

INSTITUT CHOISEUL

Briefings
Choiseul

Septembre
2025

**Les data centers :
piliers de la souveraineté
française et européenne
dans un monde
connecté**

CHOISEUL | Souveraineté



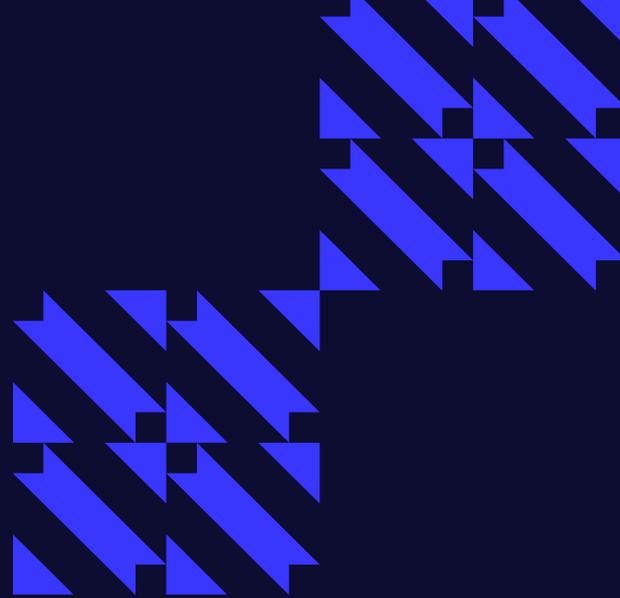
Les Briefings de l'Institut Choiseul

Conçus comme des synthèses de nos rencontres, les Briefings Choiseul sont des documents stratégiques courts et percutants, assortis de recommandations mobilisables rapidement sur des thématiques économiques d'avenir. En s'intéressant à des domaines très variés (défense, innovation, industrie, agroalimentaire, ou encore énergie, enjeux macroéconomiques ou enjeux de filière), l'Institut Choiseul croise les regards d'acteurs économiques, prescripteurs et praticiens, et formule des recommandations issues des réalités opérationnelles.

Ces documents courts et percutants dressent un état des lieux, synthétisent les enjeux et proposent des pistes d'actions concrètes. Ils sont conçus pour appeler à l'action les décideurs, parties prenantes et le grand public.

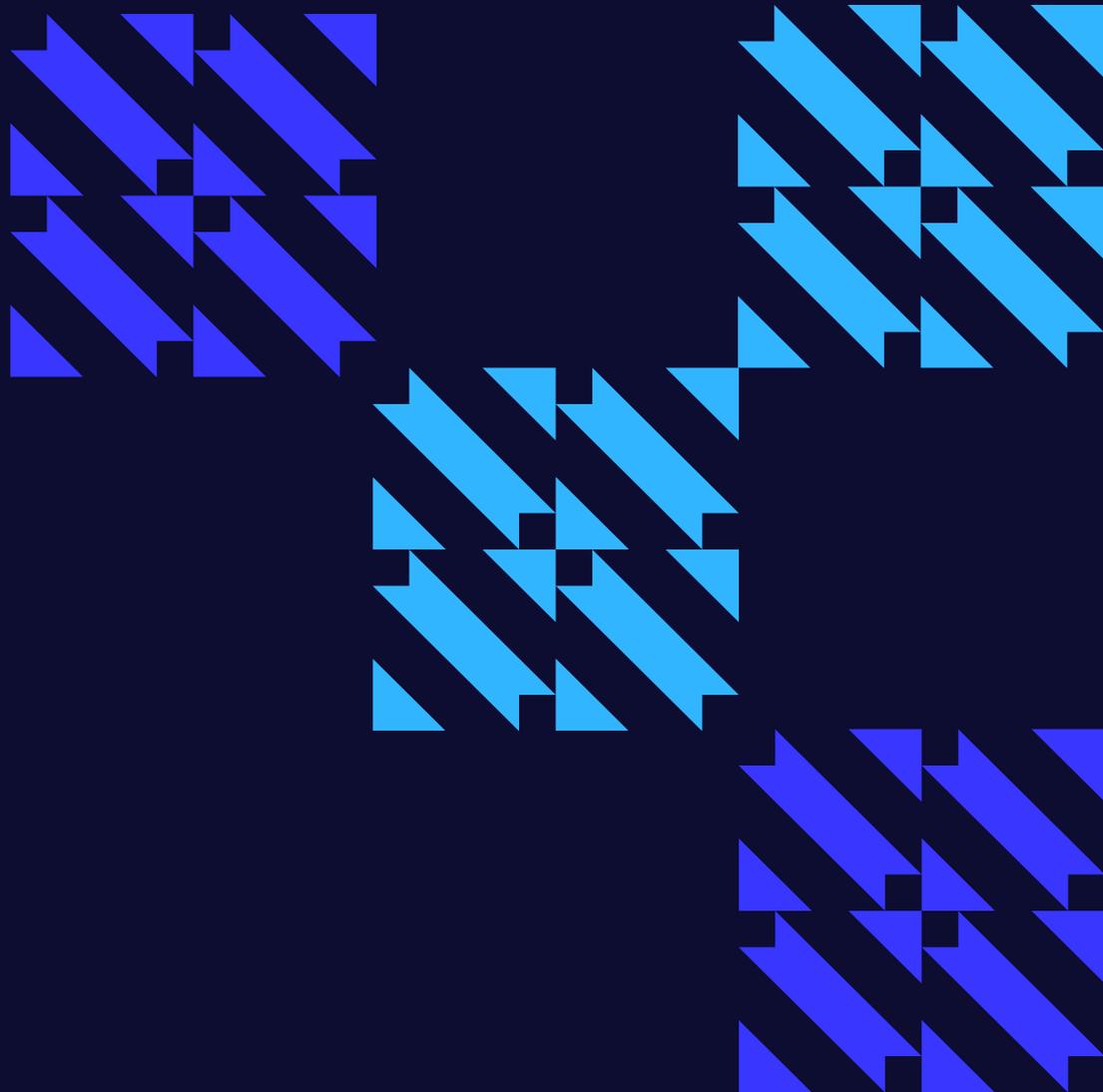
La 20ème Rencontre Souveraineté & Résilience s'est tenue le 25 juin 2025 autour d'acteurs de premier plan qui ont partagé leurs témoignages, visions prospectives et bonnes pratiques : Anne Le Hénanff, Députée de la 1ère circonscription du Morbihan, Vice-présidente du groupe d'études sur l'économie, la sécurité et la souveraineté numériques à l'Assemblée nationale, Matthieu Cales, Président de Cap Ingelec, Benjamin Revcolevschi, Directeur général d'OVHcloud et Sami Slim, CEO de Telehouse France.

Sommaire



Introduction	9
I. Constats - enjeux factuels	11
II. Défis - menaces	17
III. Propositions	20
À propos	22

Introduction



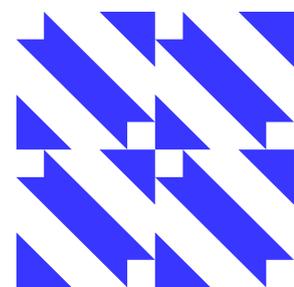
Introduction

Si nos sociétés pouvaient se résumer à un grand corps numérique, les data centers en seraient le cœur : ils collectent, traitent et distribuent les données – ces cellules vitales – à travers un réseau de câbles et de flux, comme autant de vaisseaux irriguant notre quotidien connecté. Véritables usines à données, ils sont au cœur du fonctionnement ininterrompu des services numériques, en alimentant les algorithmes d'intelligence artificielle et contribuent à la performance économique des entreprises comme à l'efficacité des services publics. Ces infrastructures concentrent aujourd'hui des enjeux stratégiques majeurs — énergétiques, géopolitiques, environnementaux et de souveraineté. Dans ce contexte, la souveraineté ne réside pas nécessairement dans une autonomie absolue : elle suppose plutôt la capacité à choisir et maîtriser ses dépendances, à faire des arbitrages stratégiques et d'assurer, en toutes circonstances, la résilience et l'agilité nécessaires pour conserver la maîtrise de son destin numérique.

Leur consommation d'énergie, leur impact environnemental, leur rôle stratégique dans l'hébergement de données sensibles, leur gouvernance et leur localisation deviennent autant de défis à anticiper, à encadrer, à maîtriser. En France, ces tensions se doublent d'une ambition : faire des data centers un levier de souveraineté numérique. Cela suppose de bâtir une capacité nationale et européenne résiliente, sécurisée et alignée avec les objectifs de transition écologique.

Face à la montée en puissance de l'intelligence artificielle, à l'hyper-concentration du marché mondial entre les mains quelques de géants non européens, et aux risques croissants liés à la cybersécurité, la France et l'Union européenne doivent élaborer une stratégie pragmatique numérique et d'innovation. Dans ce contexte, les data centers apparaissent comme des infrastructures clés — à la fois leviers de souveraineté et moteurs de croissance. Le secteur connaît une forte expansion, portée par l'essor du cloud, de l'IA et des besoins croissants en capacités de traitement. Si l'Irlande a longtemps concentré les implantations pour des raisons fiscales, la France s'impose désormais comme une destination de choix, grâce à une électricité décarbonée et compétitive, une connectivité internationale de premier plan (notamment via Marseille) et un cadre réglementaire attractif. Autant d'atouts qui renforcent son positionnement stratégique dans la nouvelle géographie numérique mondiale.

Nous proposons ici d'en décrypter les enjeux, les leviers et les limites, en articulant les dimensions techniques, industrielles, géopolitiques et environnementales des data centers. Car il ne s'agit plus seulement d'optimiser nos infrastructures : il s'agit de faire des choix décisifs pour le futur numérique du pays.



3 000

Les USA dominent le marché mondial avec 3000 data centers sur son territoire. En parallèle, l'Europe continentale est fragmentée : on recense plus de 300 data centers en France, 456 au Royaume-Uni et 487 en Allemagne.

70 %

70 % du marché est capté par les hyperscalers essentiellement américains (AWS, Microsoft Azure, Google Cloud).

109 milliards d'euros

À l'occasion du Sommet de l'IA organisé à Paris en février, 109 milliards d'euros d'investissements ont été annoncés dans les data centers et l'IA.

5 ans

À cause de la lourdeur des procédures actuelles, il faut aujourd'hui 5 ans en moyenne pour construire un data center en France.

49 %

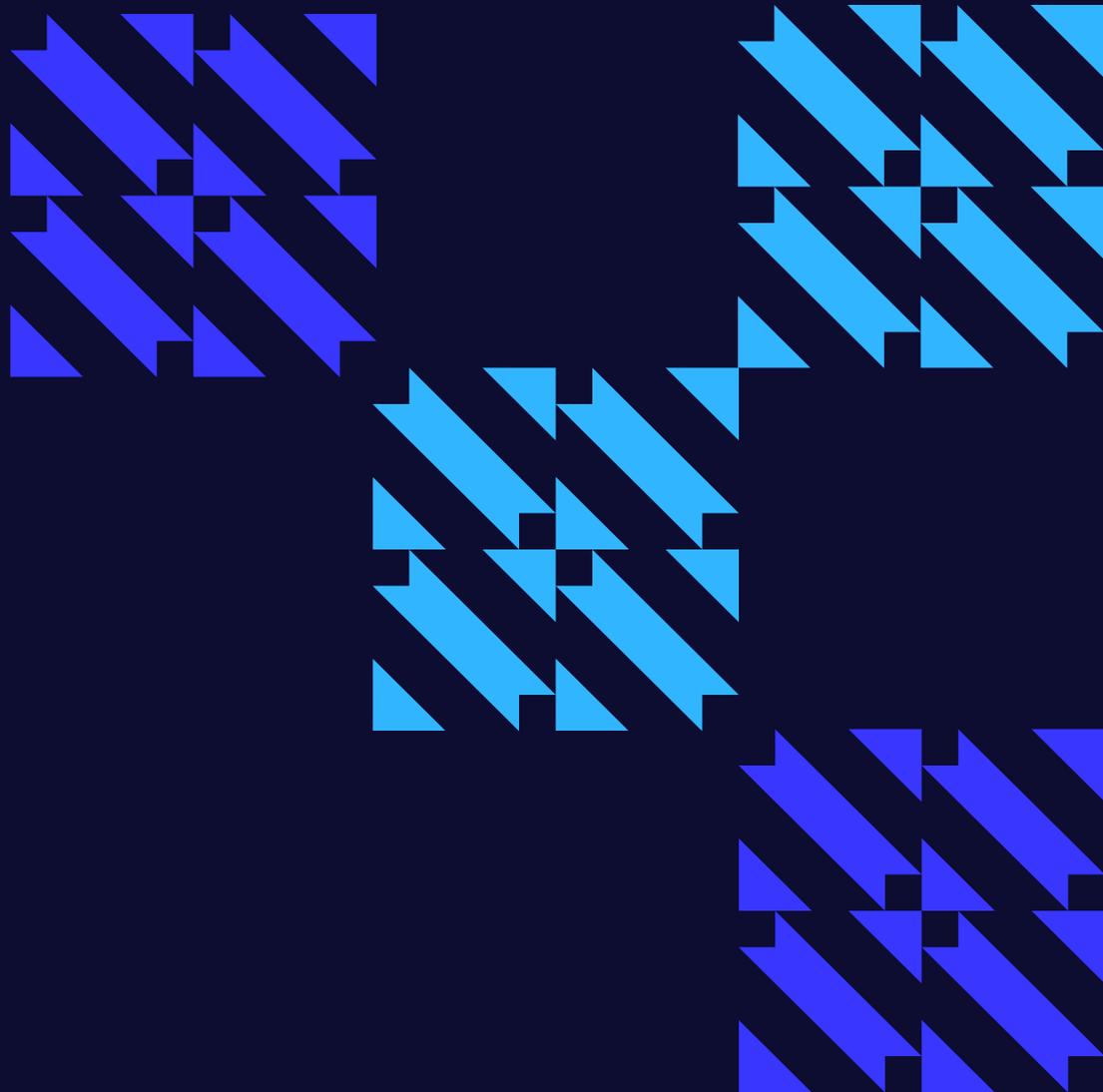
Le baromètre 2024 du CESIN révèle que 49 % des entreprises françaises interrogées ont subi au moins une cyberattaque réussie et impactante dans l'année.

46 %

46 % de l'empreinte carbone liée au numérique en France est imputable aux data centers.

Partie 1

Constats - Enjeux factuels



I Constats - enjeux

A) Des infrastructures qui font tourner le monde

Les data centers, piliers méconnus de notre quotidien numérique...

Développés dans les années 90 avec la montée des usages Internet, les data centers sont des infrastructures sécurisées où sont hébergés les serveurs assurant le stockage et le traitement de nos données numériques. Ces coffres-forts numériques sont sollicités à chaque utilisation de services en ligne (site web, application, logiciels, terminaux mobiles, etc) et doivent garantir, à la fois, la continuité de service, la sécurité des données et des équipements, tout en répondant à des exigences croissantes en matière d'efficacité énergétique et de respect de l'environnement. Ces centres de données assurent donc le fonctionnement quotidien d'un large éventail de services essentiels : paiement en ligne, navigation sur internet, enregistrement de mots de passe, partage de photos, ou encore fonctionnement des outils d'intelligence artificielle.

On distingue généralement deux grandes catégories de data centers. Les data centers d'exploitation détenus par des entreprises ou des administrations, qui y hébergent leurs propres serveurs pour leurs besoins internes. Et en face, les data centers d'infrastructure qui proposent des services d'hébergement à des tiers ou mettent des serveurs à disposition en location. Ce second modèle est largement dominé par de grands acteurs du numérique, essentiellement américains...

... et de l'essor de l'intelligence artificielle.

Le développement fulgurant de l'intelligence artificielle bouleverse un marché des infrastructures numériques déjà sous forte pression. Au cœur de cette transformation, les data centers deviennent un champ de bataille stratégique, et l'Europe y affiche un retard préoccupant. Pourtant, une opportunité majeure se dessine : l'essor des usages liés à l'intelligence artificielle génère des besoins spécifiques et massifs qui pourraient justifier une politique industrielle ambitieuse.

En effet, l'intelligence artificielle impose, à une vitesse inédite, la création de data centers de nouvelle génération, capables de gérer des volumes colossaux de données et une puissance de calcul démultipliée. Pour répondre à cette trajectoire exponentielle, les

infrastructures existantes doivent être redimensionnées, renforcées et rendues hautement évolutives. L'intelligence artificielle n'est pas un simple moteur d'innovation numérique : elle agit comme un accélérateur systémique, reconfigurant les rapports de force industriels à l'échelle mondiale. Or, pour l'instant, l'Europe ne représente que 4% de la puissance de calcul mondiale des intelligences artificielles.

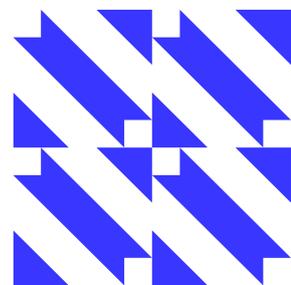
Cette dynamique impose un réalignement stratégique : plusieurs États dont la France, structurent des filières industrielles capables de répondre à cette nouvelle donne. Sur le plan national, les conditions sont réunies : ingénierie d'excellence, stabilité géographique, énergie décarbonée, écosystème dynamique, accompagnement renforcé des projets par les pouvoirs publics. Autant d'atouts qui bien, coordonnés, peuvent faire émerger un leadership dans l'IA et les data centers.

À cette mutation technologique s'ajoutent de nouveaux défis cruciaux : une pression énergétique considérable (plus rapide, plus puissante mais également plus énergivore), des enjeux accrus de cybersécurité et un rythme de transformation effréné. Selon Huawei, la consommation électrique des data centers, aujourd'hui estimée entre 2 à 3 % de la consommation mondiale, pourrait atteindre 13 % d'ici 2030 (et jusqu'à 25% selon McKinsey avec un rythme d'augmentation des besoins de 13% par an en Europe).

Cette dynamique alimente une nouvelle course à la puissance de calcul, où la maîtrise simultanée des data centers, des semi-conducteurs avancés et des matières premières critiques constitue un levier stratégique déterminant. Ceux qui domineront cette chaîne technologique dicteront demain les règles de la maîtrise des flux numériques, de la sécurité des infrastructures critiques et de l'influence géopolitique.

Une profonde dépendance aux acteurs extraeuropéens

Avec près de 3 000 data centers, les États-Unis dominent le marché mondial, tant en nombre qu'en capacité de stockage. Leur puissance totale est estimée à 5 % des capacités d'électricité du pays (soit 23 GW, dont 3,3 GW spécifiquement alloués à



l'intelligence artificielle). En comparaison, l'Europe continentale reste fragmentée : on recense plus de 300 data centers en France, 456 au Royaume-Uni et 487 en Allemagne, mais l'ensemble du continent ne consacre que 0,25 GW à l'intelligence artificielle. La Chine, bien que comptant un nombre légèrement inférieur (443 centres), s'impose comme un acteur incontournable avec certains des plus grands centres au monde — comme celui de China Telecom en Mongolie intérieure, qui atteint 10,7 millions de pieds carrés.

En France, Marseille illustre ce basculement stratégique : cinquième plateforme mondiale d'Internet, la ville est devenue un hub de connectivité internationale grâce à ses câbles sous-marins et à l'implantation de sept data centers. Mais seuls deux sont détenus par des acteurs français. La plupart des data centers en France — notamment dans le domaine de la colocation, c'est-à-dire la location d'espace et de puissance informatique à des tiers — sont opérés par des entreprises américaines ou détenus par des capitaux étrangers (Microsoft, G42, Brookfield, etc.). Cette dynamique, renforcée par les annonces du Sommet de l'IA, illustre une situation paradoxale : bien qu'elle contribue à développer des activités et des emplois localement, elle conforte une dépendance stratégique sur le plan industriel et décisionnel.

Côté cloud et intelligence artificielle, la dépendance est encore plus marquée. En France comme en Europe, plus de 70 % du marché est capté par les hyperscalers — essentiellement américains (AWS,

Microsoft Azure, Google Cloud). Cette domination dans les services cloud se traduit par un contrôle extraterritorial sur les données, des standards propriétaires fermés, et une captation massive de la valeur.

Face à cette double dépendance — infrastructures physiques d'un côté, services numériques critiques de l'autre — la France a engagé une reprise en main à travers un cadre réglementaire rénové et des investissements ciblés. Ainsi, face au manque de coordination au sein de la filière française, le gouvernement a engagé une dynamique écosystémique ambitieuse en lançant les Comités Stratégiques de Filière « Infrastructures Numériques » et « Logiciels et Solutions Numériques de Confiance ». L'objectif : fédérer les acteurs autour de priorités claires et partagées. Cette démarche gagnerait à être étendue à l'échelle du continent pour permettre une collaboration plus structurée et efficace avec nos partenaires européens.

Mais ces efforts ne pourront pleinement porter leurs fruits que dans le cadre d'une stratégie européenne cohérente, capable de mutualiser les ressources, de coordonner les filières industrielles et de promouvoir l'émergence de véritables champions continentaux. En particulier, le manque de structuration des écosystèmes français — comparé, par exemple, à l'organisation industrielle allemande — freine la montée en puissance d'un cloud souverain et limite la coopération stratégique avec nos partenaires européens.

B) Cadres d'action français et européens : deux vitesses, un même défi

Au niveau national, un cadre attractif en pleine transformation

L'année 2025 aura été marquée par un tournant majeur dans la stratégie française autour de l'intelligence artificielle et des infrastructures numériques. À l'occasion du Sommet de l'IA organisé à Paris en février, 109 milliards d'euros d'investissements ont été annoncés dans les data centers et l'IA. Dès le mois de mai, 26 milliards d'euros ont été confirmés lors du sommet Choose France. Ce mouvement s'inscrit dans une dynamique engagée dès 2024, avec déjà 7 milliards d'euros programmés sur ces problématiques.

Au-delà des annonces, une volonté politique claire se dessine, accompagnée d'un effort législatif soutenu pour adapter le cadre réglementaire aux exigences de la révolution numérique. Le projet de loi sur la simplification de la vie économique, adopté à l'Assemblée nationale le 17 juin et en attente d'adoption par la commission mixte paritaire, prévoit un allègement

ciblé des procédures (règles environnementales, urbanisme, raccordement électrique) afin de faciliter l'implantation de nouveaux data centers. Il introduit notamment la possibilité de conférer à certains projets le statut de « projet d'intérêt national majeur » (PINM), ouvrant droit à des procédures exceptionnelles et accélérées. En effet, à cause de la lourdeur des procédures actuelles, il faut aujourd'hui 5 ans en moyenne pour construire un data center en France.

L'objectif est clair : garantir la capacité du pays à héberger ses données sur son propre territoire, première condition d'une autonomie stratégique numérique et réduire la dépendance technologique vis-à-vis des acteurs étrangers et renforcer l'autonomie stratégique de la France. Car les chiffres parlent d'eux-mêmes : la quasi-totalité des projets en cours implique des capitaux étrangers. Microsoft prévoit ainsi d'investir 4 milliards d'euros en France pour étendre ses capacités cloud et IA (notamment à Mulhouse, Marseille et en région parisienne), former aux métiers de l'IA, et soutenir 2 500 startups fran-

çaises. De leur côté, Mistral AI et Bpifrance portent, avec le fonds émirati MGX, un projet de méga-data center de 1,4 GW pour un investissement estimé à 8,5 milliards d'euros.

La société G42, également émiratie, accompagne la modernisation de deux sites dans l'Isère, tandis que le fonds canadien Brookfield prévoit l'installation d'un data center de 1 GW dans le Nord pour un montant de 10 milliards d'euros.

Ces implantations, si elles traduisent un effet d'attraction certain, interrogent toutefois sur la maîtrise stratégique de ces infrastructures : où sont localisées les données ? Qui contrôle les flux ? Qui peut avoir accès aux serveurs ou aux données qui y sont hébergées ? Quels standards de cybersécurité sont imposés ? À ce titre, un point de vigilance concerne la compatibilité entre SecNumCloud — la certification française garantissant un haut niveau de souveraineté des services cloud — et le futur EUCS européen. Ce dernier, encore en cours de définition, pourrait adopter des critères moins stricts, notamment vis-à-vis de l'extraterritorialité des lois étrangères. Une telle divergence risquerait de fragiliser la construction d'un cadre harmonisé de confiance numérique à l'échelle européenne.

Malgré ces interrogations, ces dynamiques confirment que la France dispose d'atouts structurels reconnus : une électricité majoritairement décarbonée (90% en 2024), une capacité de production excédentaire, un cadre stable qui permet d'envisager un déploiement massif de data centers à empreinte carbone maîtrisée, 35 sites pré identifiés compatibles avec l'hébergement de data centers (raccordés au réseau haute tension, avec des surfaces allant de 18 à 150 hectares), une position géographique stratégique, etc. Autant d'éléments qui positionnent la France comme un terrain stratégique pour le développement de l'intelligence artificielle et des infrastructures numériques en Europe.

Au niveau européen, une lente montée en puissance

L'Union européenne a également engagé plusieurs chantiers qui tendent à structurer un cadre commun de régulation et de pilotage stratégique. La directive révisée sur l'efficacité énergétique (2023/1791) impose aux opérateurs de data centers d'une puissance supérieure à 500 kW une obligation annuelle de reporting, portant sur leur consommation d'énergie et d'eau, leur efficacité énergétique (PUE), la part d'énergies renouvelables utilisées, ainsi que la valorisation de la chaleur fatale. Cette transparence, centralisée au sein d'une base de données européenne, doit permettre non seulement une évaluation consolidée des performances, mais aussi une orientation ciblée des financements publics vers les infrastructures les plus sobres et résilientes. À cela s'ajoute une obligation de réutilisation de la chaleur résiduelle pour les centres supérieurs à 1 MW, assortie de sanctions financières en cas de manquement : une incitation claire à l'intégration environnementale des infrastructures numériques.

Sur le volet de la cybersécurité, deux textes européens structurants incarnent cette volonté d'harmonisation et de résilience. Le règlement DORA (Digital Operational Resilience Act) et la directive NIS 2 constituent deux piliers essentiels de la stratégie communautaire. Le premier cible spécifiquement le secteur financier, en lui imposant des exigences renforcées de gestion des risques numériques et de continuité opérationnelle. NIS2 élargit le spectre aux entités opérant dans des secteurs jugés critiques (énergie, santé, transports, infrastructures numériques, etc.), en uniformisant les standards de cybersécurité à l'échelle de l'Union. Ces textes poursuivent une double ambition : d'une part, accroître la résilience collective face à l'intensification des cybermenaces ; d'autre part, limiter la dépendance stratégique à l'égard d'acteurs extra-européens en imposant des obligations de contrôle et de localisation des services. À travers cette régulation, l'Union européenne affirme sa volonté de reprendre la main sur ses infrastructures numériques critiques et de construire une autonomie stratégique fondée sur la sécurité, la confiance et la transparence.

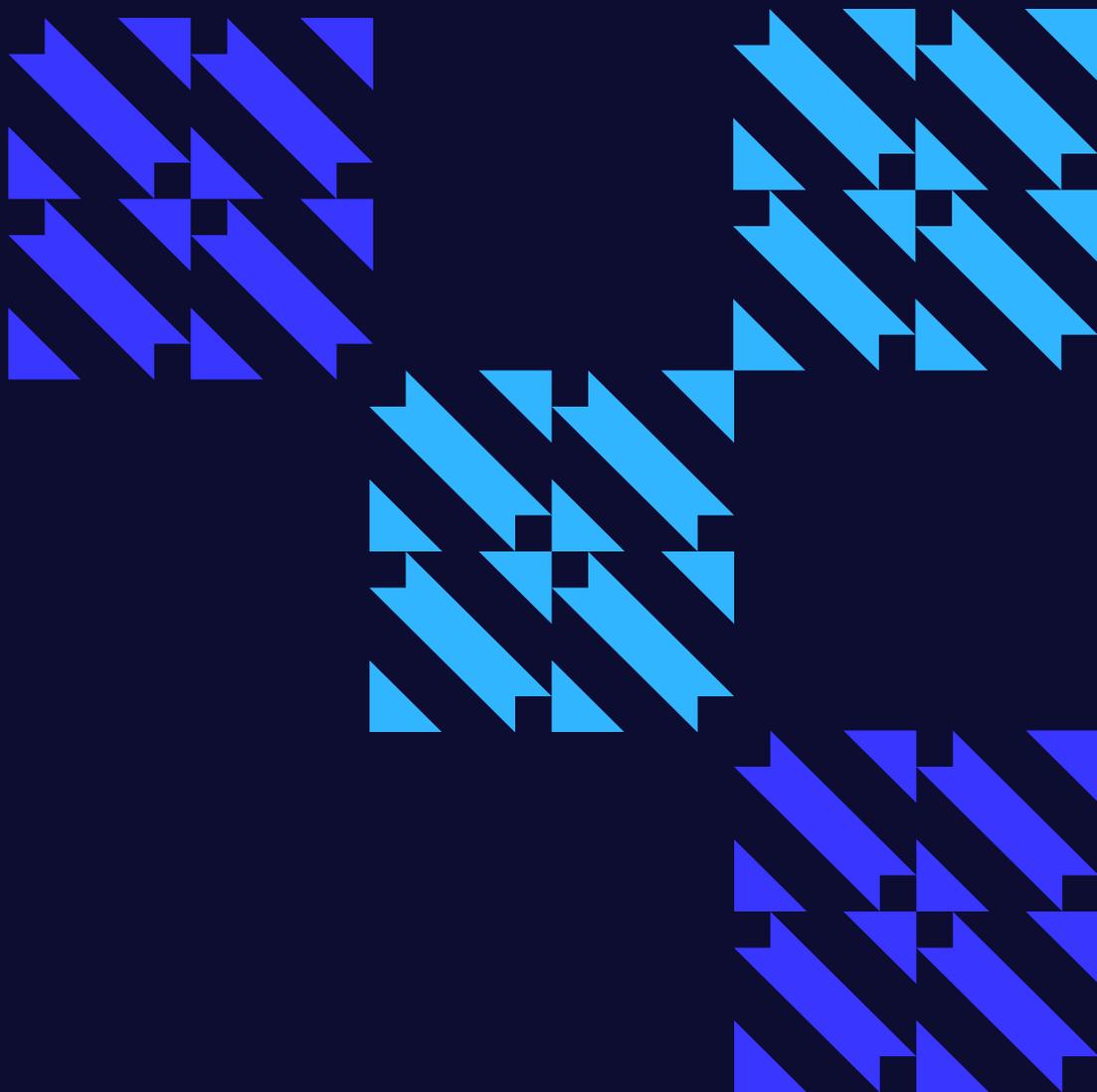
Cette dynamique législative s'accompagne d'un effort de coordination industrielle. Le Code européen de conduite pour l'efficacité énergétique des data centers (EU DC CoC), soutenu par la Commission, réunit aujourd'hui plus de 400 acteurs volontaires (opérateurs, fournisseurs, régulateurs) autour d'un référentiel de bonnes pratiques visant à favoriser l'innovation, la sobriété énergétique et le partage d'expériences. Dans le même esprit, des projets financés par Horizon Europe soutiennent la recherche appliquée sur des solutions de refroidissement durable, l'intégration des énergies renouvelables dans les data centers, et la réduction de leur empreinte environnementale.

Cependant, cette montée en puissance réglementaire et industrielle ne masque pas les fragilités persistantes de l'Union européenne. La capacité de production de serveurs, les chaînes d'approvisionnement en composants critiques et les ressources énergétiques nécessaires au fonctionnement de data centers de nouvelle génération restent, dans leur grande majorité, dépendantes de pays tiers. Le retard européen dans la fabrication de semi-conducteurs, malgré l'impulsion du Chips Act, témoigne d'un déficit d'intégration stratégique dans les segments amont de la chaîne de valeur numérique. Par ailleurs, la faible mutualisation des investissements et l'hétérogénéité des réglementations nationales ralentissent l'émergence d'une coordination européenne complète.

Une fragmentation excessive du numérique européen risquerait de morceler son espace numérique et de fragiliser la mutualisation des infrastructures. La souveraineté numérique européenne ne se construira pas contre les autres mais par une gestion maîtrisée et stratégique de ces alliances.

Partie 2

Défis - menaces



II Défis - menaces

A) Face à une fragmentation industrielle et une dépendance stratégique : une souveraineté à bâtir

L'Europe en position de vulnérabilité numérique

La question de l'hébergement des données est au cœur des enjeux de souveraineté numérique. Longtemps abordée sous l'angle de la protection des données personnelles, la souveraineté s'est imposée dans le débat public avec l'adoption du Cloud Act par les États-Unis en 2018. Cette loi fédérale confère aux autorités américaines un droit d'extraterritorialité leur permettant d'accéder à toute donnée détenue par une entreprise soumise à leur législation, y compris lorsque ces données sont stockées hors des États-Unis. En clair, des données hébergées en France ou en Europe peuvent être réclamées par Washington si elles sont contrôlées, directement ou indirectement, par une entité américaine.

À cette insécurité s'ajoute une nouvelle menace : le shutdown. Un fournisseur non européen peut décider ou être contraint de suspendre la fourniture de ses services à des clients européens, en dégrader les performances, refuser leur montée en charge ou conditionner leur accès à des mises à jour payantes. Cette vulnérabilité rappelle que la maîtrise de l'infrastructure conditionne celle des usages. Ce risque s'amplifie dans un contexte géopolitique incertain : un changement de doctrine à Washington pourrait entraîner la fermeture brutale de services numériques stratégiques pour des raisons politiques, économiques ou de sécurité nationale — exposant ainsi l'Europe à un arrêt partiel de son économie connectée sans recours immédiat.

Face aux risques pesant sur les données, dans le cadre des discussions sur le projet de loi Simplification, les députés ont récemment adopté un amendement visant à exclure du statut de projet d'intérêt national majeur (PINM) les datacenters dont le propriétaire ou l'opérateur relève de la législation d'un pays tiers à l'Union européenne ne garantissant pas un niveau de protection des données équivalent à celui du RGPD. En l'état, et dans l'attente des débats en Commission mixte paritaire, certains acteurs étrangers pourraient donc être exclus de ce statut, y compris les acteurs américains si le Data Privacy Framework venait à être invalidé.

Le choix d'un fournisseur cloud est ainsi devenu un acte stratégique pour toute organisation. Plusieurs initiatives françaises traduisent la volonté de bâtir une alternative crédible aux géants non-européens. Le projet NumSpot

(Docaposte, Bouygues Telecom, Dassault Systèmes, Banque des Territoires) propose une offre souveraine certifiée SecNumCloud par l'ANSSI. Le projet Bleu, porté par Capgemini et Orange en partenariat technologique avec Microsoft, progresse vers cette même certification. OVHcloud propose un catalogue de services équivalents à celui des acteurs majeurs du marché et bénéficie des plus hauts niveaux de certification européens, dont SecNumCloud. Enfin, Mistral AI a implanté son premier data center chez Eclairion, spécialisé dans l'hébergement en colocation de calculateurs haute densité, illustrant l'alignement entre innovation et autonomie stratégique.

Ces initiatives traduisent une dynamique nationale structurante. Malgré les dépendances persistantes, la France avance vers un écosystème numérique plus souverain, sécurisé et compétitif. Mais cette progression se heurte à une réalité européenne plus préoccupante : l'absence d'un champion cloud intégré, capable de rivaliser avec les hyperscalers américains, et une dépendance technologique critique sur de nombreux maillons de la chaîne de valeur — serveurs, composants, logiciels, services managés — dominée par des acteurs non-européens.

Cette vulnérabilité s'accompagne d'une menace croissante sur la sécurité des données. Selon Statista, le coût des cyberattaques en France a atteint 119 milliards d'euros en 2024. Le baromètre 2024 du CESIN révèle que 49 % des entreprises françaises interrogées ont subi au moins une cyberattaque réussie et impactante dans l'année. Ce constat illustre à la fois l'intensité de la menace et l'urgence d'investir dans une cybersécurité robuste.

La sécurité des data centers devient ainsi un enjeu stratégique. Une faille peut exposer des secteurs vitaux — santé, énergie, défense, services publics — à des attaques majeures. Les data centers de niveau 3 et 4 offrent des garanties élevées en matière de continuité, redondance et résilience. Des outils comme les SIEM (Security Information and Event Management) renforcent la capacité de détection et de réaction face aux menaces.

Sécuriser les data centers n'est plus une option : c'est une condition essentielle à la résilience numérique nationale, à la protection des intérêts stratégiques

et à la compétitivité économique. À l'échelle européenne, une véritable stratégie de souveraineté doit se construire autour de ces infrastructures critiques, jusqu'aux technologies de rupture comme le quantique, indispensable à la maîtrise de l'intelligence artificielle de demain. Sans projection stratégique sur les capacités d'hébergement, de calcul et d'interconnexion, les efforts actuels sur le cloud, les données et l'IA resteront incomplets.

La course technologique impose une vision d'anticipation : sans data centers implantés sur le territoire national, maîtrisés par des acteurs souverains et adaptés aux besoins de demain — y compris en calcul intensif et quantique — l'Union européenne risque un déclas-

sement durable. Forte de ses initiatives pionnières, de ses atouts énergétiques, de la qualité de ses talents et de son écosystème en structuration, la France peut jouer un rôle moteur en entraînant ses partenaires vers une vision commune du cloud de confiance et de l'indépendance technologique.

Mais cette ambition ne pourra se concrétiser que dans une dynamique collective. C'est en mobilisant le cadre européen que la France transformera son avance nationale en levier d'influence. L'initiative InvestAI, dotée de 200 milliards d'euros, envoie un signal fort : celui d'une volonté partagée de bâtir une autonomie technologique durable, résiliente face aux logiques de dépendance imposées par les superpuissances numériques.

Stratégie commune : des initiatives encore trop faibles

Des initiatives qui coordonnent l'effort européen existent. On peut citer, le projet Gaia-X, lancé en 2020 à l'initiative de la France et de l'Allemagne et qui vise à bâtir une fédération européenne de services cloud décentralisés reposant sur des standards ouverts, interopérables et transparents. Porté par une association à but non lucratif, le projet réunit aujourd'hui près de 300 membres issus de l'industrie, du numérique et de la recherche. L'objectif : offrir aux utilisateurs (organisations et espaces de données) une réelle liberté de choix de leurs services de cloud par la fourniture d'informations comparables et transparentes reposant sur un socle commun de règles de sécurité, de souveraineté des données et de gouvernance éthique. Mais malgré ses promesses, Gaia-X peine à produire des effets concrets à grande échelle. Les difficultés de pilotage, les divergences nationales et la participation controversée d'acteurs non européens (Microsoft, Huawei) ont brouillé la lisibilité de l'initiative.

En 2023, une coalition de parlementaires fran-

çais, eurodéputés et représentants de l'écosystème tech, ont, eux, porté le Buy European Tech Act pour instaurer une préférence européenne dans les marchés publics numériques. L'objectif : rééquilibrer la compétition face aux géants américains et chinois, en favorisant les solutions cloud, logiciels et services IT issus de fournisseurs européens. Ce projet, encore à l'état de proposition, vise à stimuler la relocalisation industrielle, protéger les données stratégiques des institutions publiques et renforcer la montée en gamme des technologies européennes. Inspiré du Buy American Act aux États-Unis, il cristallise un tournant potentiel dans la politique industrielle de l'UE, à condition de surmonter les contraintes juridiques (règles de l'OMC, concurrence intra-européenne) et d'obtenir un soutien politique fort à Bruxelles. Les auditions récemment menées dans le cadre des travaux de la Commission d'enquête sénatoriale sur la commande publique mettent également en évidence l'attention croissante portée, en France, à l'introduction d'une préférence européenne dans les marchés publics.

Un écosystème fragmenté et une industrie encore inaboutie face aux hyperscalers

Malgré des avancées réglementaires notables, l'Union européenne reste confrontée à de profondes faiblesses industrielles qui compromettent sa capacité à rivaliser avec les grandes puissances numériques. Le marché européen demeure fragmenté, tiraillé entre des politiques nationales peu coordonnées, des réglementations hétérogènes et des investissements rarement mutualisés. Cette dispersion freine la montée

en puissance d'un écosystème intégré et compétitif, empêchant l'émergence de champions continentaux capables de rivaliser avec les hyperscalers américains ou chinois.

Premier frein, sur le plan technologique, l'Union accuse un retard critique sur les semi-conducteurs avancés : seuls 10 % des puces mondiales sont produites en Europe, un chiffre que le Chips Act vise à doubler d'ici 2030 — sans garantie de souveraineté sur les technologies de pointe. Par ailleurs, l'Union pèse peu dans la

gouvernance mondiale des standards numériques : qu'il s'agisse des protocoles d'Internet, des normes d'interopérabilité ou des architectures cloud, son influence reste marginale, largement dépassée par les agendas technologiques américains ou chinois. Ce déficit industriel est particulièrement visible dans le domaine du cloud. Malgré une volonté affichée de souveraineté, plus de 70 % du marché européen du cloud est capté par trois entreprises américaines : AWS, Microsoft et Google. Ce déséquilibre n'est pas seulement technologique, il est aussi géoéconomique : il expose les États membres à une dépendance critique, tant juridique — via l'extraterritorialité de lois comme le Cloud Act — qu'économique, par la captation de valeur (« LLMisation » de l'économie) et de données stratégiques.

Or, les data centers ne sont pas de simples infrastructures techniques : ce sont des actifs souverains. Leur contrôle conditionne la maîtrise des flux numériques, la sécurisation des activités critiques et la résilience des chaînes de valeur. Et l'Europe ne manque pas d'atouts pour faire émerger une puissance industrielle numérique européenne : réseau électrique relativement décarboné, forte densité de marché, vivier de compétences en ingénierie numérique, et capacité d'investissement public significative (InvestEU, Fonds européen pour l'innovation, Chips Act). Encore faut-il une stratégie industrielle claire, mutualisée et cohérente pour transformer ce potentiel en puissance.

Au-delà de leur fonction numérique, les data centers peuvent aussi devenir des leviers d'indépendance énergétique. Mieux intégrés aux réseaux, ils facilitent l'absorption des énergies renouvelables intermittentes et contribuent à stabiliser le système électrique européen. Leur implantation à proximité des pôles de production de données stratégiques (recherche, industrie, services publics) renforce également la sécurité des flux et la souveraineté des usages.

L'avenir des data centers européens ne peut être pensé en silo. Il s'inscrit dans une géoéconomie du numérique, où produire, héberger, sécuriser et interconnecter les données devient un attribut clé de la puissance stratégique. Pour éviter que l'Union européenne ne soit réduite à un espace de transit entre deux superpuissances numériques, il est impératif de bâtir un réseau d'infrastructures critiques européennes, fondé sur une gouvernance partagée, des normes communes et une stratégie industrielle ambitieuse.

La commande publique, levier stratégique encore sous-utilisé

Dans cette dynamique de construction d'une autonomie technologique, la commande publique représente un levier stratégique encore insuffisamment mobilisé. Face à la captation de valeur par les géants extra-européens, plusieurs initiatives cherchent à réorienter les flux de commande vers les acteurs européens.

Dans le même esprit, le 22 mai 2025, plus de 300 entreprises françaises — dont Mistral AI, Airbus, Michelin, Orange, Crédit Agricole ou Station F — se sont réunies au sein de consortiums comme l'Innovation Makers Alliance pour défendre une souveraineté numérique européenne, notamment à travers la transformation de la commande publique. Leurs propositions : création d'une plateforme d'appels d'offres publics et privés, instauration d'un « bonus souveraineté », et réservation d'une part des marchés aux PME et start-up technologiques européennes. Objectif : stimuler la demande intérieure et ancrer durablement l'innovation sur le territoire.

La commande publique représente pourtant un levier économique majeur, avec près de 2 000 milliards d'euros mobilisés chaque année, à l'échelle européenne, par plus de 200 000 agences. Cette puissance d'achat pourrait être davantage orientée vers les acteurs garantissant la protection contre les lois extraterritoriales et soutenant la souveraineté technologique du continent. À ce titre, l'étude du Cigref, publiée en avril 2025, met en lumière les bénéfices économiques d'une telle mesure : si 15 % des dépenses liées aux logiciels et services cloud à usage professionnel en Europe étaient réorientées vers des acteurs européens, cela générerait environ 75 milliards d'euros de chiffre d'affaires et près de 500 000 emplois. Certains acteurs publics commencent à intégrer ces critères dans leurs appels d'offres, pondérant les solutions selon leur niveau de résilience juridique et technique.

La commande publique doit constituer un vecteur de transformation décisif : elle doit permettre de sécuriser un débouché, financer l'amorçage technologique et faire émerger une offre compétitive alignée sur les standards européens. Elle n'est donc pas seulement un outil de soutien, mais un véritable instrument de politique industrielle, qui doit être utilisé au service du renforcement de l'offre européenne.

B) Sobriété numérique : le défi environnemental des data centers

Indispensables à l'économie numérique, les data centers soulèvent toutefois d'importants défis environnementaux. Leur consommation électrique est particulièrement élevée, en raison du fonctionnement continu des serveurs et de leur besoin de refroidissement. Selon l'ADEME et l'Arcep, 46 % de l'empreinte carbone liée au numérique en France est imputable aux data centers. L'Agence internationale de l'énergie estime que la consommation électrique mondiale de ces infrastructures pourrait atteindre, d'ici cinq ans, l'équivalent de celle du Japon.

L'impact environnemental ne se limite pas à l'électricité. La question de la consommation d'eau est de plus en plus discutée, notamment avec l'essor de l'IA générative. Certaines estimations, fondées sur des pratiques américaines, avancent qu'il faudrait près d'un demi-litre d'eau pour générer entre 10 et 50 questions d'intelligence artificielle. Toutefois, ces données doivent être fortement nuancées : la majorité des data centers en France utilisent des systèmes de refroidissement fermés ou à air, très peu consommateurs d'eau, sauf en cas de pics de chaleur extrêmes. Contrairement aux États-Unis, où de nombreux centres de données — notamment ceux d'Amazon, Google ou Microsoft — sont installés dans des régions arides et recourent massivement à l'eau pour le refroidissement, la situation française est bien différente. À ce titre, France Datacenter rappelle régulièrement que les chiffres alarmistes largement relayés dans les médias ne reflètent pas les réalités du secteur français.

Plus largement, les data centers peuvent avoir un effet local sur la température ambiante lorsqu'ils rejettent la chaleur issue du refroidissement dans l'atmosphère. Ils peuvent aussi abriter des équipements

sensibles, comme des cuves à fioul, des gaz fluorés ou des batteries au plomb ou au lithium. Néanmoins, ces installations sont rigoureusement encadrées. Tous les sites sont soumis à la réglementation sur les installations classées pour la protection de l'environnement (ICPE), ce qui implique des autorisations strictes. Par ailleurs, l'usage des gaz fluorés est en nette diminution, voire supprimé sur certains sites au profit de solutions plus vertes.

La France dispose de plus de 300 data centers, largement alimentés par une électricité décarbonée (à plus de 90 % grâce au nucléaire et aux énergies renouvelables). OVHcloud, par exemple, utilise 92 % d'énergies renouvelables sur ses sites. Ces performances font de la France un territoire pionnier en matière d'écoresponsabilité numérique. À l'inverse, certains projets récents menés à l'étranger interrogent. Amazon prévoit par exemple d'implanter trois nouveaux centres de données dans la région sèche d'Aragon, en Espagne, avec une consommation estimée supérieure à celle de l'ensemble de la région, équivalente à l'irrigation de 233 hectares de maïs — sans même compter l'eau nécessaire à la production d'électricité.

Ces éléments rappellent la nécessité de favoriser l'implantation de data centers en France et en Europe, là où les conditions énergétiques, climatiques et réglementaires permettent un impact environnemental mieux maîtrisé. Faute de quoi, la montée en charge des usages — notamment liés à l'IA — risque d'alimenter une dépendance accrue à des infrastructures situées dans des zones moins durables, et de creuser un déséquilibre écologique au niveau mondial.

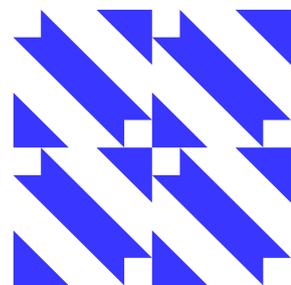
La chaleur des data centers : un potentiel qui pourrait être valorisé ?

Les data centers génèrent une chaleur fatale massive, souvent gaspillée alors qu'elle pourrait être valorisée pour chauffer des logements ou des équipements publics à proximité. Cependant, les projets de récupération de cette chaleur restent marginaux, en raison de coûts d'investissement élevés, de températures souvent trop basses (souvent <math><30^{\circ}\text{C}</math>), et de l'éloignement des sites par rapport aux zones habitées. On peut citer l'exemple du géant américain Equinix qui fournit 9GWh de chaleur fatale pour alimenter une partie du centre aquatique olympique et la zone d'aménagement concerté de la Plaine Saulnier. L'entreprise a également atteint son objectif d'énergies 100% renouvelables en Europe grâce, par exemple, à des fermes éoliennes en France.

L'Union européenne s'est également mobilisée pour accompagner cette transition qui vise à réduire l'impact environnemental des data cen-

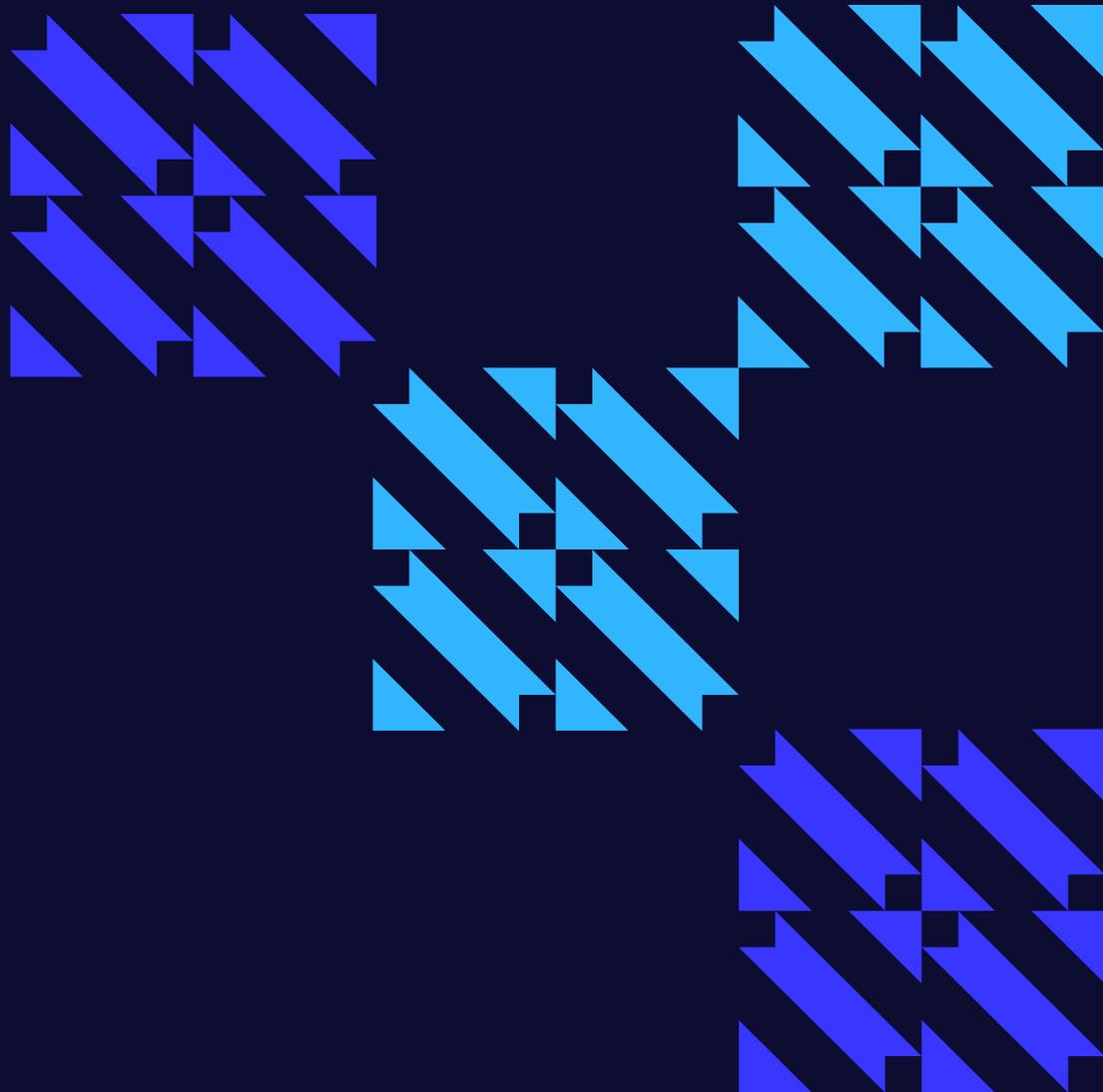
ters. La directive sur l'efficacité énergétique de 2023 contraint les data centers les plus puissants à valoriser la chaleur produite. Une évolution prometteuse, mais encore entravée par des freins techniques et économiques.

Parmi les solutions émergentes, la géothermie de surface offre également un double intérêt : en contribuant au refroidissement décarboné des infrastructures, elle limite la production de chaleur fatale en amont, tout en permettant, dans certains cas, de stocker temporairement l'excédent de chaleur pour une valorisation différée via les réseaux de chaleur. Bien que peu développée à ce stade, elle constitue une piste prometteuse pour renforcer la performance énergétique et la résilience des data centers.



Partie 3

Propositions



III Propositions

A) Trouver l'équilibre entre soutien public et pression régulatrice

Vers une stratégie européenne intégrée pour des data centers souverains, durables et compétitifs

L'Europe se trouve à un tournant stratégique dans la construction de sa souveraineté numérique. Celle-ci ne pourra s'ériger que dans la durée, par l'articulation étroite du droit, de la technologie, de l'innovation, de l'énergie, des ressources minérales et du capital humain. Les data centers peuvent devenir les piliers d'une puissance numérique durable — à condition d'être pensés, construits et pilotés à l'échelle européenne. Car face à l'accélération des transformations numériques et à l'intensification des rivalités géoéconomiques, le cadre législatif français, aussi volontariste soit-il, reste insuffisant pour peser seul face aux dynamiques mondiales. C'est en mutualisant et coordonnant nos efforts, nos compétences et nos infrastructures que l'Union européenne pourra prétendre à une véritable autonomie stratégique, fondée sur une maîtrise collective des flux, des technologies et des usages.

1. Structurer une politique industrielle européenne du numérique

- **Subordonner les objectifs nationaux à une stratégie de filière européenne**, en fixant des feuilles de route communes sur les infrastructures critiques (cloud, data centers, IA), afin d'aligner les investissements, les normes et les priorités de développement.
- **Favoriser la constitution de groupements d'entreprises européennes**, à l'image du modèle Airbus, pour mutualiser les efforts de R&D, accélérer l'innovation, et faire émerger des champions industriels continentaux. L'objectif : créer un véritable « Airbus du cloud » en fédérant les principaux acteurs du numérique autour d'infrastructures partagées, interopérables et souveraines, capables de rivaliser avec les hyperscalers étrangers.
- **S'inspirer du modèle américain en instaurant un « Buy European Tech Act »**, visant à réserver une part des marchés publics et des achats stratégiques aux entreprises européennes du numérique. En fléchissant plus systématiquement la commande publique – près de 2 000 milliards d'euros annuels en Europe – vers des solutions locales et souveraines, il s'agit de transfor-

mer l'acte d'achat en levier d'autonomie stratégique et de financement de l'innovation.

- **Encourager l'émergence de services européens compétitifs** en encourageant les utilisateurs, privés et publics, à se réunir pour en confier le développement à un acteur ou un consortium d'acteurs sélectionné, auquel ils garantissent un montant et une durée minimum de commandes à l'issue du développement. Cet « appel à développement de service » pourrait être assorti de pénalité, pesant sur le fournisseur en cas d'échec ou de retard dans la réalisation du projet.

- **Construire une fiscalité européenne incitative en mettant en place une fiscalité commune sur les services numériques et les data centers**, pour lutter contre le dumping fiscal intra-européen, harmoniser les conditions de concurrence, et financer les infrastructures souveraines.

2. Décentraliser et territorialiser les infrastructures numériques

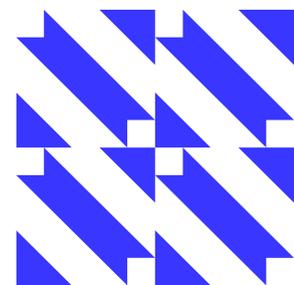
- **Soutenir l'implantation de micro data centers (edge computing)** dans les territoires ruraux, industriels ou isolés, pour réduire la latence, désaturer les grands pôles urbains, et renforcer la résilience locale.
- **Adapter les règles d'aménagement et de raccordement électrique** pour favoriser l'émergence de ces data centers décentralisés, tout en assurant un maillage cohérent avec les priorités énergétiques et industrielles régionales.
- **Développer et promouvoir des standards techniques européens ouverts et interopérables**, afin de limiter la dépendance aux solutions propriétaires et de structurer un écosystème numérique européen résilient et compétitif.
- **Impliquer pleinement les collectivités territoriales** (régions, départements, agglomérations) dans la stratégie numérique. Leur rôle est déterminant pour ancrer la souveraineté numérique dans les territoires, à l'image de ce que représente une banque locale pour l'épargne : une donnée produite localement devrait pouvoir être hébergée localement.

3. Faire des data centers un levier de transition écologique

- **Créer un label européen des data centers circulaires**, valorisant ceux intégrant des pratiques exemplaires : réemploi de matériel, recyclage des composants électroniques, récupération des eaux usées, matériaux bas carbone.
- **Instaurer des quotas d'usage de chaleur fatale** imposant la réutilisation d'un pourcentage minimal de la chaleur produite, avec un suivi public et des incitations économiques.
- **Encourager, en partenariat avec RTE, la flexibilité énergétique des data centers**, en favorisant ceux capables d'ajuster leur consommation en temps réel selon la disponibilité d'électricité renouvelable.
- **Fixer des objectifs ambitieux en matière d'efficacité énergétique et hydrique**, afin de guider l'ensemble de la filière vers une sobriété accrue dans l'usage de ces ressources.

4. Renforcer la coopération vertueuse au-delà de l'espace européen

- **Nouer des alliances technologiques stratégiques avec des États tiers partageant les standards européens** de transparence, de non-ingérence et de respect des libertés numériques (Canada, Japon, Inde), afin de sécuriser les échanges de données et les chaînes de valeur critiques.
- **Co-développer avec ces partenaires des projets structurants** (cloud, IA, cybersécurité) dans une logique de co-innovation et de réciprocité, pour bâtir une «route de la soie numérique» fondée sur la souveraineté partagée.



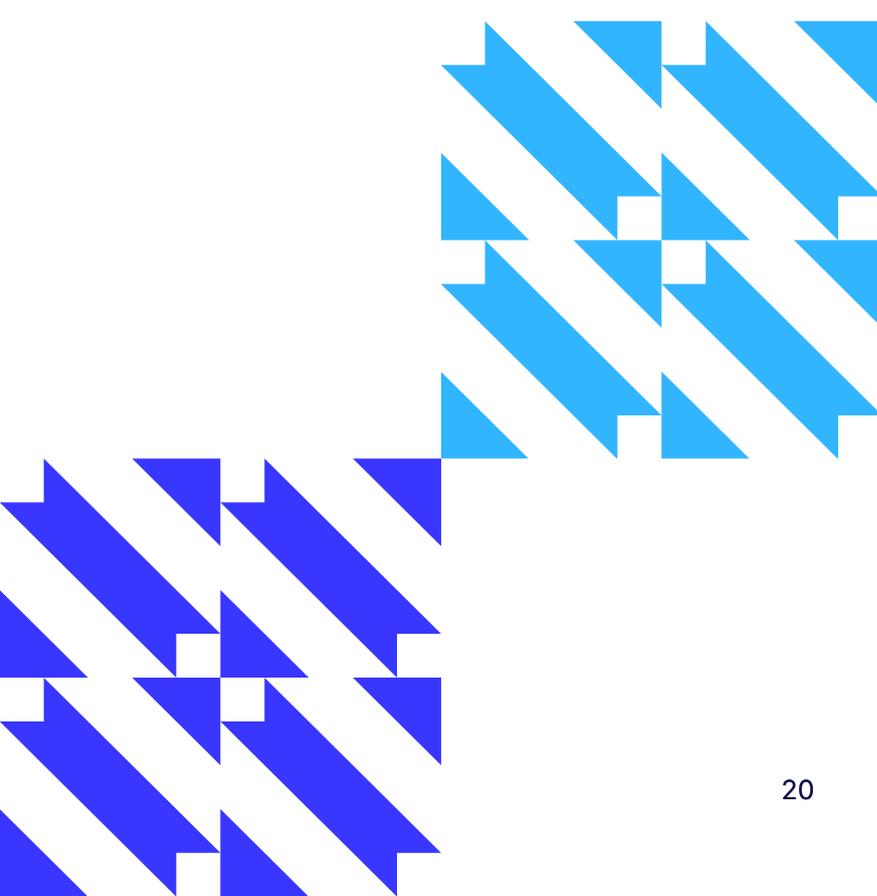
Institut Choiseul

L'Institut Choiseul est un think and do tank indépendant et non partisan. Il se dédie au décryptage des grands enjeux économiques et à la fédération de la jeune génération économique.

Pour alimenter le débat public et incarner les dynamiques économiques en cours, l'Institut Choiseul produit des Notes Stratégiques, des études ponctuelles et des palmarès de jeunes décideurs. Pour fédérer et animer ses communautés, il déploie des événements de haut-niveau mêlant networking convivial, témoignages d'experts et de praticiens et échanges sur des sujets de prospective, sur différents territoires et verticales économiques, en France, en Europe et en Afrique.

Au croisement de la communauté d'affaires et du cercle de réflexion, l'Institut Choiseul offre une plateforme aux décideurs économiques privés comme publics pour s'identifier mutuellement, se mettre en réseau, promouvoir leurs initiatives et réfléchir aux grandes tendances économiques de demain.

À propos



Les partenaires de l'Initiative Souveraineté

L'Institut est accompagné par un noyau dur de partenaires fondateurs, tous acteurs français ou européens, qui prennent une part active à la discussion et à la formalisation de recommandations :



AIRFRANCEKLM
GROUP



Allianz

Amundi
ASSET MANAGEMENT

antidox



Butagaz
GAZ & ÉLECTRICITÉ

Capgemini



EightAdvisory

eraMET

ESL&NETWOI
Groupe ADIT

LE GROUPE
Groupama

GICAN

GICAT
Groupement des Industries Françaises de défense
et de sécurité terrestres et aéroterrestres

Lithium
de France
chaleur & lithium géothermal

matmut

MBDA

NAVAL
GROUP

PMI
PALUEL-MARMONT
INVESTISSEMENT

saur

Séché

SEGULA
TECHNOLOGIES

SNCF

TELEHOUSE
Every connection matters

THALES

14, rue Gaillon
7502 Paris, France

EMAIL
contact@choiseul.info

www.choiseul.info

YOUTUBE
Institut Choiseul

TWITTER / X
@instchoiseul

LINKEDIN
Institut Choiseul

Ce Briefing ne peut être vendu.
© Choiseul 2025. Tous droits réservés.

INSTITUT CHOISEUL

