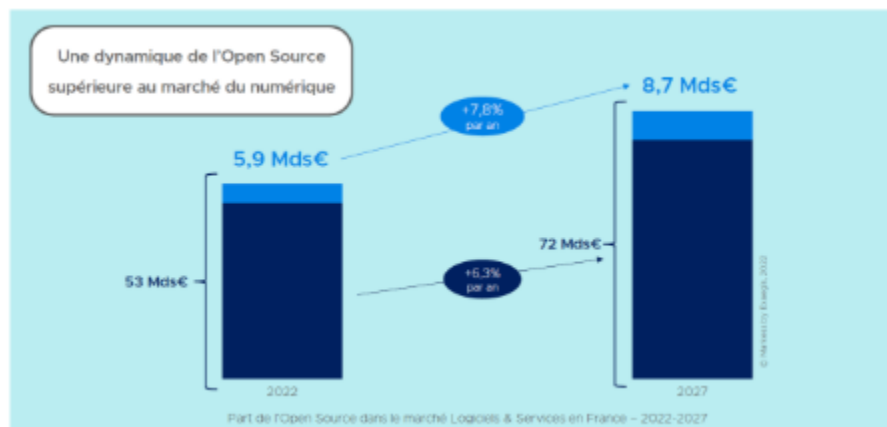
Cinquième avantage, les solutions techniques sont souvent de grande qualité, et maitrisées par leurs propriétaires. La preuve en est que les grands éditeurs de solutions se basent très largement sur ces solutions techniques sur leurs propres plateformes. M. Renaud Chaput en donne ainsi un exemple : *« La plateforme Azure de Microsoft est construite sur des logiciels libres ; ils y ont simplement apposé un logo et embauché des dizaines de milliers de développeurs pour le produit. Google Cloud et les services d'Amazon sont entièrement construits sur du logiciel libre »*. Signal, Mme Whittaker décrivait l'effet d'émulation créé par l'ouverture du code, qui incitait l'ensemble des acteurs à l'amélioration des solutions open source : *« Au cours des dix dernières années, nous avons acquis, par nos actions, une réputation qui nous place véritablement comme un étalon de référence. Cela signifie qu'un écosystème s'est construit autour de nous : nous ne nous limitons pas à publier du code dans une bibliothèque en ligne, mais nous avons gagné la confiance du public, non sur des opinions, mais sur des faits. Les hackers savent que, s'ils peuvent contribuer, ils trouveront un emploi chez nous »* ⁽¹⁵⁰²⁾.

La transition vers le libre peut ainsi être indolore pour les utilisateurs – *« il n'y a pas de résistance à l'adoption si vous leur proposez un logiciel meilleur que celui qu'ils utilisent »*, relève Nicolas Vivant. *« Signal est un projet d'Échirolles, ils vous diront qu'ils n'ont pas noté de grands changements. Pourtant, ces changements sont énormes : l'équipe, préparation budgétaire, reporting, monitoring, documentation, tout a changé. »* ⁽¹⁵⁰³⁾.

Sixième avantage, le code du logiciel libre est auditable par toute personne qui souhaite vérifier l'absence d'insertion de fonctionnalités cachées. Tout utilisateur pourra ainsi vérifier les risques liés à l'absence de fondement même de la politique de Signal, dont le caractère open source des solutions est la manifestation. Les politiques en vue de l'introduction de *« backdoors »* : *« Pour nous, la communication privée est un droit fondamental et une vie pleine de sens ne sont pas possibles. Nous existons pour protéger ce droit et nous nous engageons à utiliser du logiciel et des protocoles open source qui sont essentiels à la protection de la vie privée. (...) Pour nous, des arguments convaincants, mais cela demeure insuffisant lorsqu'il est question d'un élément aussi fondamental que la vie privée et valider par soi-même, en accédant aux fondements techniques. (...) Ainsi, il n'est nul besoin de nous faire confiance, pas mon objectif, car toutes les preuves sont accessibles »*.

Markess en 2022 ^([505]). Cette étude apporte des éléments d'éclairage importants sur la taille du marché et sa dynamique, en 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 – représente 11 % du marché total des logiciels et services numériques. Le marché est en croissance de 7,8 % par an (+ 6,3 % par an). L'open source représentait 63 800 équivalents temps plein en 2022.

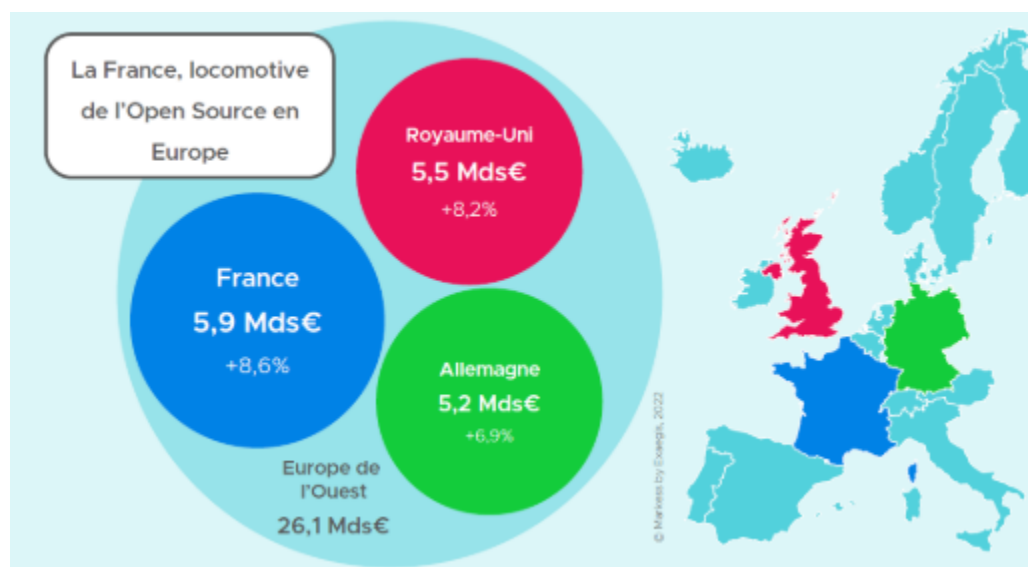


Source : Markess.

Fait intéressant, l'étude relève que les services de cloud open source IaaS et PaaS sont en croissance de 21 % des services dans l'open source en 2027, soit un volume d'affaires de 1,7 milliard d'euros. *Les technologies open source sont à la base de nombreux services cloud vendus. Parmi elles, CloudWatch pour le monitoring et les plateformes de gestion des services Cloud, Keycloak pour la gestion des identités, MongoDB et MariaDB pour les bases de données. Parse pour les solutions serverless promises à 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 l'ensemble des besoins. Elle anticipe une très forte croissance de l'activité dans le domaine de l'intelligence artificielle.

Enfin, l'étude positionne la filière française de l'open source par rapport à ses homologues européens. Elle occupe 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 de l'open source au PIB européen ^([506]). Là encore, les conclusions montrent que cette filière est d'ores et déjà un secteur clé de l'économie numérique.

Tout d'abord, le développement des briques et produits open source repose sur les constituer un risque pour la pérennité des produits. Comme le relève M. Gosset, « *Nous sommes logicien logiciel libre : le financement de la maintenance. C'est bien d'avoir un logiciel qui sort en 2026, mais qui ne fonctionne plus en 2027, en 2028 et au-delà ?* » Une rupture de continuité dans la maintenance, en l'absence de changement de gouvernance, peuvent constituer de graves vulnérabilités pour l'ensemble de l'écosystème, comme expliqué M. Renaud Chaput. *Des failles de sécurité et des bugs apparaissent, nécessitant des corrections de volontaires qui maintiennent des logiciels libres très spécifiques mais omniprésents dans nos téléphones. Une faille a été découverte dans une bibliothèque logicielle gérée par une seule personne sur son temps libre dans le monde entier. Cette personne a rappelé que, malgré l'utilisation massive de son travail, elle n'est pas financée.* » ⁽⁵⁰⁸⁾

Rendre le logiciel ergonomique et facile d'accès nécessite, en outre, un engagement significatif et toujours les moyens. Pour M. Chaput, « *la vraie difficulté pour beaucoup de logiciels libres est que ce n'est pas un métier. Énormément de logiciels libres ont été initiés par des passionnés, qui ont peut-être trouvé d'autres projets en plus de leur travail. Chez Mastodon, nous nous sommes rendu compte que pour créer un logiciel, on est au point que l'on oublie que c'en est un, qui n'est pas « moche » et qui marche mieux que les autres logiciels. Les personnes qui y travaillent à temps plein. C'est un effort constant. Nous avons récemment lancé un logiciel simple, mais qui a nécessité neuf mois de travail pour deux personnes afin d'atteindre cette simplicité. Beaucoup de logiciels libres ont du mal à atteindre, car ils sont souvent développés par des personnes bénévoles 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 libres, éditeurs de logiciels, soit sur leurs fonds propres en avance de phase, soit pour répondre directement à une problématique pour l'open source est de pouvoir trouver des développeurs à même de répondre à des besoins de façon vertueuse, sans que les premiers ne supportent un coût démesuré, ce qui suppose de mutualiser les efforts en open source.

M. Chaput soulignait ainsi la difficulté à faire porter à des petites collectivités le coût du développement territorial. « *J'ajoute qu'au niveau des coûts, il y a une vraie question de mutualisation. Lorsqu'un logiciel a s'il n'a que trois clients, ses coûts fixes sont probablement les mêmes à 90 % que s'il en avait deux ou trois. Je pense que c'est vrai pour tous les logiciels libres : un des avantages des géants du numérique est justement l'automatisation massive qui leur permet d'opérer pour des millions de clients avec un nombre très limité de développeurs. Ce qui est le fruit d'années d'investissements se chiffrant en centaines de millions ou en milliards de dollars. Dans la fonction publique américaine, qui ont amené ces géants à une taille telle que leurs coûts de revient deviennent très faibles. L'informatique : on peut automatiser beaucoup de choses, mais la mise en place de cette automatisation est aux très petites structures qui sont les premières à se lancer dans la suite territoriale de financer le développement, c'est un peu leur faire supporter le coût de rattrapage de dix, quinze ou vingt ans de retard sur la concurrence réelle.* »

L'objectif est donc de parvenir à un équilibre entre contributions individuelles et collectives, et administrations, de façon à maintenir le code dans la durée. M. Pierre-Yves Gosset, coordinateur de l'association, défend un tel engagement ⁽⁵⁰⁹⁾ : « *Si l'on considère le logiciel libre comme un produit sur étagère qui se vend tout seul, la vraie difficulté est de passer d'une stratégie de consommation à une stratégie de contribution. Cela ne se fait pas sans travailler dessus, sans le maîtriser, cela ne fonctionnera pas (...). Il faut contribuer à ce code. Dans les administrations ou les entreprises, on constate une grande difficulté à opérer cette bascule. On dit : je ne vais pas contribuer en plus. Si le discours était : « vous n'avez peut-être pas payé le logiciel, mais vous faites des améliorations pour le bien commun et l'intérêt général », je pense que nous aurions déjà franchi un pas.* »

une déclaration d'intérêt fondée sur ces communs numériques. » ([511]).

Tout en saluant l'initiative qu'il a contribué à porter, M. Henri Verdier a regretté que « *modestes, de l'ordre de quelques millions d'euros* ». Pour Mme Ophélie Coelho, si ce type de projet de standards communs, il pâtit du manque de coordination entre États membres et de la lenteur des *des acteurs et des intérêts au sein de l'Union* ». : « *Les projets sont toujours très intéressants communiquent pas suffisamment entre eux. J'ai eu l'occasion de discuter avec certains responsables. C'est regrettable, car plusieurs Edic sont compatibles entre eux ou avec d'autres projets européens des couches technologiques déjà développées ailleurs. Je me demande parfois s'il ne faudrait pas recherche nucléaire (Cern) du numérique, qui rassemblerait la recherche, les choix stratégiques de Nous avons un vrai problème de cohérence. La politique industrielle de l'Europe, si tant est qu'il manque de cohésion d'ensemble.* » ([512])

Une généralisation de ce type de financement serait conforme au principe « *public 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
Comme le souligne M. Renaud Chaput, il est essentiel que, « *lorsqu'une ville, une entreprise ou un 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 comme l'a expliqué M. Nicolas Vivant : « *Un passage au logiciel libre ne consiste pas simplement c'est un nouveau paradigme, un nouveau projet, une nouvelle façon de travailler, et donc un changement informatique est une équipe avec des compétences techniques, des équilibres et des habitudes de travail. Quand les compétences, parfois durement acquises, reposent sur des logiciels propriétaires, et que l'un changement de cap induit forcément des bouleversements qu'il ne faut pas négliger. Tenter de combler 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 talents qui disposaient des compétences attendues et d'une appétence pour le logiciel libre, par une recherche

Le profil de compétences des personnels constitue bien un élément clé. Le directeur du Le Baron, a mis en avant cet atout : « *La culture du logiciel libre est intrinsèquement liée aux ressources domaine dans lequel les ministères ne sont pas tous égaux. Il se trouve que nos trois ministères prioritaires, car nous figurons parmi les quelques grands ministères à bénéficier de corps de fonctionnaires sein du ministère de l'éducation nationale, par exemple, nous nous appuyons sur le corps des ITRF (de formation), dont une partie possède une expertise numérique. Nous disposons donc d'un grand nombre de personnes qualifiées, qui se maintiennent à niveau sur ces questions. Nombre d'entre eux ont été formés très tôt à l'utilisation de technologies libres. Par conséquent, cette culture du libre est profondément ancrée dans présente dans leurs pratiques* » ([513]).

ii. Pour une contribution des agents publics aux communs

Au-delà du soutien financier, les administrations peuvent contribuer directement aux communs : la gendarmerie nationale, qui participe à la communauté du libre, et du ministère de l'éducation nationale les outils pédagogiques reposant sur des logiciels libres, et met à leur disposition une forge logicielle commune.

La politique en faveur des communs numériques éducatifs a été exposée par M. Audran Le

Recommandation n° 15 : Permettre aux agents de l'État de contribuer, l'équivalent d'une journée par an, dans une logique d'intérêt général (exemple : Forge des communs numériques, Grist, Debian, Wikipedia, et
Une telle mesure permettra de renforcer la contribution des administrations aux communautés développant des connaissances détenues par les agents publics, et de favoriser la connaissance des logiciels libres au sein des per

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 une République numérique du 7 octobre 2016, en son article 16, prévoit que les administrations « *assurent la pérennité et l'indépendance de leurs systèmes d'information. Elles encouragent l'utilisation des logiciels libres, le développement, de l'achat ou de l'utilisation, de tout ou partie de ces systèmes d'information* ». Bien que 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 le logiciel libre – étudier, modifier ou faire modifier, et partager – répondent à des impératifs d'intérêt général (l'équipement), alors une administration qui, dans son appel d'offres, choisit de se priver de l'une de ces options au profit d'autres intérêts contradictoires de même valeur, selon un principe de proportionnalité somme toute*

L'orientation de la commande publique vers les logiciels libres est limitée par plusieurs facteurs. On rencontre les communes pour mutualiser leurs investissements dans le cadre actuel ; l'impossibilité de l'installation de logiciels libres sur le budget d'investissement, qui pourrait être amorti sur plusieurs années. La procédure des marchés publics favorise souvent les gros groupes, au détriment des petits acteurs.

Sur ce dernier point, des instruments juridiques ont été créés pour favoriser le développement des petites entreprises, tels que le partenariat d'innovation prévu par l'article 31 de la directive 2014/24/UE.

La Centrale d'achat de l'informatique hospitalière (CAIH), s'est emparée du dispositif. Elle vise à mettre en place pour un partenariat d'innovation visant à concevoir, expérimenter et industrialiser une suite logicielle 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 des 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), dans une démarche offensive en matière de souveraineté, nous avons conclu un partenariat d'innovation. Nous ne faisons pas de choix technologique en amont ; un industriel nous accompagne dans la conception, l'assemblage de briques open source, qui doit tenir compte des spécificités du domaine de la santé. HospiConnect –, son déploiement et le support. Nous avons également été accompagnés par un avocat en matière numérique qui nous aide à privilégier des industriels français, que ce soit pour les briques de résilience*

« *Au terme de ce travail interne de conception qui a duré six mois, nous avons lancé le processus de sélection pour franchir différentes étapes. Après avoir reçu neuf candidatures, nous avons retenu les trois industriels les plus pertinents. En juin, nous choisirons celui d'entre eux qui nous accompagnera. Celui-ci travaillera ensuite en partenariat avec les autres candidats, à la construction du produit. L'intérêt de ce type de marché est qu'au terme du processus, dans un an, nous pourrions le renouveler en chargeant, le cas échéant, un autre industriel de déployer et d'accompagner la communauté hospitalière. Nous avons tout intérêt à ce que d'autres acteurs saisissent l'opportunité de ces technologies 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

d. Prévenir l'appropriation par les Big Tech

B. LA NÉCESSAIRE GÉNÉRALISATION DES STANDARDS OUVERTS

Les logiciels open source se développent sur des standards ouverts, qui sont aujourd'hui sur le marché. Le renforcement des obligations d'interopérabilité constitue le second levier essentiel pour les 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 informations soient renseignées selon des formats communs, à l'aide de protocoles partagés et des interfaces (API) sur lesquelles il est possible de se connecter.

Les standards ouverts permettent de **lutter contre les positions monopolistiques des Big Tech** qui ne puissent les concurrencer en proposant leurs produits. L'Autorité de la concurrence a souligné *la standardisation comme l'imposition d'obligations d'interopérabilité au titre de la régulation sectorielle, la transparence et la contestabilité des marchés du secteur numérique, protéger et promouvoir l'innovation, permettre aux utilisateurs à changer de fournisseurs de services et à se tourner vers les fournisseurs qui répondent à 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**. *Les petits acteurs européens très compétents pouvaient se connecter et proposer leurs services, cela permettrait de casser la capacité de contrôle, observe Alexandra Lutz. Il faut rappeler qu'au niveau européen, 99 % des entreprises sont petites et moyennes, il faut soutenir, plutôt que de tout miser sur quelques géants ». Comme le confirme Mme Francesca M. « chacun peut contribuer selon ses capacités et ses disponibilités ». L'interopérabilité permet aussi de réduire la peur de manquer quelque chose, qui pousse à rester sur les plateformes concentrant le plus grand nombre d'utilisateurs possible, demain, de quitter Instagram pour rejoindre Mastodon tout en continuant à suivre des comptes*.

De plus, l'interopérabilité **présente l'avantage de permettre l'intégration de solutions** aux besoins des utilisateurs. Les standards ouverts proposent de fait une alternative à l'écosystème propriétaire **fédérée et décentralisée** qui préserverait la qualité de l'expérience utilisateur. Le directeur de recherche souligne le potentiel à travers l'exemple du réseau social Mastodon : *« Au lieu d'utiliser une grosse machine centralisée, l'ensemble des utilisateurs et des données, vous pouvez avoir 10 000 machines détenues par autant de personnes, ainsi, par exemple. Comme les machines utilisent les mêmes protocoles, les utilisateurs peuvent discuter entre eux de cet ancien monde, fondé sur des colonies numériques dans lesquelles un grand acteur refuse la participation des utilisateurs, et changer de paradigme pour aller vers des écosystèmes numériques reposant sur des plateformes décentralisées »*.

Cette interopérabilité est vectrice de **résilience**, puisqu'en cas de défaillance ou d'indisponibilité, les utilisateurs peuvent reporter les usages sur les autres et d'assurer la continuité de l'activité, là où la monoculture et la dépendance créent un risque systémique. M. Nicolas Vivant a salué la grande solidité de ces infrastructures ouvertes : *« Le serveur plante, cela ne plantera pas Mastodon. La messagerie utilisée par l'État, Tchap, sur laquelle reposent les services aux collectivités, repose sur la même architecture distribuée. Si demain Tchap tombe, les collectivités pourront continuer à fonctionner. Seules les solutions libres et fédérées permettent ce niveau de résilience. Cette décentralisation (réseau IP européen) sur la résilience de l'internet en Ukraine en situation de guerre a montré que l'interopérabilité est essentielle. Parce qu'en Ukraine, il n'y a pas quatre grands opérateurs, mais des dizaines de milliers de petits opérateurs, il est impossible de détruire l'infrastructure internet globale du pays. »*

Enfin, une architecture décentralisée favorise un **modèle économique plus respectueux de l'environnement et de la démocratie**, dans lequel les utilisateurs pourront exercer leur liberté de choix pour peser sur les décisions. M. Bastien Le Querrec, juriste à La Quadrature du net, *« un tel cadre favoriserait l'émergence de solutions alternatives, françaises et européennes, qui pourraient, au sein de cet écosystème de réseaux sociaux interopérables, offrir une alternative viable à la domination des géants »*.

En matière de cloud, le règlement européen sur les données du 22 décembre 2023 (Data Act) vise à garantir l'accès des données à leur fournisseur et à favoriser le recours au multi-cloud en imposant des obligations de portabilité applicables depuis le 12 septembre 2025. La Commission européenne est habilitée à adopter des mesures d'interopérabilité.

Certaines mesures ont été introduites par anticipation en droit français par la loi Sren de 2023, article 28, que les fournisseurs de services cloud assurent leur interopérabilité avec les services d'autre fournisseurs numériques entre les deux offres. Pour ce faire, ils sont tenus de mettre à disposition des API et des interfaces permettant à des services tiers de communiquer avec leurs services. L'Arcep est chargée de vérifier le respect de ces modalités par l'édition de spécifications d'interopérabilité et de portabilité. Dans ses recommandations, elle a recommandé des bonnes pratiques de transparence et de stabilité des API, tout en promouvant l'adoption de standards, mais il est cependant encore trop tôt pour en dresser le bilan, compte tenu du calendrier d'application du Data Act aux fournisseurs.

Des obligations de ce type ont également été instituées en droit de la concurrence. Conformément à l'article 101 du TFUE, les 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 fournisseurs de matériels et logiciels contrôlés par le système d'exploitation. Le 19 mars 2025, la Commission a adopté des décisions visant à préciser les obligations d'Apple pour améliorer la connectivité des appareils et certaines fonctionnalités de l'iPhone, et renforcer l'efficacité et la transparence du traitement des données par Apple. La Commission a également ouvert, en janvier 2026, une procédure pour vérifier que Google respecte les obligations limitant l'accès des fournisseurs tiers de services d'intelligence artificielle aux fonctionnalités d'Android.

L'article 7 édicte une obligation d'interopérabilité horizontale spécifique pour leurs services de messagerie. Les contrôleurs d'accès de fournir sur demande et gratuitement les interfaces techniques nécessaires. L'objectif de cette œuvre est cette interopérabilité s'agissant des conversations individuelles, et de deux ans pour les conversations de groupe. Seulement deux fournisseurs de services de messagerie, BirdyChat et Haiket, ont annoncé, en 2025, être interopérables avec WhatsApp au cours de l'année 2026 ⁽⁵²¹⁾.

M. Umberto Berkani a reconnu que le « *DMA constitue à cet égard un premier élément de son œuvre, d'ailleurs, dans ses rapports, des avancées concrètes en termes d'interopérabilité, de portabilité des données des clients. Il est toutefois prématuré d'en mesurer pleinement les effets puisque, comme tout texte nouveau, il s'agit d'entreprises visées, et il faudra attendre que cette pratique soit validée par les cours de justice.* » ⁽⁵²²⁾

Si l'article 53 du DMA prévoit que la Commission européenne doit évaluer à échéance régulière l'impact de l'interopérabilité aux réseaux sociaux, ce n'est toujours pas le cas aujourd'hui. Le droit à la portabilité des données RGPD peut s'en trouver limité, faute d'interfaces techniques.

Dans certains cas, ces verrous techniques sont délibérément mis en place par les plateformes. Chavalarias s'agissant de X ⁽⁵²³⁾ : « *Certains volets du RGPD, concernant, notamment, la portabilité des données, ont permis aux utilisateurs de réclamer leurs archives sur X afin d'utiliser OpenPortability dans d'autres services. Néanmoins, nous n'en sommes pas encore à la portabilité effective des données. Dans le cas de X, les données ont été supprimées. À l'époque de Twitter, des API (Application Programming Interfaces, interfaces de programmation) efficaces permettaient de transférer les données d'une plateforme à une autre. Elles ont été délibérément supprimées pour empêcher la portabilité effective des données qui existait du temps de Twitter* ».

Pour permettre aux utilisateurs qui le souhaitent de quitter X, le chercheur a conduit une étude et mis à disposition un dispositif technique de portabilité des données. Le dispositif a été utilisé par plusieurs milliers d'utilisateurs, témoignant du fait que « la société civile est en attente d'une solution de ce type ». Relatant les résultats de l'étude, il conclut que « la société civile est en attente d'une solution de ce type ».

numérique, fondée sur des protocoles de standards ouverts et pilotée par la banque centrale, est désormais bancaire national. Les bénéfices de cette politique sont multiples. Outre l'autonomie stratégique, elle représente 3 à 5 % de commissions autrefois captés par les acteurs américains. Cette somme, qui représente pour la France dans les poches des consommateurs et des entreprises brésiliennes. Surtout, PIX brise le monopole du traitement des données. (...) Ce succès repose sur la vision systémique de la Banque centrale, l'Union européenne. En 2020, elle a ainsi su identifier le risque posé par le lancement concomitant de WhatsApp Payments. Si Meta aurait pu étouffer PIX, elle a imposé un délai au service de WhatsApp au nom de la protection des données » ([526]).

L'État devrait également reprendre le contrôle sur la définition des standards techniques et le fonctionnement d'internet. Comme l'a expliqué Mme Francesca Musiani, « sur la couche de l'internet, traditionnellement plus distribuée, avec des organisations comme l'Internet Corporation for Assigned Names and Numbers (ICANN) ou l'Internet Engineering Task Force (IETF) qui élabore les standards techniques. Dans ces espaces, certains acteurs disposent de fait d'une capacité d'influence supérieure, liée à des ressources humaines et économiques. (...) Les acteurs qui participent à l'élaboration des protocoles au sein de l'internet imposent des standards de fait, comme Google avec le protocole QUIC, contribuent à définir les règles et les niveaux de sécurité. »

Il s'agirait pour l'État de favoriser la consolidation de standards interopérables : « Si l'on veut favoriser la bureautique, et que l'on s'assure que les formats ouverts comme l'open document format de la libre et hégémoniques, on garantit que toute nouvelle solution devra se conformer à ce standard. C'est aussi un enjeu qui dépend pas uniquement de logiques de profit, mais de quelque chose que l'on maîtrise collectivement. »

La commande publique constitue à cet égard un levier majeur. **Le gouvernement allemand a lancé le Deutschland-Stack, qui vise à fournir un socle technologique commun de briques open source aux Länder et les communes.** Elle couvre à la fois les infrastructures (centres de données, serveurs, logiciels, données, logiciels, modèles d'IA), et les applications. Pour y parvenir, l'IT-Planungsrat, le Conseil national des normes strictes imposant des interfaces ouvertes et des formats harmonisés à l'ensemble des acteurs. L'obligation faite aux acheteurs publics de recourir au format ouvert ODF pourrait notamment renforcer l'écosystème, précise M. Etienne Gonnu : « Si toute la puissance publique utilise et impose ce format, on va quitter Microsoft, car n'importe qui d'autre peut proposer une alternative compatible. On réduit la dépendance. Ça ne résout pas tout d'un coup de baguette magique, mais cela crée de l'offre par la demande. Quand on regarde 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 les acteurs. Dans tout le sens de l'initiative **Open Interop** lancée par le comité stratégique de filière Logiciels Numériques présentée par le président du CSF M. Michel Paulin lors de son audition. Elle a pour ambition de fédérer les composants open source pour établir un socle technologique commun, avec des API fédérées, et pour améliorer une meilleure interopérabilité. Cette approche, soutenue par l'État, doit permettre de mieux articuler les offres du marché, en garantissant la liberté de choix des ministères. Mme Stéphanie Schaer a souligné l'interopérabilité : les agents publics amenés à travailler avec ces différents outils doivent pouvoir facilement passer de l'un à l'autre ».

La rapporteure relève que la France dispose déjà d'un référentiel général d'interopérabilité qui regroupe des répertoires de données, de normes et de standards, tel que le prévoit l'article 11 de l'ordonnance n° 2016-161 du 12 février 2016. La dernière mise à jour du référentiel est intervenue en 2016. À cet égard, M. Loïc Dayot a appelé à compléter et devenir contraignantes : « Actuellement, des commandes publiques qui ne respectent pas les critères d'accessibilité, d'interopérabilité, de sécurité ou de sobriété peuvent encore être passées, ce qui est intéressant de les renforcer. Pour les données personnelles, la Commission nationale de l'informatique et des libertés n'a sans doute pas assez de moyens, mais sa présence envoie un signal. Nous devons renforcer la Commission nationale de l'informatique et des libertés. »

elle démontre, »
« – de bonnes pratiques (...) sont adoptées par le producteur, le fournisseur et le environnementaux du service utilisant un algorithme d’IA ;

« – les usages et les besoins visent à rester dans les limites planétaires et ont été préalablement

Elle met l’accent sur la mesure de l’adéquation des outils d’IA aux besoins réels des utilisateurs

L’AI Act ne contient aucune disposition contraignante sur le sujet de la performance. Les obligations sont celles prévues par le point 2 d) de l’annexe XI relative à la documentation technique. L’usage général, qui prévoit que ces derniers doivent communiquer des informations concernant « l’estimée du modèle ». Dans le code de bonne pratique publié par le bureau de l’IA ^([529]), et dont l’objectif est de permettre aux modèles à se conformer à l’AI Act, le formulaire à remplir dans le cadre du chapitre relatif à la transparence et au calcul de la consommation d’énergie des modèles, reproduite ci-dessous :

Energy consumption (during training and inference)	
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. 1.0x10 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. <i>[Recommended 100 words]</i>
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. 5.1x10 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 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 on the model, namely computational resources used for inference.

Les informations demandées sont particulièrement légères (taille de 100 mots recommandée). Les fournisseurs concernant les méthodologies de calcul. Dans son avis sur les enjeux concurrentiels liés à l’IA, l’Autorité de la concurrence mettait ainsi en valeur les risques d’information trompeuse et les pratiques anticoncurrentielles ^([530]) : « des acteurs peuvent être tentés d’adopter des comportements trompeurs dans une telle situation pourrait notamment se produire lorsque la frugalité ou l’empreinte environnementale d’une méthodologie robuste en termes scientifiques. Ainsi, un ou plusieurs acteurs pourraient, individuellement ou collectivement, adopter une frugalité ou plus précisément encore l’impact environnemental faible ou mesuré de leurs solutions afin de se faire passer pour une solution erronée. Que le caractère trompeur de cette caractéristique soit volontaire ou non, elle pourrait s’appliquer à des pratiques anticoncurrentielles (abus de domination ou entente) soit parce qu’il peut porter directement préjudice à la concurrence, soit permettre de bénéficier d’avantages concurrentiels, comme l’octroi de conditions avantageuses pour l’achat. À l’égard, l’Autorité appelle les pouvoirs publics à être particulièrement vigilants dans la fixation et la mise en œuvre des 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 ouverte en avril 2026 et est désormais clôturée ^([531]). À ce stade :

– les obligations ne portent que sur les informations à divulguer. La consultation sur la performance », sans que leur caractère obligatoire ne soit précisé.

« – 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. 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 : les données nécessaires à l'entraînement des modèles. La définition retenue **n'exige pas la publication des données** de l'OSI, « Certaines personnes estiment qu'un accès total et sans restriction à toutes les données d'entraînement est primordial, arguant que toute restriction compromettrait la reproductibilité totale des systèmes d'IA, et que cette approche relèguerait l'IA open source à une niche ne pouvant être entraînée que sur des données publiques. Cette même approche par rapport à celle occupée par l'open source dans l'écosystème logiciel traditionnel. Les communautés conservent la même approche que celle présente dans l'OSD ; elles n'imposent pas une reproductibilité totale, mais rendent possibles (approche de la reconstruction reproductible) ». Exiger la publication de l'ensemble des données d'office les modèles entraînés sur la base de données privées, même acquises légalement, et de données d'exemple, données personnelles de santé). C'est pourquoi le choix a été fait de ne pas exiger la publication des données. L'OSAID 1.0 est la **reconstruction reproductible**, c'est-à-dire la capacité pour quiconque à partir de l'ensemble des informations données sur les méthodes et données d'entrée.

Parmi les institutions opposées aux choix réalisés par l'OSI, la *Free Software Foundation* et son directeur, Bradley M. Kühn, a publié les commentaires suivants ^([535]) : « Le processus d'élaboration de l'OSAID est polémique, et cet article de blog ne résume pas l'ensemble des critiques formulées par la communauté. Le processus d'élaboration. D'autres blogueurs et la presse se sont déjà penchés sur ces questions. La solution la plus simple : l'OSAID n'exige pas que le public puisse reproduire le processus scientifique de développement des modèles. D'exigences suffisantes en matière de licence et de divulgation publique des ensembles de données d'entraînement. « open source ». L'OSI a refusé d'ajouter cette exigence en raison d'une faille fondamentale dans la définition de l'open source : inutile de publier une définition à laquelle aucun système d'IA existant ne pouvait actuellement se conformer. Cela sapé le processus communautaire et amplifié le rôle des parties prenantes qui tireraient un avantage de la définition de l'OSI selon laquelle leurs systèmes sont « open source ». L'OSI aurait dû s'abstenir de publier une définition et qualifier ce document de « recommandations » provisoires (...). OSI a également privé les utilisateurs de leur voix dans ce processus. Les militants du logiciel libre devraient s'engager dans des discussions plus larges avec les créateurs de contenu pour savoir ce que signifie pour eux le terme « open source », et ce qu'ils pensent de la publication des ensembles d'apprentissage de ces systèmes tiers. La frontière entre les données et le code est si floue que nous ne pouvons plus nous fier aux vieilles conclusions toutes faites selon lesquelles « les données sont le code » (voire indisponibles), tandis que le système reste « open source ». Cet adage ne tient pas la route dans la technologie, et nous devons avancer avec prudence — en nous affranchissant des intérêts commerciaux — pour l'engouement pour l'IA — pour déterminer comment nos philosophies bien établies s'appliquent à ce domaine. »

Ces débats montrent bien l'enjeu que revêt la publication des données pour l'entraînement des modèles. Nous avons 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 les modèles « publiés dans le cadre d'une licence libre et ouverte permettant de consulter, d'utiliser, de modifier les paramètres, y compris les poids, les informations sur l'architecture du modèle et les informations de formation publiques ».

précisions supplémentaires sont requises concernant ces ensembles de données, y compris la divulgation (tels que définis dans le formulaire), conformément au considérant 107 de l'IA Act ». Ainsi, il est symptomatique d'autant plus fortes que les jeux de données sont publics, alors que les fournisseurs ont la possibilité sur les jeux de données privés utilisés.

La notice explicative précise en outre : « *Les informations demandées dans le formulaire sont narratives, simples et efficaces. Le modèle vise à garantir que les informations communiquées soient utiles pour les parties concernées, tout en évitant d'imposer un fardeau inutile aux fournisseurs de modèles de PME* ». Le bureau de l'IA invoque ici une exigence d'informer le grand public sur les modèles de données à être utilisées par les professionnels en mesure d'utiliser, analyser et reproduire les modèles (« *burden* ») est d'ailleurs extrêmement révélateur.

À titre de comparaison, l'OSAID 1.0, dont on a vu précédemment qu'elle avait été critiquée pour son approche permissive, précise que, pour être qualifiées de « suffisamment détaillées », les informations doivent contenir les critères suivants : « *(1) la description complète de toutes les données utilisées (échantillon) les données non partageables, précisant la provenance des données, leur périmètre et leur durée, comment elles ont été obtenues et sélectionnées, les procédures d'étiquetage, ainsi que les méthodologies de traitement, la liste de toutes les données d'entraînement accessibles au public et des sources où les obtenir, et 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 transparence définie par l'OSI. Tous les modèles auto-labellisés « open source » ne le sont pas en réalité (voir annexe 1), ce qui donne 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. Cette recommandation devra faire l'objet d'actions au niveau français, vers les fournisseurs de modèles, mais aussi 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, notamment endossée par le pôle open source de la Dinum, par le Conseil national du logiciel libre, et il convient de poursuivre le combat pour la transparence sur les données d'entraînement.

– 1 –

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 question. Cette situation est une menace pour la démocratie, notre économie, nos droits et notre santé.

d'euros, dont 1 milliard de coût de licences qui pourraient être économisés grâce à l'utilisation de logiciels open source. De nombreux verrous techniques et commerciaux, leurs propriétaires peuvent augmenter leurs prix et basculer vers la concurrence.

Cette domination passe par la conquête de l'ensemble de la stack technique, des infrastructures (clouds, réseaux internationaux, data centers) aux terminaux et aux applications à destination des particuliers. La maîtrise de la chaîne de produits, ou encore la discrimination des offres concurrentes sur les plateformes généralistes, des pratiques répréhensibles, qui ont donné lieu à 17 milliards d'euros de sanctions au titre du droit de concurrence, seul Google.

Danger géopolitique permanent. Il y a d'abord la vulnérabilité des données qui sont stockées par des entreprises multinationales, y compris sur notre sol. Lorsqu'elles le peuvent, les entreprises dont le siège est aux États-Unis répondront aux injonctions des juges américains. Et quand bien même des dispositifs techniques pourraient être mis en place – ce qui reste à démontrer –, les solutions hybrides, reposant sur des technologies américaines, pourraient être mises à disposition quelques jours à quelques mois en cas de *kill switch*. Enfin, la dépendance aux outils numériques exerce une pression sur les décideurs politiques.

Ainsi que le résumait Henri Verdier, « *nous avons tout sous les yeux : l'affaire du juge américain qui a fait débrancher des serveurs, des dominations sur des segments entiers de l'économie, des régulations, et pourtant, les choses ne bougent pas beaucoup* ».

Avec l'intelligence artificielle, le modèle américain atteindra un nouveau palier. Certes, il y a encore du chemin à lever :

L'ampleur de la transformation macro-économique. Les précédentes révolutions technologiques ont montré que le choc initial peut conduire à des effets de bulle spéculative – le FMI lui-même n'écarter pas de tels risques – avant la pénétration réelle de l'IA dans notre économie et son impact sur le nombre et la qualité des emplois. L'IA est un outil 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 maximiser leur valorisation boursière, les nouveaux empereurs de l'IA diffusent à perte leurs services. Le coût des outils d'intelligence artificielle lorsque le vrai coût des *tokens* sera intégralement reporté sur les clients.

Les limites physiques à son développement. Le développement de l'IA n'est pas dissociable de la consommation d'énergie, ce qui signifie que la taille de leur système énergétique. La construction des centrales de production d'énergie dépend des capacités des fournisseurs d'équipement et des sociétés de construction à suivre le rythme de la demande. La violence des minerais (coltan, nickel, étain ou or) indispensables à la fabrication des terminaux et des infrastructures environnementales de l'utilisation massive de l'intelligence artificielle : émissions de gaz à effet de serre, l'artificialisation des sols, rejets de polluants.

Malgré les incertitudes qui entourent encore la magnitude des transformations engendrées, il est urgent de la puissance publique d'encadrer dès maintenant son développement au vu des dangers potentiels.

Une captation de valeur significative et des investissements massifs. Quand bien même les bénéfices sont surévalués, nous ne pouvons rester sans réaction face à l'accumulation et à la concentration de la richesse entre quelques personnes. Les phénomènes que nous avons connus en quelques années – la croissance exponentielle des infrastructures – se sont encore accélérés. La pénétration des outils d'intelligence artificielle dans la vie française est fulgurante, bien plus rapide que celle d'internet. Dans les entreprises, la peur de manquer de données est 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 – conduit à affaiblir considérablement tout contrôle humain. La cybersécurité en est la conséquence la plus évidente.

Un monde numérique ouvert. La dépendance critique à des fournisseurs crée des vulnérabilités. Aucun d'entre eux ne doit maîtriser les conditions de développement des autres ni avoir un poids disproportionné. Dans la mise en œuvre technique, nous sommes confrontés à deux défis. Le premier est la conciliation d'une multitude de solutions disponibles qui communiquent entre elles et le bénéfice des effets de réseau (plus nombreux, plus la valeur tirée des infrastructures numériques est importante). Le second est de garantir 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 est une question de principe, mais un sujet transactionnel. Combien m'en coûtera-t-il de ne pas respecter le droit ? Mettra-t-il à sanctionner le déploiement de nouvelles technologies, qui reposent toujours sur les mêmes principes (groupées, invisibilisation des concurrents, etc.) ? Quel droit vaut-il mieux que j'applique, le droit européen ou américain ?

Le droit est désormais perçu comme l'ennemi, responsable de la faiblesse du secteur numérique. À l'ensemble des auditions de la commission d'enquête, aucun interlocuteur n'a fourni d'exemple concret de développement économique. Ce que nous avons montré, c'est plutôt que les modifications réglementaires européennes ont été insufflées par les Big Tech qui disposent d'énormes moyens de lobbying. Au regard de la nécessité de placer les sujets de la protection des citoyens européens et la structuration d'une industrie numérique au cœur des politiques sur la régulation du numérique.

Le numérique au service de la connaissance et de l'intérêt public. Nous avons été formés à l'usage du numérique. L'un des enjeux fondamentaux est d'encourager, dans les entreprises comme dans les administrations, une réflexion critique sur les outils que nous acceptons d'utiliser, leurs conséquences sur nos vies personnelles. Pour en finir avec la dépendance aux solutions états-uniennes, il faudra proposer des outils et sortir du statu quo. Revenir à l'ambition fondatrice d'internet : avoir accès à la connaissance sans limites, sans biais, sans pillage généralisé à des fins lucratives. Ensuite, il faut développer des usages bénéfiques pour la collectivité. Les ressources énergétiques finies, comment faire en sorte que la priorité ne soit pas systématiquement donnée à la croissance ? comment hiérarchiser les différents usages du numérique afin de respecter les objectifs climatiques de l'Union européenne ?

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 transversales de la concurrence, mais aussi de l'ensemble des textes sectoriels.

Les difficultés à trouver un consensus entre États membres pour adopter des réglementations sont nombreuses. Chaque pays européen est tenu par son propre réseau d'alliances, dans le domaine de la défense ou de la sécurité. La création d'une opportunité, et les récentes décisions du gouvernement américain ont pu faire évoluer les choses. Lors de la discussion avec des représentants de la Commission européenne, l'idée que les États-Unis sont un partenaire à ne pas perdre.

Quelle position adopter ? Selon les sujets et les circonstances, trois options sont possibles :

- adopter un modèle qui puisse entrer en résonance avec les objectifs poursuivis par d'autres États membres, voire impulser des changements par le bas, grâce à des collaborations techniques et académiques ;
- assumer la défense de notre modèle lorsque cela le requiert, dans un affrontement direct avec d'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 les entreprises européennes, un système énergétique robuste, une avance technologique dans certains domaines.

reconquérir la maîtrise de nos outils, faire respecter le droit et soutenir le développement d'un écosystème.
Plusieurs leviers devront être activés conjointement pour former une politique d'ensemble
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 réussies de la Dinum, de la DGFIP, de la gendarmerie nationale ou de la commune d'Echirolles. Des logiciels au sein des administrations reposent sur des logiciels libres, qui ont fait la preuve de leur robustesse et de leur

Les logiciels libres pouvant être utilisés, étudiés, modifiés et partagés sans restriction, permettent de réduire les coûts ; assurent une plus grande maîtrise interne ; bénéficient des améliorations s'adaptent aux besoins de l'organisation qui les déploie. Ils sont généralement développés par des développeurs, bénévoles et professionnels, qui veillent à l'identification de failles et livrent régulièrement des mises à jour, assurant une performance et un niveau élevé de sécurité. Ils apportent, enfin, une capacité accrue de mutualisation et peuvent également être utilisées par le secteur privé.

Pour que les logiciels libres puissent constituer un véritable levier d'indépendance, il est nécessaire de porter une attention particulière à leur gouvernance, en contribuant activement à leur développement et à leur financement. Il convient notamment de veiller au maintien des solutions libres déjà utilisées au sein des administrations, 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 fédère les États membres autour de la construction de communs numériques souverains. Créé à la fin de l'année 2019, l'Allemagne, des Pays-Bas, de l'Italie et du Luxembourg, l'Edic a suscité un fort effet d'entraînement. Des observateurs – la Roumanie, la Pologne, la Hongrie, le Danemark, l'Autriche, la Finlande et la Flandre – ont rejoint le projet.

Il conviendra, en priorité, de contribuer financièrement à l'expérimentation d'un *Sovereign Tech Fund* pour la production et la maintenance des briques ouvertes essentielles de bas niveau, sur le modèle du *Sovereign Tech Fund*.

Le fonds pourra notamment contractualiser avec des acteurs privés, lucratifs ou non lucratifs, pour le développement des communs, salarier des développeurs pour assurer la maintenance de briques *open source*, à titre de 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 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 *open source* essentielles.

Au niveau national, la rapporteure préconise de créer une fondation France Libre Open Source pour la production et la maintenance des briques *open source* indispensables aux produits numériques déployés par l'État (data.gouv, La Suite territoriale, demarche.numérique.gouv.fr) afin de garantir leur pérennité.

de convergence pour l'ensemble des acteurs utilisant des briques *open source* et créera de l'émulation, de la gouvernance transparente et collective. Le fait de disposer d'un organe de pilotage et de partage de la qualité des contributions au code ouvert. L'Edic *Digital Commons* jouera le même rôle structurant au sein de l'écosystème numérique.

La disponibilité des briques communes, avec de fortes garanties de sécurité et de pérennité, assurera l'ensemble de l'écosystème numérique.

Les éditeurs de logiciels trouveront toute leur place dans cette dynamique. Ils pourront développer des infrastructures communes, en proposant les services d'intégration et d'implémentation de fonctionnalités pour leurs clients.

Enfin, le soutien public aux logiciels libres sera en pleine adéquation avec le principe de solidarité et contribuera 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 proposera des fiducies de données tant sur le plan juridique, qu'opérationnel, dans l'objectif d'inscrire dans la loi le statut de données d'intérêt général support de la création d'outils de mutualisations des données d'intérêt général (données culturelles, environnementales, etc.) de faire respecter les licences attachées à ces données et notamment de limiter leur usage dans un objectif de 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 agir 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 « sur l'intermédiation de données ». L'article 12 prévoit notamment les conditions d'indépendance et de transparence des syndicats de données, serviront de cadre au développement d'outils numériques respectant les règles de protection 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 offrant aux élèves et aux étudiants un accès gratuit, ou à moindre coût, à leurs outils bureautiques. Ces pratiques tendent à enfermer les citoyens dès le plus jeune âge dans leur écosystème propriétaire, constituent un frein à la souveraineté numérique.

La doctrine Cloud au centre conduit à interdire dans les établissements scolaires l'utilisation de logiciels d'éditeurs non-européens en raison des risques en termes de protection des données, comme l'a rappelé le Parlement dans un courrier adressé aux recteurs le 28 février 2026.

En dehors de cet usage spécifique, les solutions américaines demeurent très utilisées en France. L'éducation nationale a reconduit pour quatre ans l'accord-cadre qui le lie à Microsoft pour l'utilisation de logiciels installés sur près d'un million de postes de travail et de serveurs au sein du ministère, des organismes de formation, des écoles supérieures, pour un montant maximal de 152 millions d'euros ⁽¹⁵⁴⁰⁾, dont 2,4 millions par an pour le ministère. Les établissements scolaires, les enseignants et les élèves sont, pour leur part, équipés de logiciels claires pour privilégier des logiciels français ou européens.

- *Les modalités proposées*

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 de l'informatique dans l'ensemble de la société. Pourtant, il continue d'être considéré comme une infrastructure réservée aux citoyens.

- *Les modalités proposées*

Proposition n° 7 : Prévoir que le code source des logiciels développés par une entreprise entrera dans le patrimoine d'activité.

Le code fait aujourd'hui partie du patrimoine commun de l'humanité. Les codes sources de logiciels 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 ; la préservation des codes sources permettrait notamment de conserver des codes qui ne sont plus mis à jour ;
- pour soutenir l'innovation grâce à l'accès égal pour tous et le droit de réutilisation par tous ;
- pour pouvoir être étudiés comme objets scientifiques en soi. Aux États-Unis est ainsi né le *Software Studies* », destiné à replacer le code informatique dans son contexte socio-économique et culturel ; le débat sur le sujet sera d'autant plus important dans un contexte de développement de l'intelligence artificielle et de 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 le CNRS (centre national des sciences et technologies du numérique), qui collecte et préserve le code source des logiciels développés par 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 dédié à l'histoire de l'informatique pour objectif de replacer les technologies informatiques actuelles dans l'histoire de leur développement et de proposer des expositions sur les enjeux du numérique.

LEVIER N°2 : COMMANDE PUBLIQUE ET COMMANDE PRIVÉE AU SERVICE D'UNE FILIÈRE D'EXCELLENCE NUMÉRIQUE SOURCE

Les auditions ont montré qu'un vecteur important pour soutenir l'écosystème français du numérique est la commande publique et privée. Les propositions de la rapporteure visent à orienter la commande publique et privée vers 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 une représentation commune, le fait de ne pas utiliser seulement la solution standard peut être une manière de promouvoir l'innovation.

1. La commande publique

- *Les effets attendus*

La réinternalisation aura trois avantages décisifs :

- la réalisation d'économies budgétaires très importantes. Le rapport a chiffré les coûts de solutions open source à 1 milliard d'euros par an. Ces économies s'ajouteront à celles liées à la réduction du recrutement d'agents publics dont l'IGF a montré qu'elle entraînait un surcoût de 20 % par rapport au recrutement d'agents publics ;
- pour les solutions demeurant externalisées, elle permettra à l'État de « mieux acheter », grâce à la concurrence ;
- la réduction de la dépendance aux solutions propriétaires, qui entraîne des vulnérabilités économiques (hausses brutales des tarifs) ;
- de manière générale, la sécurisation et la meilleure maîtrise globale du SI des administrations face à l'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 sociétés concessionnaires d'un service public d'ici le 1^{er} 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 des acteurs extra-européens, sur la base de solutions propriétaires. Ces choix entraînent une dépendance aux 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 dans plusieurs administrations, en particulier la gendarmerie nationale (de façon totale) et la DGFIP (de façon partielle). Elles présentent la particularité d'être dotées de compétences et d'effectifs importants, permettant de maîtriser la chaîne de briques open source.

Les conséquences en termes de finances publiques sont importantes. La commission d'enquête estime que les économies en licences en logiciels substituables sont de 1 milliard d'euros sur le périmètre des administrations d'État.

La commission d'enquête a également montré que le lien entre l'État acheteur et la filière française 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. L'État devra désormais acheter du logiciel européen et s'engageront à travailler étroitement avec les acteurs français pour anticiper les besoins en avance de phase. En contrepartie, le critère de l'open source devra s'imposer comme un critère de sélection 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 recommandation à une obligation contraignante. L'open source dans les marchés de logiciels pour les administrations et les entreprises sera obligatoire à partir du 1^{er} janvier 2030.

L'entrée en application en 2030 de l'obligation permettra de préparer les administrations et les entreprises.

Le périmètre des entités soumises à cette obligation devra également être défini pour répondre à l'objectif. Seront visées prioritairement les administrations, opérateurs, entreprises publiques chargées d'une mission de service public, ainsi que les entités privées chargées de l'exploitation d'un service public essentiel par le biais d'un contrat de service public.

obligation pour assurer l'indépendance de la France aux pressions internationales ;

– suppression des dépenses de licences : les travaux préparatoires permettront de disposer d'une généralisation de l'open source dans les administrations.

- *Deux mesures immédiates*

Proposition n° 11 : Intégrer une clause d'entiercement (escrow) ⁽¹⁵⁴¹⁾ lors de la contractualisation d'une s 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 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 de logiciels artificielle et du référentiel général d'interopérabilité.

Les administrations disposent d'ores et déjà de référentiels pour l'achat de logiciels répondant aux standards européens. La rapporteure souhaite imposer le respect de ces prescriptions dans les marchés publics.

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 européennes.

Toutefois, les éléments collectés lors des auditions confirment que le problème se pose dans 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 existent, les mêmes solutions de substitution existent, basées sur des logiciels libres ;
- un levier important réside dans le développement des compétences pour basculer vers les logiciels libres ;
- un frein identifié, spécifique aux collectivités territoriales, est celui des règles de la comptabilité. Les dépenses d'installation, de formation et d'accompagnement des utilisateurs sont aujourd'hui considérées comme des dépenses d'investissement. Ce cadre 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 les dépenses de formation) doit 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 ;
- les solutions d'IA répondant à la définition de l'OSAID 1.0.

Toutes les institutions publiques, à commencer par le gouvernement et la présidence de la République, 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 :

- la Commission européenne a créé une instance Mastodon ^([542]) ;
- en Allemagne, les ministères de la défense et des affaires étrangères ont décidé de quitter les réseaux sociaux et les affaires étrangères a fait le choix de la plateforme Blue sky ^([543]).

- aux Pays Bas, le conseil rassemblant les directeurs de communication des douze ministères et le Premier ministre hollandais, recommandant de fermer les vingt-huit comptes des ministères et des administrations et de ne conserver des comptes que pour la gestion de crise et le maintien de contact, ce qui a été prise après l'été.

- *Les effets attendus*

Grâce à leur position de leaders d'opinion, les institutions publiques pourront inciter les utilisateurs à quitter et valoriser des plateformes conformes à nos valeurs.

Pour les administrations, le fait de passer par des réseaux sociaux interopérables est une manière de sécuriser la communication et de limiter les risques sur la souveraineté informationnelle que peuvent faire peser les réseaux sociaux (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 pays ne permettent pas l'accès à leur territoire pour les biens et services étrangers. Le droit de la concurrence et la directive sur l'achat public ont la capacité des acheteurs publics à favoriser les acteurs européens, *a fortiori* français, au détriment des acteurs étrangers.

La multiplication des coups de boutoir états-uniens contre le droit international, les menaces de la fourniture du modèle d'intelligence artificielle d'Anthropic, démontrent la nécessité d'une approche européenne.

- *Les modalités proposées*

Dans le cadre des négociations qui s'ouvrent sur le paquet « souveraineté numérique » par la Commission européenne, la rapporteure appelle à :

- soutenir l'instauration d'un référentiel européen de souveraineté pour le cloud qui permette d'obtenir un droit extra-européen équivalent au référentiel SecNumCloud ; et imposer aux administrations d'y recourir dans le cadre des négociations sur le Cloud and AI Development Act (CADA) ^([545]) ;

- défendre l'extension de la préférence européenne au segment des logiciels, dans un objectif de sécurisation des approvisionnements, notamment à l'occasion de la révision de la directive sur le droit de propriété intellectuelle prochain cadre financier pluriannuel.

- *Conditions de succès*

La rapporteure propose d'accompagner les ETI, dont les systèmes d'information sont des systèmes 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. Le crédit d'impôt innovation, il permettrait à ces dernières de déduire de leur impôt sur les sociétés les dépenses de R&D.

Les dépenses éligibles couvriraient les dépenses d'intégration de solutions open source, les dépenses d'accompagnement des utilisateurs, ainsi que les dépenses relatives à l'auto-hébergement des serveurs de l'opérateur européen, garant de l'immunité aux lois extraterritoriales, pour les cinq premières années de mise en œuvre. Les dépenses de déploiement d'outils IA respectant la définition de l'OSAID 1.0 hébergées sur des cloud européens.

- *Les effets attendus*

L'objectif est de contribuer au soutien de la filière française du numérique via un soutien financier. Ce soutien est maintenu durant une période assez longue, permettra de donner une visibilité à la filière suffisamment grande pour développer 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 qu'il peut 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 données de santé en hyperscalers :

- la vulnérabilité des données aux lois extraterritoriales ;
- la dépendance aux technologies fournies, qui rendent un client des solutions hybrides comme les hébergeurs de données de santé, 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, multi-cloud, et à favoriser des pratiques de vente couplée.

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 que les 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 est 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 données de santé ne soit confié à des acteurs soumis à un droit extraterritorial. Elle doit également permettre de se prémunir contre le risque de fuite de données.

- *Les modalités proposées*

Comme l’a proposé le président Philippe Latombe, lors de l’examen du projet de loi de financement du numérique financée par le biais de subventions et ayant bénéficié du crédit impôt recherche, de la vente à un acteur extra-européen.

- *Les effets attendus*

L’État accepte une part de risque dans le financement des entreprises innovantes. Du fait que la subventionne nécessairement un nombre important d’entreprises et de projets qui ne parviennent pas à se développer, 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 depuis 2015 par l’offre de la société française Chapsvision. En parallèle, le ministre de l’armement a généralisé pour un million d’agents de la fonction publique d’un assistant conversationnel français. Ces systèmes sont également déployés par le ministère des armées et des entreprises stratégiques telles que

Il n’existe cependant aucune garantie que ces entreprises demeurent françaises à moyen terme. Les représentants présents au capital de Mistral AI, et le directeur général de ChapsVision a cédé une précédente société

Le devenir d’actifs devenus stratégiques en quelques mois, parce que l’État leur a concédé des fonds. Les mains des investisseurs dont les intérêts ne sont pas alignés avec ceux de la puissance publique. Ces fonds ont pour objectif : la performance de leur portefeuille boursier à l’occasion d’une future levée de fonds.

- *Les modalités proposées*

L’État doit renforcer son pouvoir de contrôle. Il est proposé que l’État ait recours à des actions spécifiques de ChapsVision ou de Mistral.

Ces actions spécifiques, prévues par l’article 31-1 de l’ordonnance du 20 août 2014, comprennent, indépendamment de la quotité de capital qu’il détient : un droit d’agrément sur les franchissements de droits de vote ; un droit d’opposition sur les décisions de cession, d’apport ou de transmission ; le renforcement de leurs conditions d’exploitation, si elles sont de nature à porter atteinte aux intérêts de l’État ; le renforcé sur les opérations affectant les actifs stratégiques ; et la nomination au conseil d’administration à caractère délibérative.

- *Les conditions de faisabilité*

Des actions spécifiques peuvent être mises en œuvre par décret en Conseil d’État. L’application de ChapsVision nécessiterait cependant d’actualiser l’ordonnance du 20 août 2014, qui fige le champ de l’article 31-1 de l’ordonnance de 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, la limitation aux cas de cession de parts d’entreprises publiques au secteur privé conduisait à « *restreindre les actions spécifiques, sans pour autant répondre à une contrainte valable* » ^([548]). La loi Pacte ^([549]) a élargi l’une des activités est considérée comme stratégique, au sens de l’article L. 151-3 du code monétaire et financier.

besoins d'investissements importants dans l'IA et du manque de fonds atteignant la taille critique en

Ce contrôle renforcé pourra être atteint **pour un coût maîtrisé**. Aucune acquisition ChapsVision, dont BPIFrance détient déjà une part de capital supérieure à 5 %. S'agissant de M 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 pris en compte. La croissance repose en grande partie sur la commande publique et dont la visibilité internationale a un impact positif sur l'économie française. La confiance de l'État constituera un levier de crédibilité supplémentaire pour les entreprises des marchés dans des secteurs d'activité critiques. Enfin, le dispositif des *golden shares* est encadré par un contrôle de nécessité et de proportionnalité est réalisé. C'est le meilleur gage du respect de l'équité et de l'intérêt général. D'autres mesures, comme des clauses spécifiques du pacte d'actionnaires, ne sont pas exclues 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 par le développement d'infrastructures numériques. Il est indispensable que l'État puisse garantir la continuité de service, s

- *Les modalités proposées*

Il est proposé la création d'une clause de souveraineté devant être intégrée lors de la signature d'un contrat de financement portant sur un service dont le bon fonctionnement est nécessaire à la continuité de l'État et des services publics.

Cette clause de souveraineté finale vise à garantir que des services numériques structurants re

Elle stipulerait qu'en cas de changement de contrôle au profit d'une entité dont la direction n'est pas européenne, le mécanisme s'appliquerait automatiquement pour préserver le contrôle européen sur les fonctions essentielles, 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, y compris la tierce partie dans un cadre défini (clause de souveraineté finale). Toute exploitation commerciale commerciale de cette mesure serait motivée par des enjeux de continuité de l'État et des services publics essentiels ainsi qu

- *Les effets attendus*

L'État peut financer de manière importante des services ou le fonctionnement d'infrastructures numériques publiques, car ils sont essentiels pour la société ou son activité. Il est alors indispensable que puisse garantir la continuité de service, et ce d'autant plus qu'ils sont largement déployés au sein d'administrations ou d'organisations

Une vente à un acteur extra-européen pourrait nécessiter de redévelopper ou de faire passer les données à une alternative.

La clause de souveraineté finale est donc une clause de dernier recours, qui permet de garantir la continuité de service

LEVIER N° 4 : LES INFRASTRUCTURES

Proposition n° 21 : Prendre en compte les enjeux de souveraineté des données et ne répondant pas à l'impératif de

d'artificialisation des sols.

Il apparaît finalement que les autorités nationales et européennes se sont engagées dans un développement 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 le développement des data centers par des acteurs extra-européens, des fonds d'investissement ou des acteurs immobiliers, ou dont l'utilité dépasse les besoins des acteurs européens. C'est pourquoi la rapporteure demande à l'État d'examiner l'ensemble des voies pour instaurer un moratoire dans un laps de temps resserré.

- *Les effets attendus*

Une telle décision sera nécessairement critiquée pour le signal négatif qu'elle enverrait au développement d'arrêt mis au développement de l'intelligence artificielle.

L'examen des conditions dans lesquelles les projets bénéficieraient effectivement à la collectivité 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 numérique

- *Les enseignements de la commission d'enquête*

La commission d'enquête a montré que les data centers répondant aux impératifs de souveraineté numérique. Dès lors, le développement des data centers a-t-il vocation à être confié au secteur privé, sans aucune condition ?

Aujourd'hui, le déploiement des data centers avec une haute capacité de calcul s'effectue principalement par des acteurs développés ne soit mise en regard des besoins réels. Surtout, les *hyperscalers* sont en position de force. Parmi elles, comprises celles qui sont développées par des investisseurs généralistes et des fonds d'investissement. 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 data centers pour l'intelligence artificielle.

Le contrôle public aura vocation à garantir que les capacités de calcul sont bien utilisées au profit des besoins des 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 de souveraineté, immunité aux droits extra-européens, impact environnemental (performance énergétique, faible consommation d'eau), accès à une diversité de modèles (open source, propriétaire...) et de vocations (recherche, utilité sociale, lutte contre la désinformation)

- un régime de concession, permettant à l'État de dégager des recettes fiscales par l'imposition des data centers d'inférence ou bien de garantir que les capacités de calcul sont mises à disposition des utilisateurs au profit des besoins des françaises du numérique ou les utilisateurs

- enfin, la création d'une société d'investissement à capital majoritairement public. Une telle structure pourrait être efficace sur le secteur dans la durée. De plus, elle pourrait constituer un investissement profitable pour l'État en diminuant le coût global des investissements en réduisant le coût d'accès au capital en raison d'une meilleure gouvernance.

d'assurance, ont également appliqué les sanctions et interrompu la fourniture de leurs services. Cette interprétation extensive de la portée des lois extraterritoriales et de la crainte de procédures sur le ma

L'Union européenne a jusqu'ici échoué à protéger ses ressortissants face à ces sanctions pour refusant d'activer le règlement de blocage. Ce dernier vise pourtant précisément à lutter contre les aux entreprises soumises au droit de l'Union européenne d'appliquer des sanctions illégales de pays

Au-delà des pressions exercées à l'encontre des individus, l'administration américaine européenne de représailles pour faire échec à l'application des règles numériques que l'Union adoptées.

- *Les modalités proposées*

Face à ces remises en cause répétées de la souveraineté de l'Union sur son propre territoire, demain utilisées pour faire pression sur des magistrats, des défenseurs de droits, et des responsables mobiliser l'ensemble de l'arsenal juridique mis en place pour lutter contre les tentatives de coercition

Elle appelle la Commission européenne à activer le règlement de blocage contre les sanctions européens sans fondement dans le droit européen, à commencer par celles qui visent les magistrats aurait pour conséquence d'annuler les effets des sanctions étrangères sur le territoire européen et d' les mettre en œuvre.

À moyen terme, il serait nécessaire de réviser le règlement de blocage pour le rendre véritablement prévues contre les entreprises européennes qui appliqueraient les législations extraterritoriales malgré États membres sont libres de déterminer les sanctions à imposer. La France pourrait appliquer articles L. 542-1 et suivants du code des douanes ; d'autres États n'ont pas prévu de sanctions dissuasives au sein de l'Union.

En dernier recours, la rapporteure appelle l'Union européenne à utiliser l'instrument antic coercition économique exercée par des pays tiers, permet à l'Union européenne de réagir aux tentatives de pays tiers qui viseraient à influencer les choix politiques souverains de l'Union ou d'un État membre. Si la médiation échoue, la Commission européenne peut adopter un éventail de contre-mesures incluant, douane, des restrictions à l'importation ou à l'exportation des marchandises, l'exclusion des investissements directs étrangers. La nécessité d'obtenir une majorité qualifiée de 55 % au Conseil instrument à constituer un moyen de dissuasion crédible.

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

Il est, par ailleurs, nécessaire de protéger les citoyens européens placés sans fondement sous leur accès à des services de paiement. Pour ce faire, la rapporteure appelle à mettre en place une entité des services de base en matière de banque et d'assurance. Elle ne devrait pas recourir au dollar américain, de façon à éviter tout lien de rattachement pouvant justifier une inculpation devant les tribunaux

Proposition n° 24 : Mettre en place une entité bancaire immune publique, totalement indépendante du système 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

La rapporteure a identifié quatre instruments qui pourraient être activés par la France, en ce qui concerne la protection des données, pour protéger ses ressortissants contre les abus des grandes plateformes. Ils visent à favoriser le développement de services numériques, les sanctionner, et les faire cesser, en conjuguant le recours au droit européen, au droit national 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 citoyens de se défendre contre les manquements au RGPD et de renforcer la protection des droits des personnes. En étant la première à introduire un tel recours, 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, indépendamment de tout mandat, une réclamation auprès de l'autorité de protection des données s'il y a eu des manquements prévus par le règlement ont été violés. Aucun État membre ne s'est cependant saisi de cette possibilité.

Comme l'a fait valoir M. Max Schrems lors de son audition, une telle procédure de recours collectif pourrait être utilisée par des ONG : *« Cette clause nous aurait permis de porter devant la justice de nombreuses affaires que nous recevons, titre d'exemple, nous recevons de nombreuses plaintes de parents qui nous demandent d'agir contre les abus de données de leur enfant, mais aucun d'eux n'accepte que celui-ci soit identifié comme plaignant dans une procédure collective devant une institution –, précisément par crainte de nuire à sa vie privée. L'alinéa 2 de l'article 80 nous permettrait de faire cela. »*

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 en matière de données 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 plateformes numériques et de leurs dirigeants en cas de signalement d'atteintes aux droits des personnes résultant de traitements informatiques. Elle envoie un message très clair : ce qui est interdit hors ligne est interdit en ligne. Des moyens adaptés doivent être mis en œuvre.

Le parquet de Paris a lancé une telle procédure, le 6 mai 2026, à l'encontre des sociétés de données Yaccarino pour les chefs de collecte de données à caractère personnel par un moyen frauduleux, pour la mise en œuvre d'une plateforme en ligne pour permettre des transactions illicites, la violation du secret des correspondances et la mise en œuvre d'un système de traitement automatisé de données.

Proposition n° 27 : Suspender les plateformes dangereuses.

En cas de violation grave et répétée de leurs obligations par les grandes plateformes, demander au président de la Commission européenne 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 puisse suspendre l'accès à une plateforme, cet outil ne peut être activé qu'en dernier recours, sous des conditions très strictes : l'infraction doit avoir été épuisée sans permettre de faire cesser l'infraction, et celle-ci doit entraîner un préjudice grave pour les personnes impliquant une menace pour la vie ou la sécurité des personnes, et ne pas pouvoir être évitée par l'application du droit de l'Union ou le droit national.

D'autres pays dans le monde ont pourtant réussi à imposer un tel rapport de force sans que cela ne soit contraire au respect de leur droit, comme l'a montré la suspension du réseau social X par le tribunal suprême du Brésil en 2024. Le professeur Luca Belli a souligné les différences entre les modèles de régulation européenne et brésilien : *« L'Union intervient directement par voie judiciaire pour protéger l'ordre démocratique, le modèle européen est plus indirect, centralisée autour de la Commission. Le DSA instaure un cadre graduel et rigoureusement encadré, tandis que le droit brésilien est plus direct. En vertu des principes de proportionnalité et de subsidiarité, la suspension d'une plateforme en ligne par le droit européen nécessiterait un dénouement exigeant des années de procédures, incluant injonctions de conformité, audits, sanctions, etc. »*

souvent plus prudents, voire remarquables, malgré leur mission originelle », a expliqué Luca Berni. C'est ce qui a conduit le gouvernement à adopter un rôle moteur. Par une décision du 26 juin 2025, le Tribunal suprême a ainsi prononcé l'inconstitutionnalité de la loi sur l'Internet de 2014, qui reconnaissait l'irresponsabilité des grandes plateformes sur les contenus qu'elles hébergent. Cette décision invite le gouvernement à adopter un modèle de régulation qui consacre des obligations de vigilance et de retrait immédiat des contenus

Dès lors, la rapporteure souligne l'importance de préserver une capacité d'action nationale. L'article 6-3 de la loi pour la confiance dans l'économie numérique du 21 juin 2024 dispose qu'il est possible de prescrire toutes les mesures propres à prévenir ou à faire cesser un dommage occasionné par le contenu en ligne accessible au public en ligne.

Sur ce fondement, le gouvernement a demandé à la justice, en décembre 2025, d'ordonner la suppression des contenus ayant constaté la vente de poupées pédopornographiques. La demande a été rejetée par le tribunal administratif de Paris, disproportionnée au regard du retrait des produits illicites par Shein. Ce jugement a été confirmé par la Cour de cassation. La rapporteure relève néanmoins que cette décision ne préjuge pas du succès de futures procédures en cours. 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 plateformes numériques qui contournent nos lois de façon répétée. L'objectif est de renforcer les outils pouvant être mobilisés pour faire respecter 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 de régulation aux 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 stratégie ambitieuse de réduction des dépendances pour les systèmes d'information de l'État est entravée par une approche éclatée entre les différents ministères.

La commission d'enquête n'a pu que constater une grande asymétrie de moyens, techniques et compétences entre les administrations, qui place certaines d'entre elles dans une situation de grande vulnérabilité et compromet la continuité du service régalienn ou de service public. La mutualisation des produits numériques et des clouds interministériels est limitée par l'effet d'échelle et l'effet d'entraînement. Si l'État a posé, par voie de décret ou de circulaire, un certain nombre de règles, notamment une incitation à privilégier les logiciels libres, un seuil limite d'externalisation des compétences, une obligation de confiance pour l'hébergement des données d'une sensibilité particulière, désormais consacrée par la loi, qu'elles n'étaient pas systématiquement respectées.

La procédure d'avis conforme de la Dinum sur les grands projets numériques de l'État par les administrations et ne permet pas de faire cesser les initiatives contraires à la souveraineté, comme l'achat de données de santé ou du projet Virtuo du ministère de l'éducation nationale. Le récent renforcement des règles sur les achats de logiciels à la demande restera lettre morte si l'impact des décisions de la direction n'est pas

Les instruments de pilotage font défaut. Si un travail a été lancé par la Dinum, la direction des systèmes d'information de l'État, pour les dépendances numériques de l'État, il n'existe pas d'outils de suivi centralisé des dépenses

La feuille de route chiffrée permettra aux entreprises du numérique de disposer d'une v entreprises, afin de développer leur offre en conséquence. Elle garantira également aux ministères 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 n des logiciels et des prestations de services numériques. L'information budgétaire et technique déli 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 empêchant les députés de les aborder conjointement. Sont ainsi compétentes :

- la commission des lois s'agissant de la protection des données personnelles et des attei fonctionnement de la démocratie ;
- la commission des affaires économiques pour le développement de la filière numériq économique, ou les enjeux énergétiques sous-jacents ;
- la commission de la défense et des forces armées sur les menaces informationnelles et la lu
- la commission du développement durable sur l'impact environnemental des infrastructures
- la commission des affaires culturelles et de l'éducation quant au développement des comp 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'emplo

À titre d'exemple, l'examen du projet de loi relatif à la résilience des infrastructures critique nécessité la création d'une commission spéciale dédiée du fait de sa nature transversale. De même, et de protection des droits fondamentaux conduit trop souvent à les opposer, comme l'ont illustré le droit d'auteur.

- *Les modalités proposées*

La rapporteure appelle la Conférence des présidents à créer une délégation au numérique reconnaître sa dimension transversale et structurante.

- *Les effets attendus*

La délégation au numérique permettra à l'Assemblée nationale d'articuler les différents renforcer la cohérence de son approche des politiques menées en la matière, en exerçant un contrôle

Elle est également susceptible d'encourager le travail transpartisan et de favoriser des initia de la délégation aux droits des femmes ont ainsi conduit à l'adoption de la loi du 6 novembre 202 des agressions sexuelles.

Il demeure cependant essentiel que les commissions permanentes ne se dessaisissent pas du thématiques.

Recommandation n° 10 : Assurer la représentativité des consultations menées par la Commission européenne 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 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 s

Recommandation n° 13 : Défendre au niveau européen l'obligation pour les data centers de fournir des certi maille horaire.

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

Recommandation n° 15 : Permettre aux agents de l'État de contribuer, l'équivalent d'une journée par an, à des 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 n

Recommandation n° 18 : Faire respecter la définition de l'open source dans son acception de l'OSAID 1.0, y c

LISTE DES PROPOSITIONS

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

Proposition n° 1 : Soutenir politiquement et financièrement l'Edic *Digital Commons*, qui vise à coord développement des communs numériques.

Proposition n° 2 : Créer une fondation France Libre Open Source (Flos) qui assurera la pérennité des br 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 com 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 respo comprenne l'enseignement des logiciels libres.

Proposition n° 30 : Prévoir que le code source des logiciels développés par une entreprise entrera dans le c 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 opérat sociétés concessionnaires d'un service public d'ici le 1^{er} janvier 2030.

Proposition n° 11 : Intégrer une clause d'entiercement (*escrow*) lors de la contractualisation d'une structure p

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 aux 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'adoption d'un vote.

M. le président Philippe Latombe. Nous arrivons au terme des travaux de notre commission. Au cours de ces travaux, desquelles nous avons entendu 112 personnes – chercheurs, représentants d'associations, d'entreprises –, nous nous sommes déplacés à Bruxelles.

Ces travaux ont permis d'établir une cartographie inédite et très précise des dépendances et des risques numériques en Europe 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 avait été adopté par l'Assemblée nationale française et européenne. Depuis, la nouvelle donne internationale, l'affaiblissement de la régulation, le développement 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 par le 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 rapport. 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. Ils ont tous pu apporter leur contribution au secrétariat avant vendredi, douze heures. Ces contributions seront annexées au rapport.

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 son travail. Nous avons effectué, ainsi que les équipes, qui ont consacré beaucoup de temps à l'analyse des informations.

En six mois, il ne nous était pas possible d'examiner de manière approfondie des questions complexes qui constituent des sujets d'étude à part entière, ni de nous pencher en détail sur l'aspect matériel. Les données et les éléments sont donc absents du rapport. Il est à noter que le gouvernement mène un travail à ce sujet. Des travaux importants sont donc consacrés. Nous devrions débattre en septembre du projet de loi relatif à la résilience des infrastructures numériques – 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 a été créé. Le 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.

entreprises américaines pour un montant de 264 milliards d'euros.

L'utilisation par les administrations et les entreprises privées de services numériques ex-logiciels, d'outils essentiellement américains se traduit par une perte directe de valeur ajoutée pour la France. La valeur ajoutée des entreprises qui restent sur le territoire n'excède pas, dans le meilleur des cas, 28 %, alors que pour les 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 (TSN) payée par les acteurs extra-européens ne s'en acquittaient pas, leur contribution fiscale serait très limitée. Les opérateurs comme 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 d'exploitation des données à des fins commerciales. Ces données transitent par de nombreux acteurs, y compris les *data brokers*. Cela entraîne un risque systémique de fichage de la population et constitue aussi un défi de sécurité 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 vulnérable. Dans le domaine des données que dans le domaine technologique, comme l'illustrent le cas du juge Guillou et le blocage de la plateforme de santé, il faut savoir que le gouvernement américain a adressé à Microsoft plus de 5 500 demandes de données au semestre 2025 et plus de 60 000 à Google, qui les a satisfaites dans 89 % des cas. La question de la dépendance vis-à-vis des acteurs états-unis 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 du lobbying – selon laquelle il n'y aurait pas d'alternative possible. Les auditions ont montré qu'il existe des produits solides, à l'image de la plateforme des données de santé. Cela étant, les centrales de données américaines produisent des produits américains des autres. Les chiffres donnés par l'Ugap ont dû être retravaillés parce que les groupes dont la maison mère est installée en Irlande, mais qui sont clairement des opérateurs américains, ne font pas cette distinction.

L'idée selon laquelle il n'y aurait pas de solution alternative est véhiculée par les passeurs de données, les conseils ou de service qui réalisent une grande partie de leur chiffre d'affaires par le biais, notamment, de la vente de 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 agit 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 aux entreprises numériques s'est concentré sur l'émergence de licornes et de start-up sans être systématiquement associé à des investissements dans les infrastructures. Cette absence de conditionnalité des aides et des prises de participation est de nature à favoriser la dépendance, alors que le passage à l'échelle est complexe sur le marché européen et qu'il n'y a aucune équivalence entre les 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 neutre et non comme une politique en tant que telle. Nous sommes confrontés à plusieurs enjeux et défis qui dépassent les compétences ministérielles. Les ministères les plus dépendants au cloud extra-européen et aux solutions américaines sont ceux qui détiennent le moins de compétences numériques propres. Les taux d'externalisation peuvent dépasser 90 %, ce qui signifie que le chef de projet lui-même était externalisé. Dans ce cas de figure, on parle de projet déployé. En outre, l'État peine à coordonner les choix de ses ministères ; il conviendrait qu'ils adoptent une vision commune.

Nous nous heurtons à des difficultés en matière d'application de la réglementation. Les dépenses en matière de numérique, les Gafam, s'élèvent à près de 17 milliards d'euros, dont 12 milliards contre le seul Google. Les entreprises américaines ont au regard de leurs capacités financières. En outre, les procédures sont très longues, les sanctions sont faibles.

réflexions existantes à ce sujet, sachant que de nombreux facteurs d'incertitude demeurent. Nous ne pouvons pas prédire la pénétration de l'IA, quel type de tâches elle affectera ni quelles améliorations ou, en tout cas, qu'elle apportera. Le public s'est emparé de ces questions, notamment à la suite d'un certain nombre de licenciements qui ont été attribués à l'intelligence artificielle, même si la direction du Trésor nuance ce lien de causalité. Ces annonces ont des motifs mais le lien entre le développement de l'IA dans les entreprises et l'évolution de l'emploi est une préoccupation.

La protection des données, dans le cadre du déploiement de l'IA, est peu régulée. La réglementation 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 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 les besoins. Nous ne divulguons ni les terrains identifiés ni les emplacements exacts mais fournissons des indications sur la répartition. Les projets se concentrent dans deux régions : sans surprise, l'Ile-de-France, et la région Auvergne-Rhône-Alpes.

RTE a réservé 15 gigawatts (GW) de capacité de raccordement aux projets de data centers dans le parc nucléaire français, une proportion très élevée. Au-delà de la question de la soutenabilité, il s'agit de la répartition. Après analyse approfondie, nous avons pu établir la décomposition suivante : 2 GW sont destinés à des opérateurs américains ; 2,5 GW à des acteurs extra-européens autres que ces opérateurs ; 9 GW à des acteurs européens. En logique d'investissement, ce qui ne nous permet pas de savoir qui seront les utilisateurs finaux – des entreprises ou des *hyperscalers*, qui ont la capacité de payer ; enfin, 1,4 GW seulement à des acteurs européens. La part la plus importante, une très large proportion captée par des acteurs extra-européens, nous devons nous mobiliser si nous voulons réduire nos dépendances.

J'ajoute que parmi les opérateurs accompagnés par la task force, 35 % sont français et plus de 50 % sont européens.

Le rapport comporte à la fois des recommandations et des propositions. Les recommandations sont consensuelles, à mettre en œuvre assez rapidement, je pense à la publication des décrets de la loi sur la souveraineté numérique, dite loi Sren,

Les propositions quant à elles concernent des enjeux plus structurants, comme l'open source. Nous proposons une fondation dédiée à l'open source. Elle encouragerait divers acteurs – État, opérateurs privés, associations – à rassembler des briques pour ensuite les utiliser selon leurs besoins propres. Nous suggérons que la Fondation Sovereign Tech Fund allemande finance la maintenance des outils open source. À côté du Conseil européen (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 compétences à l'open source français et européens, lesquels sont très en avance. Il importe également de réorienter la consommation d'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 généraliser le mécanisme de l'*escrow* dans les contrats signés par une structure publique avec un partenaire privé. Dernier, ladite structure a accès aux éléments indispensables au fonctionnement du logiciel. Pour garantir la transparence, il 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 mener à bien des réformes profondément enracinées.

Nous proposons, en outre, de renforcer de manière graduelle les contreparties qui s'imposent.

Après cette présentation longue mais synthétique, je vous soumettrai trois modifications du m... le soin d'ouvrir une phase d'échanges.

M. Vincent Thiébaut (HOR). Vous avez mené un nombre considérable d'auditions et j... 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 l... quatre-vingts licences existantes. L'open source n'est nullement une garantie de souveraineté et d... avec ces outils dans le cadre de mon activité professionnelle. Il implique des contraintes en termes... financier et économique, les utilisateurs sont, en outre, fortement liés, soit à un prestataire, soit à... notamment avoir recours pour toute modification de code ou mise à jour. Certes, pour les PME, le... mais le coût de maintenance reste très élevé.

Ma deuxième remarque concerne l'aspect financier. Pour ce qui est du domaine bancaire, vo... Nous avons bien vu quelles avaient été les répercussions des sanctions américaines qu'a subies... 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... enjeu européen a jusqu'à présent été un peu négligé. Lors du débat sur le projet de loi-cadre sur le... souveraineté que posait le recours à des *wallets* comme Apple Pay ou Google Pay pour l'achat de... aussi avoir à l'esprit pour les transactions bancaires concernant l'e-commerce, qui ne reposent pas no...

Mme Virginie Duby-Muller (DR). Je vous félicite pour cet important travail, dont l'actual... récent recours au *kill switch* par l'administration américaine montre en effet que les questionneme... souveraineté sont loin de relever de la fiction.

La proposition n° 18 porte sur le remboursement des aides à l'amorçage. Je comprends... démarche me semble trop répressive. Ne serait-il pas plus vertueux de faire en sorte de préserver l'in... Souvent, ce n'est pas par choix qu'elles quittent notre pays. Veillons à accompagner leur croissance,

J'appuie la proposition n° 28 visant à créer un ministère dédié au numérique. Ces dernière... connu plusieurs rattachements administratifs, successifs : le Premier ministre, sans disposer d'admini... Bercy. Le ministère que vous envisagez serait-il placé sous la tutelle du premier ministre ? C'est à vo... menées en ce domaine suppose un pilotage politique. Autre question : aurait-il la Dinum (direction... périmètre ?

M. Nicolas Bonnet (EcoS). Je me joins à mes collègues pour vous féliciter du travail accom... 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, tie... communauté est fournie, plus il y a de moyens pour le développer, plus il est simple à mettre à... coûteuse, ce qui contribue à diminuer la facture à long terme. L'open source n'est certes pas synonyme... à réduire notre dépendance. Nous avons tout intérêt à massifier le recours à ces logiciels qui offrent... propriétaires détenus par les Big Tech ne nous donneront jamais accès. Prenons le cas de Microso... Windows 10 puisque le code source n'est pas ouvert ; dès lors que le support n'est plus assuré... incontournable.

À cet égard, la proposition consistant à favoriser le recours à l'open source dans les PME me...

Je vous sou mets une autre piste : fournir un package de logiciels en open source aux... typiquement les petites communes. Cela leur ferait faire des économies extraordinaires. Compte ten... terme pas plus cher que les logiciels sous licence, qui sont en grande majorité américains.

cinq ans et qu'en cas de cession au cours de cette période, la part non amortie doit être remboursée : le plan de financement du rachat inclurait cette obligation.

Notons que le financement européen pose question de manière générale. Je fais ici référence aux marchés des capitaux, dont le rapport Draghi faisait déjà état. Nous n'avons pas pu aller au bout de la discussion 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. Il est sûr y avoir des désaccords, c'est le propre de l'Assemblée nationale, mais au moins partageons-nous des idées et avançons 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 gestion française, ou du moins développée en France. L'éditeur le plus utilisé par les TPE-PME, SAP, est entièrement développée en France, à Metz notamment. Beaucoup de solutions sont donc souveraines et fiscales.

Par ailleurs, n'oublions pas que les mises à jour font partie du contrat de maintenance des logiciels, à quelques centaines d'euros. Mais pour les sociétés qui fonctionnent en open source, il faut compter le déplacement.

Dans la mesure où nous disposons d'un écosystème purement national, notamment en ce qui concerne le numérique, nous devrions donc défendre à la fois l'open source et les solutions souveraines. Je suis entièrement d'accord avec vous sur la question de la place de Microsoft, mais l'écosystème numérique français ne se résume pas à ce seul acteur. Il faut au moins de nous entendre sur une définition très précise.

Quant aux questions énergétiques, je suis également d'accord : nous devrions en débattre. Je pense à la société Stellaria, qui conçoit des SMR, c'est-à-dire des petits réacteurs modulaires, qui présentent l'avantage d'être d'énergie décarbonée.

Mme Cyrielle Chatelain, rapporteure. Je suis d'accord avec ce qui vient d'être dit à propos de la définition, qui doit effectivement être précise, l'interopérabilité est également très importante. À ce stade, nous sommes d'accord sur l'open source aux PME, mais de les inciter financièrement à opter pour les opérateurs qui l'utilisent, c'est une question de dépendance. Nous avons rencontré certains éditeurs français dont l'offre se fonde sur l'open source. L'argent public que nous consacrons à juste titre au développement numérique des entreprises est important. C'est d'ailleurs tout l'objet du Buy European Act, que nous appelons de nos vœux dans le rapport, mais le cadre réglementaire des acteurs européens est insuffisant ; nous sommes d'accord.

Je suis également d'accord avec vous concernant les questions bancaires. Une partie du rapport concerne le numérique et de l'euro numérique, mais comme ce sont des projets en cours, nous n'en avons pas fait des propositions.

S'agissant du remboursement des aides publiques, nous aurons certainement des visions différentes sur la question de l'amortissement. Il ne s'agit pas de calculer ce qu'on a donné à une entreprise au cours de sa vie et de lui demander de tout rembourser en cas de rachat. Mais ce qui lui a été transmis pour son développement est une opération économique de valorisation. Quoi qu'il en soit, si une telle proposition devait être soumise, elle devrait être soumise, qu'elle serait amplement débattue avant d'être éventuellement adoptée.

Quant au ministère du numérique, nous ne nous exprimons pas sur son organisation, car c'est le rôle du ministre. Cela étant, il serait logique que l'Ariane (autorité référente pour l'intelligence artificielle) soit au sein du ministère, pourquoi pas de plein exercice et doté de services importants. Cet aspect est lié à la définition des données qui sont communiquées à l'écosystème, afin que celui-ci développe les produits adéquats. C'est

proposons donc un tableau avec différentes couleurs – il faudra aussi prévoir un dégradé en noir global, ce qui nous permet d’anonymiser les informations.

M. Nicolas Bonnet (EcoS). Si des valeurs absolues donneront effectivement des informations versés aux opérateurs étrangers, en l’occurrence américains, serait-il possible de disposer également

Mme Cyrielle Chatelain, rapporteure. Le tableau figurant page 213 répond à votre demande pas des chiffres pour l’ensemble des ministères : tous ne nous ont pas communiqué leurs dépenses apparaissent dans les couleurs les plus sombres, celui de la défense affiche à la fois des dépenses élevées, le ministère de la justice fait aussi état de montants conséquents, mais pour un nombre d’utilisateurs très faibles 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 a pu plus parler. La commission d’enquête sur l’audiovisuel public, qui s’est tenue en parallèle de la nôtre, mais les chiffres donnés par la gendarmerie ont été repris de nombreuses fois. C’est d’ailleurs en cela que sont utiles : souligner les choix précoces de certaines administrations pourrait en conduire d’autres sur le même chemin.

En l’espèce, je ne vois pas d’autre solution que celle proposée par la rapporteure, sachant que 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 Caïn. Les documents fournis par écrit ne me semblaient pas relever du secret des affaires, mais un point a peut-être échappé à la commission. Khazna est pressenti pour réaliser la première tranche du projet, mais l’annonce publique n’a pas encore été faite. Entre cette entreprise et MGX, qui soutient le projet, est connu. C’est à contrecœur que je retirerai le projet 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. À l’égard, que l’information peut déjà être trouvée en creusant un peu.

Mme Cyrielle Chatelain, rapporteure. Dans ce cas, je conserve l’information, étant rapporteure, je 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 le 15 juillet. Au compte tenu du délai de cinq jours francs que nous impose l’article 144-2 de notre règlement, il ne pourra être fait sur son contenu jusqu’à cette date. Les exemplaires qui vous ont été fournis pour cette réunion.

Je remercie l’ensemble des administrateurs et des agents qui nous ont accompagnés.

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 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 la sécurité (Irsem)

Mardi 17 mars 2026

- MM. Emmanuel Marcovitch, président de section à la première chambre de la Cour des comptes 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 » à la direction de la transformation de l'Otan
- Mme Catherine Mayenobe, directrice générale déléguée de la Caisse des dépôts, directrice des opérations, M. Arnaud Martin, directeur des risques opérationnels, M. Patrick Laurens-Frings, directeur de la direction des systèmes d'information du groupe, et M. Philippe Blanchot, directeur des relations institutionnelles, international

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 « Liberté d'expression et de 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, direction générale du groupe
- M. Martin Untersinger, journaliste au Monde, et MM. Antoine Schirer et Sébastien Bourdon, journalistes

- Institut national de la santé et de la recherche médicale (Inserm) : M. Damien Rousset, directeur général, et M. 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) 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 », directeur général d'OVH, et Mme Julia Mouzon, déléguée permanente du comité stratégique de la filière logicielle, 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 Lemaire, directeur général de la Fédération bancaire française (FBF) *
 - M. Erick Lacourrège, directeur général des moyens de paiements de la Banque de France, et M. Jean-Louis Lemaire, directeur général de l'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'Etat
 - MM. Lionel Schweitzer et Jean-Christophe Thorel, administrateurs de la Centrale d'achat du numérique de l'Etat
- 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. 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
- M. Octave Klabar, président-directeur général d’OVHcloud *, et Mme Solange Viegas Dos Reis, dir
- 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, présid 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
- 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

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 pla
 - 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 nu

Jeudi 7 mai 2026

- Audition commune de :
 - M. Tomasz Blanc, chef du service des systèmes d’information de la direction générale des finances
 - 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 géné bureau concurrence, numérique, économie du logement

– 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 du 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 LE VICE-PRÉSIDENT

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. Brenden Van Alsenoy, responsable de l'unité « politiques et consultation »

CONTRIBUTIONS DES GROUPES POLITIQUES ET DES D

CONTRIBUTION DE M. PHILIPPE LATOMBE, PRÉSIDENT DE LA COMMISSION D'ENQ

Les travaux de la commission d'enquête sur les dépendances structurelles et les vulnérabilités systémiques de l'indépendance de la France sont venus valider les analyses qui sont les miennes depuis plus de six ans. Je retire de ces travaux un certain nombre de propositions que j'ai déjà eu l'occasion de promouvoir à de nombreuses occasions, tant en matière de numérique, questions orales et écrites, articles, tribunes) que dans mes prises de parole publiques, au sein de colloques. Je prendrai pour exemple la création d'un ministère de plein exercice avec des compétences transversales, permettant de l'architecture numérique de l'État et d'élaborer une véritable stratégie pour un secteur, le numérique, qui est au service des humaines.

Je me suis aussi à maintes reprises exprimé sur la nécessité d'une DINUM recentrée sur son cœur de métier (comme le 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 France, protéger notre économie et booster nos entreprises face à une concurrence souvent déloyale des autres puissances économiques, à 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 toutes les critiques.

Enfin, je suis d'accord sur une nécessaire modernisation de la protection des données personnelles, dans la continuité de la vie privée, protection des droits et libertés, transparence, limitation des finalités, minimisation des données, 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) situés à l'étranger, tout en conservant leur protection juridique. L'objectif serait d'assurer la continuité de l'État en cas de conflit. L'Estonie, par exemple, a mis en place une ambassade de données au Luxembourg pour sécuriser certains de ses services. L'Allemagne a adopté une approche distribuée : la Pologne a été le premier pays à héberger des copies de registres gouvernementaux.

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 minimales.

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

ANNEXE N° 1 :

LISTE DES ENTITÉS AYANT RÉPONDU À UN QUESTIONNAIRE ÉCRIT D

I. QUESTIONNAIRE SUR LES ACHATS NUMÉRIQUES ET LE STOCKAGE DES DONNÉES DES

- 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 DE
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
VITALE (OIV)**

- 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 RAPPORTEUR AUX ADMINISTRATIONS DE L'ÉTAT



COMMISSION D'ENQUÊTE SUR LES DÉPENDANCES
STRUCTURELLES ET LES VULNÉRABILITÉS
SYSTEMIQUES DANS LE SECTEUR DU NUMÉRIQUE ET
LES RISQUES POUR L'INDÉPENDANCE 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 de 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 représentant de chaque entité publique 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 des 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 :

pourraient passer les entités d'ingénierie :

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, 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 à sensibilité particulière (au sens de la circulaire « Cloud au centre » du 31 mai 2020) ? 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 clouds 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 et acteurs non européens ?
16. Avez-vous élaboré une cartographie des process clés gérés par votre ministère et de la résilience associés ? Quelles sont les dépendances non substituables à un horizon de 3 ans ?
17. Quelles stratégies mettez-vous en œuvre pour limiter les dépendances et vulnérabilités de votre 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 logiciels conteneurisés (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 fonctions 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 services ?
 - 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, qualité 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'achat ?

- 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

- ([15]) M. Alain David et Mme Laetitia Saint-Paul, rapport d'information sur l'irruption de l'intelligence artificielle dans les ingénieries, [nationale.fr/dyn/17/dossiers/irruption_intelligence_artificielle_dans_ingerences_etrangeres](https://www.conseil-constitutionnel.fr/dyn/17/dossiers/irruption_intelligence_artificielle_dans_ingerences_etrangeres)
- ([16]) Auditions des 9 avril et 7 mai 2026.
- ([17]) Audition du 1^{er} avril 2026.
- ([18]) Audition du 9 avril 2026.
- ([19]) M. Arnaud Leparmentier, « IA : la folle course des géants américains de la tech », Le Monde, 7 février 2026 https://www.lemonde.fr/technologies/article/2026/02/07/ia-la-folle-course-des-geants-americains-de-la-tech_6665758_3234.html
- ([20]) 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](#)
- ([21]) M. Dany Wattebled, rapporteur de la commission d'enquête du Sénat sur les coûts et les modalités effectifs de la commande publique française, « L'urgence d'agir pour éviter la sortie de route : Piloter la commande publique au service de la souveraineté économique », juin 2025, <https://www.senat.fr/travaux-parlementaires/structures-temporaires/commissions-denquete/commission-denquete-sur-les-couts-et-le-mesure-de-leur-effet-dentrainement-sur-leconomie-francaise.html>
- ([22]) Le complément à 100 % est constitué des projets pour lesquels aucune information n'est disponible sur ce critère.
- ([23]) Pour une présentation détaillée de la doctrine Cloud au centre, voir chapitre I, C., 1.
- ([24]) direction générale de l'enseignement supérieur et de l'insertion professionnelle.
- ([25]) direction générale de la gendarmerie nationale.
- ([26]) direction générale de la police nationale.
- ([27]) Audition de M. Baptiste Grigy, directeur des systèmes d'information du Commissariat à l'énergie atomique et aux énergies alternatives.
- ([28]) ministère de l'agriculture, de l'agro-alimentaire et de la souveraineté alimentaire.
- ([29]) ministère de l'Europe et des affaires étrangères.
- ([30]) Audition de M. Tomasz Blanc, chef du service des systèmes d'information de la direction générale des finances publiques (DGFiP).
- ([31]) Circulaire du Premier ministre du 5 juillet 2021.
- ([32]) Anssi, catalogue des produits, services, profils de protection et sites certifiés, qualifiés, agréés, en juin 2026
- ([33]) Réponse écrite de la Dinum au questionnaire de la rapporteure.
- ([34]) Audition de M. Mathieu Weill, directeur de la transformation numérique du ministère de l'Intérieur, le 9 avril 2026.
- ([35]) Audition du général Marc Boget, directeur de l'agence du numérique des forces de sécurité intérieure (Anfsi), le 7 mai 2026.
- ([36]) Audition de M. Audran Le Baron, directeur du numérique pour l'éducation au ministère de l'éducation nationale, le 9 avril 2026.
- ([37]) Audition de Mme Marie-Pierre Fontanel, directrice des systèmes d'information du CNRS, le 1^{er} avril 2026.
- ([38]) Audition de M. Damien Rousset, directeur général délégué à l'administration de l'Inserm, le 1^{er} avril 2026.
- ([39]) Audition de M. Yves Billon, chef du service du numérique au secrétariat général des ministères économiques et financiers, le 9 avril 2026.
- ([40]) Cour des comptes, « Les enjeux de souveraineté des systèmes d'information civils de l'État », septembre 2025.
- ([41]) Audition de M. Damien Rousset, directeur général délégué à l'administration de l'Inserm, le 1^{er} avril 2026.
- ([42]) Audition de M. Tomasz Blanc, chef du service des systèmes d'information de la DGFiP, le 7 mai 2026.
- ([43]) Audition de Mme Stéphanie Schaer, directrice interministérielle du numérique, le 14 avril 2026.
- ([44]) Audition commune de M. David Amiel, ministre de l'action et des comptes publics, et de Mme Anne Le Hénanff, ministre déléguée chargée de la souveraineté industrielle, énergétique et numérique, chargée de l'intelligence artificielle et du numérique.
- ([45]) Audition commune de M. David Amiel et de Mme Anne Le Hénanff, le 20 mai 2026.
- ([46]) Audition de M. Vincent Strubel, directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi), le 30 avril 2026.
- ([47]) Insee, les comptes de la Nation en 2020, juillet 2021 <https://www.insee.fr/fr/statistiques/5412399?sommaire=5354786>
- ([48]) Audition, ouverte à la presse, de Mme Catherine Mayenobe, directrice générale déléguée de la Caisse des dépôts, directeur général adjoint, le 18 mars 2026.
- ([49]) Audition de M. Henri d'Agrain, le 30 avril 2026.
- ([50]) Audition Henri d'Agrain, délégué général du Club informatique des grandes entreprises françaises (Cigref), le jeudi 30 avril 2026.
- ([51]) Insee, Les entreprises en France édition 2023, décembre 2023 <https://www.insee.fr/fr/statistiques/7678542?sommaire=768107>
- ([52]) European securities and markets authority, novembre 2025, [List of designated CTPPs](#)
- ([53]) Table ronde sur les services de paiement, le mercredi 8 avril 2026.
- ([54]) M. Philippe Laulanie, table ronde sur les services de paiement, le mercredi 8 avril 2026.
- ([55]) Table ronde sur les services de paiement, le mercredi 8 avril 2026.
- ([56]) Table ronde sur les services de paiement, le mercredi 8 avril 2026.
- ([57]) Daniel Leisegang, [Europäischer Bezahlendienst Wero nutzt Amazon-Server, Netzpolitik.org](#), avril 2026 <https://netzpolitik.org/2026/europaeischer-bezahlendienst-wero-nutzt-amazon-server/#netzpolitik-pw>
- ([58]) L'Eurosystème, qui regroupe la Banque centrale européenne et les banques centrales nationales des États membres de la zone euro.
- ([59]) Réponses écrites au questionnaire de la rapporteure.

- [f82]) L'utilisation de la moyenne des trois dernières années permet de neutraliser l'effet des contrats pluriannuels qui exigent le renouvellement des licences.
- [f83]) Audition de M. Baptiste Grigy, directeur des systèmes d'information du Commissariat à l'énergie atomique et aux énergies alternatives.
- [f84]) Audition de M. Damien Rousset, directeur général délégué à l'administration de l'Institut national de la santé et de la recherche médicale.
- [f85]) Audition de Mme Marie-Pierre Fontanel, directrice des systèmes d'information du Centre national pour la recherche scientifique.
- [f86]) Table ronde sur les acheteurs publics, le 9 avril 2026.
- [f87]) Asterès, « De la dépendance technologique à la captation économique : ce que les hausses tarifaires du cloud-logiciel coûtent aux entreprises ».
- [f88]) Le cabinet Asterès relève un potentiel biais de sélection induit par l'enquête : « les entreprises les plus concernées par les hausses de tarifs ont répondu, ce qui peut conduire à une surestimation de l'ampleur des hausses observées. La concordance avec d'autres enquêtes de l'enquête questionnaire ».
- [f89]) Audition de Mme Marie-Laure Denis, présidente de la Cnil, le 15 avril 2026.
- [f90]) Audition de Mme Marie-Laure Denis, présidente de la Cnil, le 15 avril 2026.
- [f91]) Audition de M. Max Schrems, fondateur de l'association Noyb, le 26 mars 2026.
- [f92]) Ibid.
- [f93]) Rapport du Comité européen de protection des données sur la mise en œuvre par la Commission européenne de la décision d'adhésion adoptée le 4 novembre 2024.
- [f94]) Belot, Emma et al., « Le contrôle du data privacy framework par le tribunal de l'Union européenne : une validation sous le prisme du RGPD », n° 26, 2026.
- [f95]) Arrêt du Tribunal de l'Union européenne du 3 septembre 2025 (T-443/23).
- [f96]) Audition de M. Max Schrems, fondateur de l'association Noyb, le 26 mars 2026.
- [f97]) Cour suprême des États-Unis, Trump, président des États-Unis et al. v. Slaughter, 29 juin 2026 (n° 25-332).
- [f98]) Audition de Mme Katia Roux, chargée de plaidoyer pour Amnesty International, le 25 mars 2026.
- [f99]) Audition de M. Robin Berjon, directeur de l'agence Supramundane, le 10 mars 2026.
- [f100]) Audition de Mme Meredith Whittaker, présidente de la fondation Signal, le 25 mars 2026.
- [f101]) Audition de Mme Marie-Laure Denis, présidente de la Cnil, le 15 avril 2026.
- [f102]) Cnil, délibérations SAN-2020-012 et SAN-2020-013 du 7 décembre 2020.
- [f103]) Cnil, délibérations SAN-2021-023 et SAN-2021-024 du 31 décembre 2021.
- [f104]) Cnil, délibération SAN-2022-023 du 19 décembre 2022.
- [f105]) Cnil, délibérations SAN-2025-004 et SAN-2025-005 du 1^{er} septembre 2025.
- [f106]) CEPD, Lignes directrices 05/2020 portant sur le consentement au sens du RGPD du 4 mai 2020, paragraphe 39.
- [f107]) Cnil, Lignes directrices relatives aux cookies et aux traceurs du 4 juillet 2019.
- [f108]) Cnil, « Cookie walls : la Cnil publie des premiers critères d'évaluation », 16 mai 2022.
- [f109]) Audition de Mme Marie-Laure Denis, présidente de la Cnil, le 15 avril 2026.
- [f110]) Table ronde sur la protection des données personnelles le 1^{er} avril 2026.
- [f111]) CEPD, Lignes directrices 03/2022 relatives aux interfaces trompeuses dans les interfaces des plateformes de médias sociaux adoptées le 14 février 2023.
- [f112]) Avis 24-A-05 de l'Autorité de la concurrence relatif au fonctionnement concurrentiel du secteur de l'intelligence artificielle générative.
- [f113]) Audition de Mme Mélanie Dulong de Rosnay, directrice de recherche au Centre national de la recherche scientifique (CNRS), le 31 mars 2026.
- [f114]) Audition de Mme Meredith Whittaker, présidente de la fondation Signal, le 25 mars 2026.
- [f115]) Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (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 2001/17/CE, 2002/20/CE, 2002/46/CE, 2004/38/CE, 2006/123/CE, 2006/29/CE, 2006/42/CE, 2006/60/CE, 2006/70/CE, 2006/86/CE, 2006/95/CE, 2007/15/CE, 2007/23/CE, 2007/26/CE, 2007/30/CE, 2007/46/CE, 2008/56/CE, 2008/68/CE, 2008/91/CE, 2008/1008/CE, 2008/1009/CE, 2008/1010/CE, 2008/1011/CE, 2008/1012/CE, 2008/1013/CE, 2008/1014/CE, 2008/1015/CE, 2008/1016/CE, 2008/1017/CE, 2008/1018/CE, 2008/1019/CE, 2008/1020/CE, 2008/1021/CE, 2008/1022/CE, 2008/1023/CE, 2008/1024/CE, 2008/1025/CE, 2008/1026/CE, 2008/1027/CE, 2008/1028/CE, 2008/1029/CE, 2008/1030/CE, 2008/1031/CE, 2008/1032/CE, 2008/1033/CE, 2008/1034/CE, 2008/1035/CE, 2008/1036/CE, 2008/1037/CE, 2008/1038/CE, 2008/1039/CE, 2008/1040/CE, 2008/1041/CE, 2008/1042/CE, 2008/1043/CE, 2008/1044/CE, 2008/1045/CE, 2008/1046/CE, 2008/1047/CE, 2008/1048/CE, 2008/1049/CE, 2008/1050/CE, 2008/1051/CE, 2008/1052/CE, 2008/1053/CE, 2008/1054/CE, 2008/1055/CE, 2008/1056/CE, 2008/1057/CE, 2008/1058/CE, 2008/1059/CE, 2008/1060/CE, 2008/1061/CE, 2008/1062/CE, 2008/1063/CE, 2008/1064/CE, 2008/1065/CE, 2008/1066/CE, 2008/1067/CE, 2008/1068/CE, 2008/1069/CE, 2008/1070/CE, 2008/1071/CE, 2008/1072/CE, 2008/1073/CE, 2008/1074/CE, 2008/1075/CE, 2008/1076/CE, 2008/1077/CE, 2008/1078/CE, 2008/1079/CE, 2008/1080/CE, 2008/1081/CE, 2008/1082/CE, 2008/1083/CE, 2008/1084/CE, 2008/1085/CE, 2008/1086/CE, 2008/1087/CE, 2008/1088/CE, 2008/1089/CE, 2008/1090/CE, 2008/1091/CE, 2008/1092/CE, 2008/1093/CE, 2008/1094/CE, 2008/1095/CE, 2008/1096/CE, 2008/1097/CE, 2008/1098/CE, 2008/1099/CE, 2008/1100/CE, 2008/1101/CE, 2008/1102/CE, 2008/1103/CE, 2008/1104/CE, 2008/1105/CE, 2008/1106/CE, 2008/1107/CE, 2008/1108/CE, 2008/1109/CE, 2008/1110/CE, 2008/1111/CE, 2008/1112/CE, 2008/1113/CE, 2008/1114/CE, 2008/1115/CE, 2008/1116/CE, 2008/1117/CE, 2008/1118/CE, 2008/1119/CE, 2008/1120/CE, 2008/1121/CE, 2008/1122/CE, 2008/1123/CE, 2008/1124/CE, 2008/1125/CE, 2008/1126/CE, 2008/1127/CE, 2008/1128/CE, 2008/1129/CE, 2008/1130/CE, 2008/1131/CE, 2008/1132/CE, 2008/1133/CE, 2008/1134/CE, 2008/1135/CE, 2008/1136/CE, 2008/1137/CE, 2008/1138/CE, 2008/1139/CE, 2008/1140/CE, 2008/1141/CE, 2008/1142/CE, 2008/1143/CE, 2008/1144/CE, 2008/1145/CE, 2008/1146/CE, 2008/1147/CE, 2008/1148/CE, 2008/1149/CE, 2008/1150/CE, 2008/1151/CE, 2008/1152/CE, 2008/1153/CE, 2008/1154/CE, 2008/1155/CE, 2008/1156/CE, 2008/1157/CE, 2008/1158/CE, 2008/1159/CE, 2008/1160/CE, 2008/1161/CE, 2008/1162/CE, 2008/1163/CE, 2008/1164/CE, 2008/1165/CE, 2008/1166/CE, 2008/1167/CE, 2008/1168/CE, 2008/1169/CE, 2008/1170/CE, 2008/1171/CE, 2008/1172/CE, 2008/1173/CE, 2008/1174/CE, 2008/1175/CE, 2008/1176/CE, 2008/1177/CE, 2008/1178/CE, 2008/1179/CE, 2008/1180/CE, 2008/1181/CE, 2008/1182/CE, 2008/1183/CE, 2008/1184/CE, 2008/1185/CE, 2008/1186/CE, 2008/1187/CE, 2008/1188/CE, 2008/1189/CE, 2008/1190/CE, 2008/1191/CE, 2008/1192/CE, 2008/1193/CE, 2008/1194/CE, 2008/1195/CE, 2008/1196/CE, 2008/1197/CE, 2008/1198/CE, 2008/1199/CE, 2008/1200/CE, 2008/1201/CE, 2008/1202/CE, 2008/1203/CE, 2008/1204/CE, 2008/1205/CE, 2008/1206/CE, 2008/1207/CE, 2008/1208/CE, 2008/1209/CE, 2008/1210/CE, 2008/1211/CE, 2008/1212/CE, 2008/1213/CE, 2008/1214/CE, 2008/1215/CE, 2008/1216/CE, 2008/1217/CE, 2008/1218/CE, 2008/1219/CE, 2008/1220/CE, 2008/1221/CE, 2008/1222/CE, 2008/1223/CE, 2008/1224/CE, 2008/1225/CE, 2008/1226/CE, 2008/1227/CE, 2008/1228/CE, 2008/1229/CE, 2008/1230/CE, 2008/1231/CE, 2008/1232/CE, 2008/1233/CE, 2008/1234/CE, 2008/1235/CE, 2008/1236/CE, 2008/1237/CE, 2008/1238/CE, 2008/1239/CE, 2008/1240/CE, 2008/1241/CE, 2008/1242/CE, 2008/1243/CE, 2008/1244/CE, 2008/1245/CE, 2008/1246/CE, 2008/1247/CE, 2008/1248/CE, 2008/1249/CE, 2008/1250/CE, 2008/1251/CE, 2008/1252/CE, 2008/1253/CE, 2008/1254/CE, 2008/1255/CE, 2008/1256/CE, 2008/1257/CE, 2008/1258/CE, 2008/1259/CE, 2008/1260/CE, 2008/1261/CE, 2008/1262/CE, 2008/1263/CE, 2008/1264/CE, 2008/1265/CE, 2008/1266/CE, 2008/1267/CE, 2008/1268/CE, 2008/1269/CE, 2008/1270/CE, 2008/1271/CE, 2008/1272/CE, 2008/1273/CE, 2008/1274/CE, 2008/1275/CE, 2008/1276/CE, 2008/1277/CE, 2008/1278/CE, 2008/1279/CE, 2008/1280/CE, 2008/1281/CE, 2008/1282/CE, 2008/1283/CE, 2008/1284/CE, 2008/1285/CE, 2008/1286/CE, 2008/1287/CE, 2008/1288/CE, 2008/1289/CE, 2008/1290/CE, 2008/1291/CE, 2008/1292/CE, 2008/1293/CE, 2008/1294/CE, 2008/1295/CE, 2008/1296/CE, 2008/1297/CE, 2008/1298/CE, 2008/1299/CE, 2008/1300/CE, 2008/1301/CE, 2008/1302/CE, 2008/1303/CE, 2008/1304/CE, 2008/1305/CE, 2008/1306/CE, 2008/1307/CE, 2008/1308/CE, 2008/1309/CE, 2008/1310/CE, 2008/1311/CE, 2008/1312/CE, 2008/1313/CE, 2008/1314/CE, 2008/1315/CE, 2008/1316/CE, 2008/1317/CE, 2008/1318/CE, 2008/1319/CE, 2008/1320/CE, 2008/1321/CE, 2008/1322/CE, 2008/1323/CE, 2008/1324/CE, 2008/1325/CE, 2008/1326/CE, 2008/1327/CE, 2008/1328/CE, 2008/1329/CE, 2008/1330/CE, 2008/1331/CE, 2008/1332/CE, 2008/1333/CE, 2008/1334/CE, 2008/1335/CE, 2008/1336/CE, 2008/1337/CE, 2008/1338/CE, 2008/1339/CE, 2008/1340/CE, 2008/1341/CE, 2008/1342/CE, 2008/1343/CE, 2008/1344/CE, 2008/1345/CE, 2008/1346/CE, 2008/1347/CE, 2008/1348/CE, 2008/1349/CE, 2008/1350/CE, 2008/1351/CE, 2008/1352/CE, 2008/1353/CE, 2008/1354/CE, 2008/1355/CE, 2008/1356/CE, 2008/1357/CE, 2008/1358/CE, 2008/1359/CE, 2008/1360/CE, 2008/1361/CE, 2008/1362/CE, 2008/1363/CE, 2008/1364/CE, 2008/1365/CE, 2008/1366/CE, 2008/1367/CE, 2008/1368/CE, 2008/1369/CE, 2008/1370/CE, 2008/1371/CE, 2008/1372/CE, 2008/1373/CE, 2008/1374/CE, 2008/1375/CE, 2008/1376/CE, 2008/1377/CE, 2008/1378/CE, 2008/1379/CE, 2008/1380/CE, 2008/1381/CE, 2008/1382/CE, 2008/1383/CE, 2008/1384/CE, 2008/1385/CE, 2008/1386/CE, 2008/1387/CE, 2008/1388/CE, 2008/1389/CE, 2008/1390/CE, 2008/1391/CE, 2008/1392/CE, 2008/1393/CE, 2008/1394/CE, 2008/1395/CE, 2008/1396/CE, 2008/1397/CE, 2008/1398/CE, 2008/1399/CE, 2008/1400/CE, 2008/1401/CE, 2008/1402/CE, 2008/1403/CE, 2008/1404/CE, 2008/1405/CE, 2008/1406/CE, 2008/1407/CE, 2008/1408/CE, 2008/1409/CE, 2008/1410/CE, 2008/1411/CE, 2008/1412/CE, 2008/1413/CE, 2008/1414/CE, 2008/1415/CE, 2008/1416/CE, 2008/1417/CE, 2008/1418/CE, 2008/1419/CE, 2008/1420/CE, 2008/1421/CE, 2008/1422/CE, 2008/1423/CE, 2008/1424/CE, 2008/1425/CE, 2008/1426/CE, 2008/1427/CE, 2008/1428/CE, 2008/1429/CE, 2008/1430/CE, 2008/1431/CE, 2008/1432/CE, 2008/1433/CE, 2008/1434/CE, 2008/1435/CE, 2008/1436/CE, 2008/1437/CE, 2008/1438/CE, 2008/1439/CE, 2008/1440/CE, 2008/1441/CE, 2008/1442/CE, 2008/1443/CE, 2008/1444/CE, 2008/1445/CE, 2008/1446/CE, 2008/1447/CE, 2008/1448/CE, 2008/1449/CE, 2008/1450/CE, 2008/1451/CE, 2008/1452/CE, 2008/1453/CE, 2008/1454/CE, 2008/1455/CE, 2008/1456/CE, 2008/1457/CE, 2008/1458/CE, 2008/1459/CE, 2008/1460/CE, 2008/1461/CE, 2008/1462/CE, 2008/1463/CE, 2008/1464/CE, 2008/1465/CE, 2008/1466/CE, 2008/1467/CE, 2008/1468/CE, 2008/1469/CE, 2008/1470/CE, 2008/1471/CE, 2008/1472/CE, 2008/1473/CE, 2008/1474/CE, 2008/1475/CE, 2008/1476/CE, 2008/1477/CE, 2008/1478/CE, 2008/1479/CE, 2008/1480/CE, 2008/1481/CE, 2008/1482/CE, 2008/1483/CE, 2008/1484/CE, 2008/1485/CE, 2008/1486/CE, 2008/1487/CE, 2008/1488/CE, 2008/1489/CE, 2008/1490/CE, 2008/1491/CE, 2008/1492/CE, 2008/1493/CE, 2008/1494/CE, 2008/1495/CE, 2008/1496/CE, 2008/1497/CE, 2008/1498/CE, 2008/1499/CE, 2008/1500/CE, 2008/1501/CE, 2008/1502/CE, 2008/1503/CE, 2008/1504/CE, 2008/1505/CE, 2008/1506/CE, 2008/1507/CE, 2008/1508/CE, 2008/1509/CE, 2008/1510/CE, 2008/1511/CE, 2008/1512/CE, 2008/1513/CE, 2008/1514/CE, 2008/1515/CE, 2008/1516/CE, 2008/1517/CE, 2008/1518/CE, 2008/1519/CE, 2008/1520/CE, 2008/1521/CE, 2008/1522/CE, 2008/1523/CE, 2008/1524/CE, 2008/1525/CE, 2008/1526/CE, 2008/1527/CE, 2008/1528/CE, 2008/1529/CE, 2008/1530/CE, 2008/1531/CE, 2008/1532/CE, 2008/1533/CE, 2008/1534/CE, 2008/1535/CE, 2008/1536/CE, 2008/1537/CE, 2008/1538/CE, 2008/1539/CE, 2008/1540/CE, 2008/1541/CE, 2008/1542/CE, 2008/1543/CE, 2008/1544/CE, 2008/1545/CE, 2008/1546/CE, 2008/1547/CE, 2008/1548/CE, 2008/1549/CE, 2008/1550/CE, 2008/1551/CE, 2008/1552/CE, 2008/1553/CE, 2008/1554/CE, 2008/1555/CE, 2008/1556/CE, 2008/1557/CE, 2008/1558/CE, 2008/1559/CE, 2008/1560/CE, 2008/1561/CE, 2008/1562/CE, 2008/1563/CE, 2008/1564/CE, 2008/1565/CE, 2008/1566/CE, 2008/1567/CE, 2008/1568/CE, 2008/1569/CE, 2008/1570/CE, 2008/1571/CE, 2008/1572/CE, 2008/1573/CE, 2008/1574/CE, 2008/1575/CE, 2008/1576/CE, 2008/1577/CE, 2008/1578/CE, 2008/1579/CE, 2008/1580/CE, 2008/1581/CE, 2008/1582/CE, 2008/1583/CE, 2008/1584/CE, 2008/1585/CE, 2008/1586/CE, 2008/1587/CE, 2008/1588/CE, 2008/1589/CE, 2008/1590/CE, 2008/1591/CE, 2008/1592/CE, 2008/1593/CE, 2008/1594/CE, 2008/1595/CE, 2008/1596/CE, 2008/1597/CE, 2008/1598/CE, 2008/1599/CE, 2008/1600/CE, 2008/1601/CE, 2008/1602/CE, 2008/1603/CE, 2008/1604/CE, 2008/1605/CE, 2008/1606/CE, 2008/1607/CE, 2008/1608/CE, 2008/1609/CE, 2008/1610/CE, 2008/1611/CE, 2008/1612/CE, 2008/1613/CE, 2008/1614/CE, 2008/1615/CE, 2008/1616/CE, 2008/1617/CE, 2008/1618/CE, 2008/1619/CE, 2008/1620/CE, 2008/1621/CE, 2008/1622/CE, 2008/1623/CE, 2008/1624/CE, 2008/1625/CE, 2008/1626/CE, 2008/1627/CE, 2008/1628/CE, 2008/1629/CE, 2008/1630/CE, 2008/1631/CE, 2008/1632/CE, 2008/1633/CE, 2008/1634/CE, 2008/1635/CE, 2008/1636/CE, 2008/1637/CE, 2008/1638/CE, 2008/1639/CE, 2008/1640/CE, 2008/1641/CE, 2008/1642/CE, 2008/1643/CE, 2008/1644/CE, 2008/1645/CE, 2008/1646/CE, 2008/1647/CE, 2008/1648/CE, 2008/1649/CE, 2008/1650/CE, 2008/1651/CE, 2008/1652/CE, 2008/1653/CE, 2008/1654/CE, 2008/1655/CE, 2008/1656/CE, 2008/1657/CE, 2008/1658/CE, 2008/1659/CE, 2008/1660/CE, 2008/1661/CE, 2008/1662/CE, 2008/1663/CE, 2008/1664/CE, 2008/1665/CE, 2008/1666/CE, 2008/1667/CE, 2008/1668/CE, 2008/1669/CE, 2008/1670/CE, 2008/1671/CE, 2008/1672/CE, 2008/1673/CE, 2008/1674/CE, 2008/1675/CE, 2008/1676/CE, 2008/1677/CE, 2008/1678/CE, 2008/1679/CE, 2008/1680/CE, 2008/1681/CE, 2008/1682/CE, 2008/1683/CE, 2008/1684/CE, 2008/1685/CE, 2008/1686/CE, 2008/1687/CE, 2008/1688/CE, 2008/1689/CE, 2008/1690/CE, 2008/1691/CE, 2008/1692/CE, 2008/1693/CE, 2008/1694/CE, 2008/1695/CE, 2008/1696/CE, 2008/1697/CE, 2008/1698/CE, 2008/1699/CE, 2008/1700/CE, 2008/1701/CE, 2008/1702/CE, 2008/1703/CE, 2008/1704/CE, 2008/1705/CE, 2008/1706/CE, 2008/1707/CE, 2008/1708/CE, 2008/1709/CE, 2008/1710/CE, 2008/1711/CE, 2008/1712/CE, 2008/1713/CE, 2008/1714/CE, 2008/1715/CE, 2008/1716/CE, 2008/1717/CE, 2008/1718/CE, 2008/1719/CE, 2008/1720/CE, 2008/1721/CE, 2008/1722/CE, 2008/1723/CE, 2008/1724/CE, 2008/1725/CE, 2008/1726/CE, 2008/1727/CE, 2008/1728/CE, 2008/1729/CE, 2008/1730/CE, 2008/1731/CE, 2008/1732/CE, 2008/1733/CE, 2008/1734/CE, 2008/1735/CE, 2008/1736/CE, 2008/1737/CE, 2008/1738/CE, 2008/1739/CE, 2008/1740/CE, 2008/1741/CE, 2008/1742/CE, 2008/1743/CE, 2008/1744/CE, 2008/1745/CE, 2008/1746/CE, 2008/1747/CE, 2008/1748/CE, 2008/1749/CE, 2008/1750/CE, 2008/1751/CE, 2008/1752/CE, 2008/1753/CE, 2008/1754/CE, 2008/1755/CE, 2008/1756/CE, 2008/1757/CE, 2008/1758/CE, 2008/1759/CE, 2008/1760/CE, 2008/1761/CE, 2008/1762/CE, 2008/1763/CE, 2008/1764/CE, 2008/1765/CE, 2008/1766/CE, 2008/1767/CE, 2008/1768/CE, 2008/1769/CE, 2008/1770/CE, 2008/1771/CE, 2008/1772/CE, 2008/1773/CE, 2008/1774/CE, 2008/1775/CE, 2008/1776/CE, 2008/1777/CE, 2008/1778/CE, 2008/1779/CE, 2008/1780/CE, 2008/1781/CE, 2008/1782/CE, 2008/1783/CE, 2008/1784/CE, 2008/1785/CE, 2008/1786/CE, 2008/1787/CE, 2008/1788/CE, 2008/1789/CE, 2008/1790/CE, 2008/1791/CE, 2008/1792/CE, 2008/1793/CE, 2008/1794/CE, 2008/1795/CE, 2008/1796/CE, 2008/1797/CE, 2008/1798/CE, 2008/1799/CE, 2008/1800/CE, 2008/1801/CE, 2008/1802/CE, 2008/1803/CE, 2008/1804/CE, 2008/1805/CE, 2008/1806/CE, 2008/1807/CE, 2008/1808/CE, 2008/1809/CE, 2008/1810/CE, 2008/1811/CE, 2008/1812/CE, 2008/1813/CE, 2008/1814/CE, 2008/1815/CE, 2008/1816/CE, 2008/1817/CE, 2008/1818/CE, 2008/1819/CE, 2008/1820/CE, 2008/1821/CE, 2008/1822/CE, 2008/1823/CE, 2008/1824/CE, 2008/1825/CE, 2008/1826/CE, 20

- [146]) Audition de M. Max Schrems, fondateur de l'association Noyb, le 26 mars 2026.
- [147]) Rapport du directeur du bureau administratif des tribunaux américains sur les activités de la Cour de surveillance du renseignement.
- [148]) Audition de M. Henri Verdier le 10 mars 2026.
- [149]) 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 ;
– M. Julien Lépine, représentant en France d'Amazon Web Services Europe, Moyen-Orient, Afrique (AWS EMEA), et M. Arnaud Lemaire, représentante européenne de AWS.
- [150]) Rapport fait au nom de la commission d'enquête sur les coûts et les modalités effectifs de la commande publique et la mesure de la transparence par M. le sénateur Dany Wattebled, enregistré à la présidence du Sénat le 8 juillet 2025.
- [151]) 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 ;
– M. Julien Lépine, représentant en France d'Amazon Web Services Europe, Moyen-Orient, Afrique (AWS EMEA), et M. Arnaud Lemaire, représentante européenne de AWS.
- [152]) <https://www.microsoft.com/en-us/corporate-responsibility/reports/government-requests/customer-data>
- [153]) <https://transparencyreport.google.com/user-data/overview>
- [154]) https://d1.awsstatic.com/onedam/marketing-channels/website/aws/en_US/whitepapers/compliance/Amazon_AWS_Information_Request.pdf
- [155]) Audition de M. Martin Untersinger, journaliste au Monde, et MM. Antoine Schirer et Sébastien Bourdon, journalistes indépendants.
- [156]) Table ronde réunissant des représentants en France des Gafam le 13 mai 2026.
- [157]) Audition de M. Vincent Strubel le 30 avril 2026.
- [158]) Table ronde réunissant des représentants en France des Gafam le 13 mai 2026.
- [159]) Ibid.
- [160]) Audition de M. Vincent Strubel le 30 avril 2026.
- [161]) Mourad Krim, « AWS European Sovereign Cloud : étanche technologiquement, perméable juridiquement », IT social, 16 janvier 2026.
- [162]) Audition de M. Vincent Strubel le 30 avril 2026.
- [163]) Anssi, Référentiel d'exigences pour les prestataires de services d'informatique en nuage (SecNumCloud), version 3.2 du 8 mars 2026.
- [164]) <https://www.anthropie.com/news/fable-mythos-access>
- [165]) Audition de Nicolas Guillou, juge à la Cour pénale internationale, le mercredi 8 avril 2026
- [166]) 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 a été élu en 2018, 18 février 2026.
- [167]) Audition de Mme Beti Hohler devant la commission des affaires juridiques (JURI) et la sous-commission sur les droits humains le 8 avril 2026.
- [168]) Audition de M. Nicolas Guillou le 8 avril 2026.
- [169]) Ibid.
- [170]) Le règlement (UE) 2015/751 du 29 avril 2015 relatif aux commissions d'interchange pour les opérations de paiement liées à un paiement par carte de paiement co-badgeage.
- [171]) Réponses écrites de la direction générale du Trésor au questionnaire de la rapporteure.
- [172]) Table ronde sur les services de paiement le 8 avril 2026.
- [173]) Coalition pour la Cour pénale internationale, La guerre juridique menée par les États-Unis contre le système de justice internationale (https://coalitionfortheicc.org/sites/default/files/cicc_documents/Criminalising%20Accountability%20-%202026_0.pdf)
- [174]) Institut Montaigne, Extraterritorialité américaine : une arme à double tranchant, décembre 2024.
- [175]) Coalition pour la Cour pénale internationale, La guerre juridique menée par les États-Unis contre le système de justice internationale.
- [176]) Emmanuel Breen, La compétence américaine fondée sur le dollar : réalité juridique ou construction politique ?, Groupe d'études de la Cour pénale internationale.
- [177]) Coalition pour la Cour pénale internationale, La guerre juridique menée par les États-Unis contre le système de justice internationale.
- [178]) Audition de M. Nicolas Guillou le 8 avril 2026.
- [179]) Table ronde sur les services de paiement le 8 avril 2026.
- [180]) Règlement (CE) n° 2271/96 du Conseil du 22 novembre 1996 portant protection contre les effets de l'application extraterritoriale de des actions fondées sur elle ou en découlant.
- [181]) 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.
- [182]) Siobhan McGarry, porte-parole de la Commission européenne pour le marché intérieur, citée par Le Monde, « L'UE peine à régler le conflit entre la CPI », 23 avril 2026.
- [183]) Audition de M. Nicolas Guillou le 8 avril 2026.
- [184]) Rapport d'information fait au nom de la commission des affaires européennes du Sénat sur l'extraterritorialité des sanctions économiques, 4 octobre 2018 ; Rapport d'information fait au nom de la commission des affaires étrangères et la commission des finances en France sur l'extraterritorialité de la législation américaine, enregistré le 5 octobre 2016.
- [185]) Audition de Nicolas Guillou, juge à la Cour pénale internationale, le mercredi 8 avril 2026

- ([210]) Audition de M. Umberto Berkani, rapporteur général de l'Autorité de la concurrence, le 5 mai 2026.
- ([211]) Réponse de l'Autorité de la concurrence au questionnaire de la rapporteure.
- ([212]) Audition de M. Thierry Breton, ancien commissaire européen au Marché intérieur, ancien président-directeur général d'Atos S
- ([213]) Audition de M. Umberto Berkani, rapporteur général de l'Autorité de la concurrence, le 5 mai 2026.
- ([214]) Audition de M. Umberto Berkani, rapporteur général de l'Autorité de la concurrence, le 5 mai 2026.
- ([215]) Commission staff working document Accompanying the document Report from the Commission to the European Parliament Committee on the Review of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets 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>
- ([216]) Audition de M. Michel Paulin, président du comité stratégique de filière « solutions numériques de confiance » du Conseil national du numérique, 7 avril 2026.
- ([217]) Audition de M. Eiman Ezzat, directeur général de CapGemini, et Mme Karine Brunet, directrice mondiale des opérations et du développement du groupe, le 26 mars 2026.
- ([218]) Table ronde réunissant des fournisseurs de cloud le 21 avril 2026.
- ([219]) Ibid.
- ([220]) Anssi, catalogue des produits, services, profils de protection et sites certifiés, qualifiés, agréés, juin 2026.
- ([221]) Audition de Mme Stéphanie Schaer, directrice interministérielle du numérique, et M. Jérémie Vallet, son adjoint, le 14 avril 2026.
- ([222]) Table ronde réunissant des fournisseurs de cloud le 21 avril 2026.
- ([223]) Audition de M. Michel Paulin, président du comité stratégique de filière « solutions numériques de confiance » du Conseil national du numérique, 7 avril 2026.
- ([224]) Table ronde réunissant des fournisseurs de cloud le 21 avril 2026.
- ([225]) Ibid.
- ([226]) Audition du collectif Eurostack, le 26 mars 2026.
- ([227]) Table ronde sur le logiciel libre le 6 mai 2026.
- ([228]) Commission européenne, communiqué de presse, 17 avril 2026.
- ([229]) Direction générale des services numériques de la Commission européenne, Cloud Sovereignty Framework, version 1.2.1, octobre 2025.
- ([230]) Table ronde sur les infrastructures numériques le 2 avril 2026.
- ([231]) Rapport fait au nom de la commission d'enquête sur l'influence croissante des cabinets de conseil privés sur les politiques publiques, 2022.
- ([232]) Audition de M. Aiman Ezzat, directeur général de Capgemini, le 26 mars 2026.
- ([233]) Ibid.
- ([234]) Ibid.
- ([235]) Ibid.
- ([236]) Audition du collectif #Fab8 le 29 avril 2026.
- ([237]) Réponses écrites de l'Ugap au questionnaire de la rapporteure.
- ([238]) CAIH, « La CAIH adopte son nouveau plan stratégique et lance Alternative », 26 février 2026.
- ([239]) Laurent Sounack, « La Canut propose un nouveau marché dédié aux réseaux sécurisés », ChannelNews, 17 octobre 2026.
- ([240]) Rapport fait au nom de la commission d'enquête sur les coûts et les modalités effectifs de la commande publique et la mesure de la performance sous la présidence de M. Simon Uzenat, par le rapporteur M. Dany Wattebled, et enregistré à la présidence du Sénat le 8 juillet 2026.
- ([241]) Audition du collectif #Fab8 le 29 avril 2026.
- ([242]) Réponses écrites de l'Ugap au questionnaire de la rapporteure.
- ([243]) Table ronde des acheteurs publics le 9 avril 2026.
- ([244]) Audition au Sénat de M. Edward Jossa, président de l'Ugap, le 18 mars 2025.
- ([245]) Audition de M. Thomas Jan, directeur général adjoint en charge de l'innovation et de la stratégie numérique de l'Union des industries et des métiers de la filière numérique, le 10 mars 2026.
- ([246]) Audition de M. Henri Verdier, directeur général de l'Inria, le 10 mars 2026.
- ([247]) Association française de promotion et de défense du logiciel libre.
- ([248]) Table ronde sur le logiciel libre le 6 mai 2026.
- ([249]) Audition du collectif #Fab8 le 29 avril 2026.
- ([250]) Audition commune de M. Tomasz Blanc et du général Marc Boget le 7 mai 2026.
- ([251]) Réponse du ministère de l'éducation nationale, publiée le 28 octobre 2025, à la question écrite n° 5312 de M. Philippe Latombe.
- ([252]) Table ronde sur le logiciel libre le 6 mai 2026.
- ([253]) Audition de M. Henri Verdier, directeur général de l'Inria, le 10 mars 2026.
- ([254]) Table ronde des fournisseurs de cloud, le 21 avril 2026.
- ([255]) Audition de Mme Hela Ghariani le 29 avril 2026.

- numérique du ministère de l'intérieur, et M. Yves Billon, chef du service du numérique au secrétariat général des ministères économiques et financiers.
- ([277]) Table ronde réunissant M. Audran Le Baron, directeur du numérique pour l'éducation du ministère de l'Éducation nationale, M. Mathieu Weill, directeur du numérique du ministère de l'intérieur, et M. Yves Billon, chef du service du numérique au secrétariat général des ministères économiques et financiers.
- ([278]) Réponse aux questionnaires, AP-HP.
- ([279]) Réponse au questionnaire, Cnaf.
- ([280]) Réponse au questionnaire, Cnav, Cnaf.
- ([281]) Rapport de l'Inspection générale des finances et du Conseil général de l'économie de l'industrie, de l'énergie et des technologies, publié en janvier 2023.
- ([282]) Ibid.
- ([283]) Table ronde sur le logiciel libre le 6 mai 2026.
- ([284]) Plafond des autorisations d'emplois pour l'État en 2025 (article 144 de la loi de finances pour 2025).
- ([285]) Réponses écrites du ministère de la justice au questionnaire de la rapporteure.
- ([286]) Table ronde réunissant M. Audran Le Baron, M. Mathieu Weill, et M. Yves Billon, le 9 avril 2026.
- ([287]) Audition de M. Henri Verdier, directeur général de la fondation Inria, ancien ambassadeur pour le numérique, le 10 mars 2026.
- ([288]) Table ronde sur le logiciel libre le 6 mai 2026.
- ([289]) Table ronde réunissant M. Audran Le Baron, M. Mathieu Weill, et M. Yves Billon, le 9 avril 2026.
- ([290]) Direction interministérielle du numérique et du système d'information et de communication de l'État, remplacée par la Dinum.
- ([291]) Audition de M. Henri Verdier, directeur général de la fondation Inria, ancien ambassadeur pour le numérique, le 10 mars 2026.
- ([292]) Rapport IGF CGE sur les ressources humaines numériques de l'État, janvier 2023.
- ([293]) Audition de M. Henri Verdier, directeur général de la fondation Inria, ancien ambassadeur pour le numérique, le 10 mars 2026.
- ([294]) Audition de Mme Stéphanie Schaer, directrice interministérielle du numérique, le 14 avril 2026.
- ([295]) Table ronde réunissant M. Audran Le Baron, M. Mathieu Weill, et M. Yves Billon, le 9 avril 2026.
- ([296]) Ibid.
- ([297]) Rapport d'activité 2025 de la Direction interministérielle du numérique.
- ([298]) Table ronde réunissant M. Audran Le Baron, M. Mathieu Weill, et M. Yves Billon, le 9 avril 2026.
- ([299]) Audition commune de M. Tomasz Blanc, chef du service des systèmes d'information de la direction générale des finances publiques, et M. Yves Billon, chef du service du numérique au secrétariat général des ministères économiques et financiers, à l'agence du numérique des forces de sécurité intérieure (ANFSI), le 7 mai 2026.
- ([300]) Rapport de la Cour des comptes sur le pilotage de la transformation numérique de l'État par la direction interministérielle du numérique, le 14 avril 2026.
- ([301]) Audition de M. Michel Paulin et de Mme Julia Mouzon, le 7 avril 2026.
- ([302]) Rapport de la Cour des comptes sur le pilotage de la transformation numérique de l'État par la direction interministérielle du numérique, le 14 avril 2026.
- ([303]) Audition de Mme Stéphanie Schaer, directrice interministérielle du numérique, le 14 avril 2026.
- ([304]) Ibid.
- ([305]) Ibid.
- ([306]) Rapport de la Cour des comptes sur le pilotage de la transformation numérique de l'État par la direction interministérielle du numérique, le 14 avril 2026.
- ([307]) Ibid.
- ([308]) Table ronde réunissant M. Audran Le Baron, M. Mathieu Weill et M. Yves Billon le 9 avril 2026.
- ([309]) 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.
- ([310]) Réponses écrites de la Dinum au questionnaire de la rapporteure.
- ([311]) Audition commune de M. Tomasz Blanc, chef du service des systèmes d'information de la direction générale des finances publiques, et M. Yves Billon, chef du service du numérique au secrétariat général des ministères économiques et financiers, à l'agence du numérique des forces de sécurité intérieure (ANFSI), le 7 mai 2026.
- ([312]) Réponses écrites de la Dinum au questionnaire de la rapporteure.
- ([313]) Rapport de la Cour des comptes sur les enjeux de souveraineté des systèmes d'information civils de l'État, délibéré le 11 septembre 2025.
- ([314]) Réponses écrites de la Dinum au questionnaire de la rapporteure.
- ([315]) Réponses écrites du ministère de l'intérieur au questionnaire de la rapporteure.
- ([316]) Dinum, Bilan de la doctrine Cloud au centre, décembre 2025.
- ([317]) Rapport de la Cour des comptes sur les enjeux de souveraineté des systèmes d'information civils de l'État, délibéré le 11 septembre 2025.
- ([318]) Ibid.
- ([319]) Réponses écrites de la Dinum au questionnaire de la rapporteure.
- ([320]) Réponses écrites du ministère de l'intérieur au questionnaire de la rapporteure.
- ([321]) Rapport de la Cour des comptes sur les enjeux de souveraineté des systèmes d'information civils de l'État, délibéré le 11 septembre 2025.
- ([322]) Rapport de la Cour des comptes sur le pilotage de la transformation numérique de l'État par la direction interministérielle du numérique, le 14 avril 2026.
- ([323]) Réponses écrites de la Dinum au questionnaire de la rapporteure.
- ([324]) Réponses écrites du ministère de la justice au questionnaire de la rapporteure.
- ([325]) Audition de Mme Stéphanie Schaer, directrice interministérielle du numérique, le 14 avril 2026.

- [348]) Audition de M. Max Schrems, fondateur de l'association Noyb, le 26 mars 2026.
- [349]) Avis conjoint du Comité européen de la protection des données et du Contrôleur européen de la protection des données sur la 10 février 2026.
- [350]) Table ronde sur la protection des données personnelles associant Mme Nataliia Bielova, directrice de recherche au centre Inria, de conférences en sciences de l'information et de la communication à l'UFR Culture et communication et au Centre d'études s (Cémti) de l'université Paris 8, le 1^{er} avril 2026.
- [351]) Article 3, paragraphe 1, b) du règlement omnibus numérique.
- [352]) Audition de M. Max Schrems, fondateur de l'association Noyb, le 26 mars 2026.
- [353]) Noyb, « Digital omnibus : 83,5 % des demandes d'accès ne reçoivent pas de réponse adéquate », 16 avril 2026. <https://noyb.not-properly-answered>
- [354]) Article 3, paragraphe 5 du règlement omnibus numérique.
- [355]) Article 3, paragraphe 6 du règlement omnibus numérique.
- [356]) Avis du Comité européen de la protection des données relatif à certains aspects de la protection des données liées au traitement modèles d'IA, adopté le 17 décembre 2024
- [357]) Avis conjoint du Comité européen de la protection des données et du Contrôleur européen de la protection des données sur la 10 février 2026.
- [358]) Noyb, rapport sur l'omnibus numérique, publiée le 24 février 2026.
- [359]) Audition de M. Max Schrems, fondateur de l'association Noyb, le 26 mars 2026.
- [360]) Article 3, paragraphe 3, point a) de la proposition de règlement omnibus numérique.
- [361]) Article 3, paragraphe 15, de la proposition de règlement omnibus numérique.
- [362]) Audition de Mme Marie-Laure Denis, présidente de la Cnil, le 15 avril 2026.
- [363]) Table ronde sur la protection des données personnelles le 1^{er} avril 2026.
- [364]) Audition de Mme Marie-Laure Denis, présidente de la Cnil, le 15 avril 2026.
- [365]) Audition de M. Robin Berjon, informaticien, directeur de l'agence Supramundane, le 10 mars 2026.
- [366]) Noyb, rapport sur l'omnibus numérique, publiée le 24 février 2026.
- [367]) Audition de Mme Marie-Laure Denis, présidente de la Cnil, le 15 avril 2026.
- [368]) Lignes directrices 1/2026 sur le traitement de données personnelles pour les finalités de recherche scientifique, adoptées le 15
- [369]) Avis 28/2024 relatif à certains aspects de la protection des données liés au traitement de données à caractère personnel da 2024.
- [370]) Lignes directrices 1/2024 sur le traitement des données personnelles fondé sur l'article 6(1)(f) du RGPD, adoptées le 8 octobre
- [371]) Lignes directrices 01/2025 sur la pseudonymisation, adoptées le 16 janvier 2025.
- [372]) Audition de M. Max Schrems, fondateur de l'association Noyb, le 26 mars 2026.
- [373]) Document de travail de la Commission européenne accompagnant les propositions de règlements dits omnibus numérique en final) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025SC0836>
- [374]) Audition de M. Max Schrems, fondateur de l'association Noyb, le 26 mars 2026
- [375]) Audition de M. Robin Berjon, informaticien, directeur de l'agence Supramundane, le 10 mars 2026.
- [376]) Corporate Europe Observatory et LobbyControl, « Article par article, comment les Big Tech ont influencé le recul de l'Union e 2026 (<https://corporateeurope.org/en/2026/01/article-article-how-big-tech-shaped-eus-roll-back-digital-rights>).
- [377]) <https://www.contexte.com/medias/pdf/medias-documents/2025/9/call-for-evidence-digital-omnibus.pdf>
- [378]) Audition de M. Max Schrems, fondateur de l'association Noyb, le 26 mars 2026
- [379]) Document de travail de la Commission européenne accompagnant les propositions de règlements dits omnibus numérique en final) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025SC0836>
- [380]) Audition, ouverte à la presse, de M. Henri Verdier, directeur général de la fondation Inria, ancien ambassadeur pour le numér
- [381]) Table ronde, ouverte à la presse, réunissant M. David Chavalarias, directeur de recherche au CNRS, directeur au Centre directeur de l'Institut des systèmes complexes de Paris Île-de-France (ISC-PIF), M. Robin Berjon, informaticien et consultant, dire directrice du domaine euratlantique à l'Institut de recherche stratégique de l'École militaire (Irsem), le 10 mars 2026.
- [382]) Audition, ouverte à la presse, de l'association Eurostack, représentée par Mme Cristina Caffarra, économiste, et M. Yann 26 mars 2026.
- [383]) <https://www.sba.gov/federal-contracting/contracting-guide>
- [384]) Audition, ouverte à la presse, de Mme Maya Noël, directrice générale de France Digitale, 16 avril 2026.
- [385]) Audition, ouverte à la presse, de M. Thierry Breton, ancien commissaire européen au Marché intérieur, ancien président-direct
- [386]) Audition, ouverte à la presse, de Mme Christel Heydemann, directrice générale du groupe Orange.
- [387]) Audition de M. Henri d'Agrain, délégué général du Club informatique des grandes entreprises françaises (Cigref) le 30 avril 2
- [388]) Audition de M. Henri Verdier, directeur général de la fondation Inria, ancien ambassadeur pour le numérique.
- [389]) Audition, ouverte à la presse, de M. Cédric O, ancien secrétaire d'État chargé du numérique, le 13 mai 2026.
- [390]) Audition, ouverte à la presse, de M. Cédric O, ancien secrétaire d'État chargé du numérique, le 13 mai 2026.

- de M. Florent Krieger, directeur du pôle souveraineté numérique et du secrétariat général pour l'investissement (SGFI), le 7 mai 2026
- [410]) Audition, ouverte à la presse, de Mme Catherine Mayenobe, directrice générale déléguée de la Caisse des dépôts, directrice opérationnelle, M. Arnaud Martin, directeur des risques opérationnels, M. Patrick Laurens-Frings, directeur de la transformation du groupe, et M. Philippe Blanchot, directeur des relations institutionnelles, internationales et européennes, le 18 mars 2026
- [411]) Audition conjointe, ouverte à la presse, de MM. Laurent Choukroun, président-directeur général d'Oreus et Julien Lescouart, directeur général de DataOne le 29 avril 2026.
- [412]) Audition commune, ouverte à la presse, de M. David Amiel, ministre de l'action et des comptes publics, et de Mme Anne L'écuyer, ministre de l'économie, des finances et de la souveraineté industrielle, énergétique et numérique, chargée de l'intelligence artificielle et du numérique, le 26 mars 2026
- [413]) valeur d'acquisition.
- [414]) Réponses aux questionnaires de la rapporteure.
- [415]) <https://doctolibpatient.zendesk.com/hc/fr/articles/4404181466002-O%C3%B9-sont-stock%C3%A9s-mes-donn%C3%A9es>
- [416]) Audition, de M. Arnaud Caudoux, directeur général adjoint de BPIFrance, M. Lionel Chaine, directeur des systèmes d'information, M. Jean-Luc L'expert et des programmes au sein de la direction de l'innovation et M. Thierry Sommelet, directeur au sein de la direction du capital, le 26 mars 2026
- [417]) Aurélie Trouvé, Rapport fait au nom de la commission d'enquête sur la prédation des capacités productives françaises par les géants américains, le 26 mars 2026
- [418]) <https://www.europarl.europa.eu/legislative-train/theme-a-new-plan-for-europe-s-sustainable-prosperity-and-competitiveness/fr>
- [419]) Audition du collectif Eurostack représenté par Mme Cristina Caffarra, économiste, spécialiste de la concurrence et de la réglementation, président-directeur général de probabl.ai, le 26 mars 2026.
- [420]) Audition de M. Arthur Mensch, cofondateur et directeur général de Mistral AI, le 12 mai 2026.
- [421]) <https://www.anthropic.com/news/microsoft-nvidia-anthropic-announce-strategic-partnerships>
- [422]) <https://epoch.ai/data/ai-companies?view=graph&tab=revenue>
- [423]) Communiqué de l'entreprise Anthropic, mai 2026 <https://www.anthropic.com/news/series-h>
- [424]) Fonds monétaire international, Rapport sur la stabilité financière mondiale, avril 2026, <https://www.imf.org/-/media/files/publications/external/2026/04/20260401-fmr-20260401.pdf>
- [425]) Bain, Technology report, septembre 2025 <https://www.bain.com/insights/how-can-we-meet-ais-insatiable-demand-for-compute>
- [426]) Romaric Godin, « L'incertaine viabilité économique de l'IA générative », Médiapart, 4 avril 2026 <https://www.mediapart.fr/fr/actualites/economique-de-l-ia-generative>
- [427]) Mickael Bazoge, « Uber commence à trouver l'addition de l'IA un peu salée », Next, le 26 mai 2026 <https://next.ink/brief-ai-salee/>
- [428]) Aditya Challapally, Chrise Pease, Ramesh Raskar, Pradyumna Chari, MIT Nanda, The GenAI Divide, State of AI in business 2025 https://mlq.ai/media/quarterly_decks/v0.1_State_of_AI_in_Business_2025_Report.pdf
- [429]) Traduit de l'anglais.
- [430]) Traduit de l'anglais.
- [431]) 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-2025-10-26/>
- [432]) Robin Wigglesworth, « Cisco finally did it », The Financial Times, 11 décembre 2025 [Cisco finally did it](https://www.ft.com/content/0c0c0c0c-0c0c-0c0c-0c0c-0c0c0c0c0c0c)
- [433]) Audition de M. Aïman Ezzat, directeur général de Capgemini, et Mme Karine Brunet, directrice mondiale des opérations et de la transformation, le 26 mars 2026
- [434]) « Intelligence artificielle : Société générale et BNP Paribas prévoient des milliers de suppressions de postes », France info, 23 mars 2026 [et BNP Paribas prévoient des milliers de suppressions de postes – franceinfo](https://www.franceinfo.fr/economie/intelligence-artificielle/societe-generale-et-bnp-paribas-prevoyent-des-milliers-de-suppressions-de-postes_23032026.html)
- [435]) Nicolas Madelaine, « Intelligence artificielle : HSBC viserait des suppressions d'emplois massives », Les Echos, 19 mars 2026 [d'emplois massives - Les Echos](https://www.lesechos.fr/economie-france/economie-intelligence-artificielle/hsbc-viserait-des-suppressions-d-emplois-massives_1234567890)
- [436]) Xavier Eutrope, « IA générative et destructions d'emplois : premier bilan dans la presse française », La Revue des médias, 26 mars 2026 [premier bilan dans la presse française | la revue des médias](https://www.larevuedesmedias.fr/actualites/ia-generative-et-destructions-d-emplois-premier-bilan-dans-la-presse-francaise)
- [437]) Commission de l'intelligence artificielle, IA : notre ambition pour la France, mars 2024, <https://www.economie.gouv.fr/files/ia/IA.pdf>
- [438]) Raphaële Adjerad, Gaston Vermersch, Avec l'essor de l'intelligence artificielle générative, l'investissement numérique tire davantage que l'emploi recule dans les activités informatiques des deux côtés de l'Atlantique, Insee, Note de conjoncture, mars 2026
- [439]) Martin Chopard, Elisa Cotet, Tristan Gantois, Eloïse Villani, L'intelligence artificielle, quels effets sur l'emploi ?, Direction générale de l'économie, mars 2026
- [440]) Commission de l'intelligence artificielle, *ibid.*
- [441]) Insee références, Intelligence artificielle dans les entreprises, octobre 2025
- [442]) Tania Babina, Anastassia Fedyk, Alex He, James Hodson, Artificial intelligence, firm growth, and product innovation, Janvier 2026
- [443]) Traduit de l'anglais.
- [444]) Erik Brynjolfsson, Danielle Li, Lindsey Raymond, Generative AI at work, Février 2025
- [445]) Xiang Hui, Oren Reshef, Luofeng Zhou, The Short-Term Effects of Generative Artificial Intelligence on Employment: Evidence from China, NBER Working Paper No. 288, mars 2023
- [446]) Margarita Lane, Morgan Williams, Stijn Broecke, The impact of AI on the workplace: Main findings from the OECD Employment and Migration Working Papers No. 288, mars 2023
- [447]) Pawel Gmyrek, Janine Berg, David Bescond, Generative AI and Jobs: A global analysis of potential effects on job quantity and quality, NBER Working Paper No. 288, mars 2023
- [448]) Antonin Bergaud, Exposition à l'intelligence artificielle générative et emploi : une application à la classification socio-professionnelle, Insee, Note de conjoncture, mars 2026

- ([474]) Audition de M. Fabrice Coquio, président-directeur général de Digital Realty, le 12 mai 2026
- ([475]) Le choix a été fait de se concentrer sur le réseau de transport d'électricité, sur lequel sont effectués les raccordements d'importance supérieure à 40 MW), susceptibles de concerner l'intelligence artificielle.
- ([476]) ADEME, Prospective d'évolution des consommations des data centers à court, moyen et long terme de 2024 à 2060, janvier 2026
- ([477]) <https://www.edf.fr/groupe-edf/comprendre/production/nucleaire/nucleaire-en-chiffres>
- ([478]) <https://www.digitalrealty.com/fr/data-centers/emea>
- ([479]) Réponses aux questionnaires de la rapporteure.
- ([480]) Audition conjointe, ouverte à la presse, de MM. Laurent Choukroun, président-directeur général d'Oreus et Julien Lescouart, directeur général de DataOne, le 29 avril 2026.
- ([481]) ADEME, *ibid.*
- ([482]) Autorité de la concurrence, *ibid.*
- ([483]) Mathilde Saliou, « Objectifs climatiques ou IA ? Pour le lobby des data centers, l'Europe doit choisir », *Next*, 22 juin 2026
- ([484]) https://ec.europa.eu/commission/presscorner/detail/fr/qanda_23_595
- ([485]) Mission régionale d'autorité environnementale Île-de-France, Avis délibéré sur le projet de construction d'un campus de centres de données
- ([486]) 4 000 MW installés, composés de 4 cycles combinés au gaz et 13 turbines à combustion.
- ([487]) Mission régionale d'autorité environnementale Île-de-France, Les data centers (centres de stockage de données), *Éclairages* 2026
- ([488]) <https://www.linkedin.com/pulse/les-enjeux-environnementaux-des-data-centers-val%C3%A9rie-masson-delmotte-zlxfe/>
- ([489]) Andrea Marinoni, Erik Cambria, Weisi Lin, Mauro Dalla Mura, Jocelyn Chanussot, Edoardo Ragusa, Chi Yan Tso, Yihao Zhu, *The impact of AI data centers in a warming world*, avril 2026
- ([490]) 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-partners-infrastructure/>
- ([491]) Communiqué de l'entreprise OpenAI, mars 2026, <https://openai.com/fr-FR/index/accelerating-the-next-phase-ai/>
- ([492]) Communiqué de l'entreprise Anthropic, mai 2026, <https://www.anthropic.com/news/series-h>
- ([493]) Communiqué de la Direction générale des entreprises, juin 2026, <https://www.entreprises.gouv.fr/la-dge/actualites/choix-en-faveur-de-lindustrie-de>
- ([494]) Communiqué de l'entreprise Nebius, mars 2026, <https://nebius.com/newsroom/nebius-signs-new-ai-infrastructure-agreement-v>
- ([495]) Audition conjointe, ouverte à la presse, de MM. Laurent Choukroun, président-directeur général d'Oreus et Julien Lescouart, directeur général de DataOne, le 29 avril 2026.
- ([496]) Séverin Lahaye, « Derrière la loi « simplification », l'offensive des Big Tech et du lobby des datacenters », *Observatoire des enquêtes/profits-et-pertes-derriere-le-boom-des-datacenters-en-france/derriere-la-loi-simplification-l-offensive-des-big-tech-et-du-lobby*
- ([497]) <https://culture-et-outils-libres.forge.apps.education.fr/logiciels-libres.html>
- ([498]) Table ronde sur le logiciel libre, le 6 mai 2026.
- ([499]) Audition, de Mme Meredith Whittaker, présidente de la fondation Signal, le 25 mars 2026.
- ([500]) Table ronde sur le logiciel libre, le 6 mai 2026.
- ([501]) Table ronde sur le logiciel libre le 6 mai 2026.
- ([502]) Audition, de Mme Meredith Whittaker, présidente de la fondation Signal, le 25 mars 2026.
- ([503]) Table ronde sur le logiciel libre le 6 mai 2026.
- ([504]) CNLL, Numeum, Systematic, Open source monitor France, Rapport 2023
- ([505]) 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-l-open-source-en-france-et-en-europe>
- ([506]) European commission, The impact of open source software and hardware on technological independence, competitiveness and growth
- ([507]) Audition de M. Henri Verdier le 10 mars 2026.
- ([508]) Table ronde sur le logiciel libre le 6 mai 2026.
- ([509]) Table ronde sur le logiciel libre, le 6 mai 2026.
- ([510]) Réponses écrites de l'Ambassade de France en Allemagne au questionnaire de la rapporteure.
- ([511]) Audition de Mme Stéphanie Schaer le 14 avril 2026.
- ([512]) Table ronde sur les infrastructures numériques le 2 avril 2026.
- ([513]) Table ronde réunissant des directeurs de systèmes d'information de ministères le 9 avril 2026.
- ([514]) *Ibid.*
- ([515]) Table ronde sur le logiciel libre le 6 mai 2026.
- ([516]) Table ronde des acheteurs publics le 9 avril 2026.
- ([517]) Table ronde sur les infrastructures numériques le 2 avril 2026.
- ([518]) Table ronde réunissant M. David Chavalarias, M. Robin Berjon et Mme Maud Quessard le 10 mars 2026.
- ([519]) Table ronde sur le thème de la protection des données personnelles le 25 mars 2026.
- ([520]) Rapport annuel de la Commission européenne sur l'application du règlement sur les marchés numériques (DMA), présenté le 10 mars 2026

[Accéder au dossier législatif](#)

Autres formats :

[Version PDF](#)

[Version HTML](#)

[Notice XML](#)

[Notice JSON](#)