

L'ombre du Cloud : armer l'Europe dans la guerre invisible des données

AUTEUR Gilles Babinet, Milena
Harito

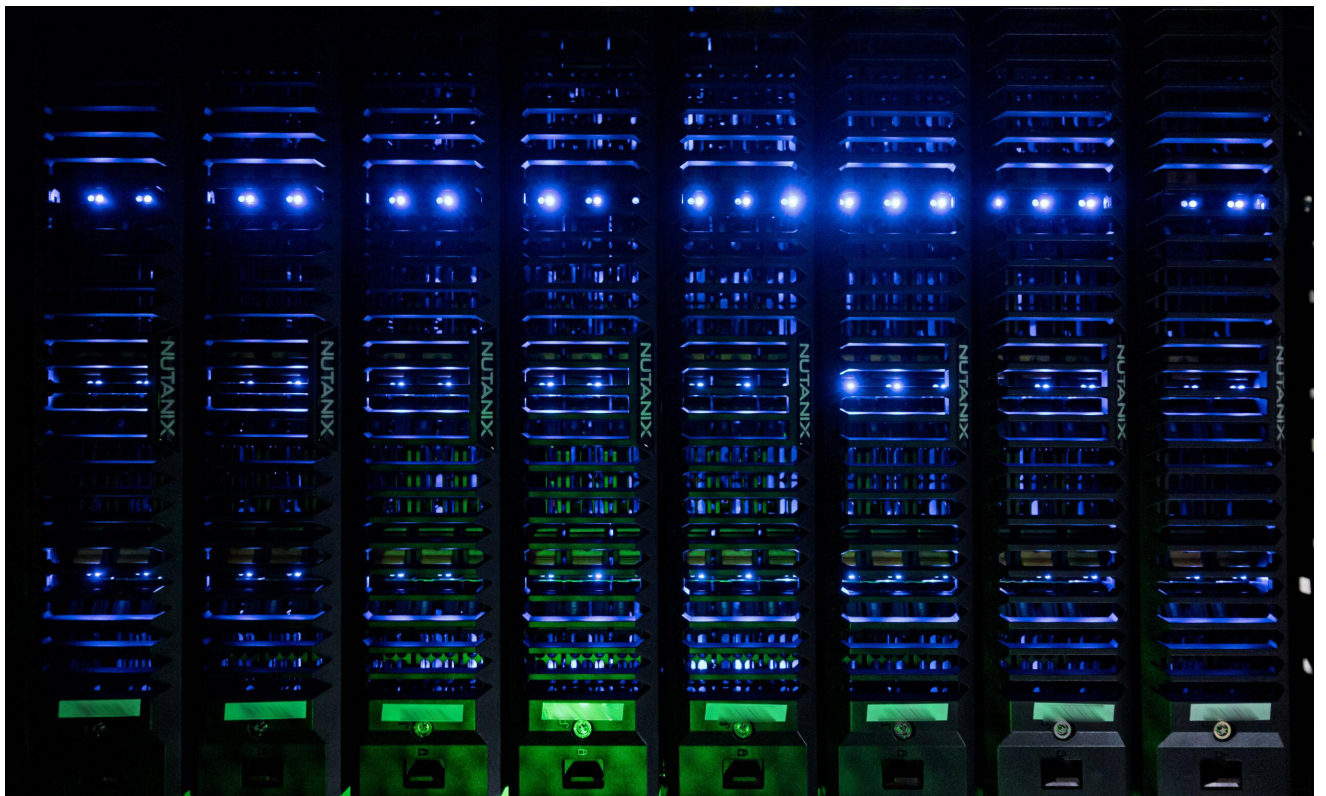
IMAGE © SYSPEO/SIPA

DATE 1 mai 2025

La propriété et la gestion de nos données personnelles ont fait de l'Union un protectorat numérique américain.

Échapper à cette emprise suppose de comprendre ce qui nous menace et dans quelles infrastructures il est aujourd'hui urgent d'investir.

Gilles Babinet et Milena Harito proposent une cartographie — et formulent des recommandations concrètes.



Dans l'étau inquiétant qui a pris la forme d'une alliance entre Trump et Poutine, l'Union européenne a, depuis cent jours, pris brutalement conscience de sa vulnérabilité si un conflit armé direct venait à se déclarer contre elle. Mais elle est soumise à d'autres risques considérables en cas d'agressions plus hybrides et horizontales. En particulier, elle se trouve particulièrement exposée sur le front de tout ce qui relève des technologies numériques.

Des hôpitaux aux banques, des modes de transport ferroviaire et aéroportuaire à nos courriels et messageries diverses, nos vies s'organisent autour de services numériques. Un dysfonctionnement mineur pourrait créer d'immenses troubles, comme l'a montré la panne informatique, non intentionnelle, qui a touché le monde entier en juin 2024 ou encore récemment les impressionnantes coupures de courant qui ont paralysé l'Espagne.

La liste des services vulnérables est longue – et ne cesse de croître.

Ces services sont fournis en Europe majoritairement par quelques entreprises américaines qui ont accumulé une puissance parfois plus importante que de nombreux pays. Certains États se rendent désormais compte de l'ampleur de leur dépendance : des armements comme l'avion F-35 sont en pratique des systèmes informatiques comprenant des millions de lignes de code, dont le fonctionnement dépend du gouvernement des États-Unis. Malgré les dénégations du Pentagone, il n'y a guère de doute sur le fait que celui-ci pourrait en prendre le contrôle par de multiples moyens – arrêt des mises à jour, arrêt des services numériques à distance ou utilisation de « *backdoors* » (portes dérobées).

Cette situation de dépendance extraordinaire s'est progressivement mise en place au cours des trente dernières années.

Bien entendu, les Européens ne peuvent pas débrancher tout système logiciel d'origine américaine du jour au lendemain.

Cela serait proprement impossible – et surtout pas nécessairement utile. Mais il serait tout aussi inconséquent de se braquer dans une position de faiblesse. Dans le nouvel ordre mondial qui se profile, encerclant chaque jour davantage l'Europe, la défense de nos frontières, de notre économie, de notre mode de vie et de nos valeurs devra se penser d'une manière nouvelle.

Nous devons cerner ce risque avec clairvoyance tant il est vrai que la domination par le numérique peut aller bien plus loin que les rapports de forces entre États, tels que nous les connaissons aujourd'hui.

Dès lors, il importe de définir, par ordre d'importance, les points d'exposition de nos vulnérabilités numériques et de créer une feuille de route pour y remédier progressivement.

En matière d'infrastructures, un dysfonctionnement mineur pourrait créer d'immenses troubles.

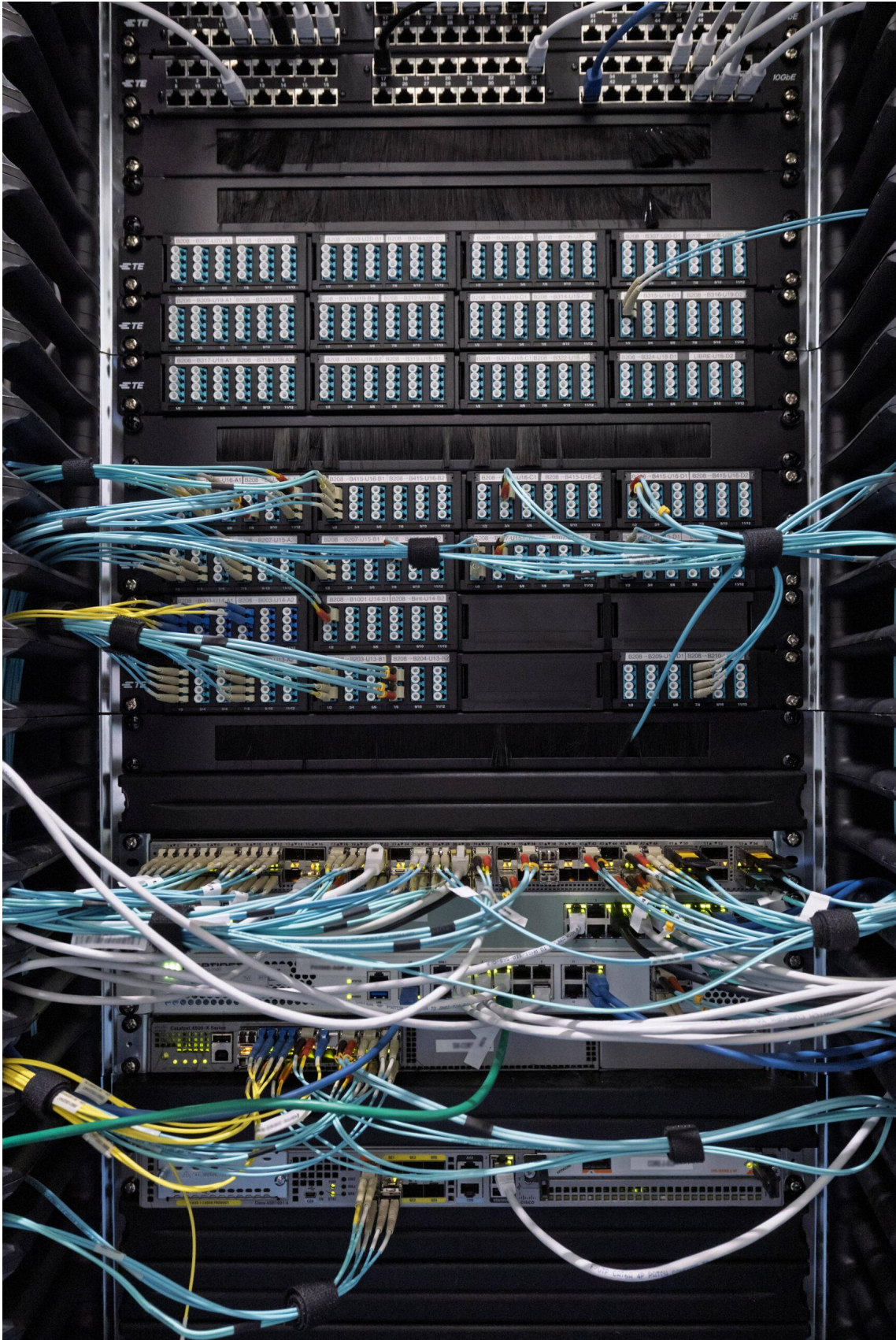


GILLES BABINET ET MILENA HARITO

Ces vulnérabilités relèvent de trois grandes catégories : la maîtrise de l'infrastructure numérique essentielle ; les services numériques – indispensables à notre résilience, mais aussi à notre compétitivité, car c'est bien dans le secteur numérique que la productivité de l'Europe a décroché depuis les années 2000 ; et la protection face à la croissance des cyberattaques et de la désinformation.



« Des hôpitaux aux banques, des modes de transport ferroviaire et aéroportuaire à nos courriels et messageries diverses, nos vies s'organisent autour de services numériques. Un dysfonctionnement mineur pourrait créer d'immenses troubles. »



« Les Européens ne peuvent pas débrancher tout système logiciel d'origine américaine du jour au lendemain. »

L'infrastructure numérique critique de l'Europe : la vulnérabilité du Cloud

En cas de guerre hybride, le point de vulnérabilité maximal des Européens, et qui subirait les impacts les plus lourds, serait l'infrastructure numérique, avec ses nombreuses couches matérielles et logicielles.

Les deux piliers de l'infrastructure indispensable – et pourtant peu visible – de notre vie numérique sont les réseaux de télécommunications et le *Cloud*.

Chacun saurait dire ce que sont les réseaux de télécommunications : des fibres, des antennes mobiles, parfois des satellites et de nombreux équipements complexes, qui permettent de réaliser les communications.

Au-dessus de ces réseaux de télécommunications, notre vie personnelle, économique et publique se passe en grande partie dans des centres de données – que nous désignons par l'expression floue de « *Cloud* ». S'il arrive que nous ayons encore quelques gigabits de données stockés dans les disques de nos ordinateurs ou dans nos entreprises, une grande partie d'entre elles s'est déjà envolée vers le « Nuage » – des photos de nos téléphones portables jusqu'aux données beaucoup plus vitales des entreprises ou des organismes publics.

Les systèmes d'information et les bases de données massives de notre vie numérique se trouvent dans ces centres gigantesques, composés d'infrastructures physiques, de connectivité, d'énergie, de supercalculateurs, ainsi que de nombreuses couches de logiciels et d'outils informatiques sophistiqués – y compris d'intelligence artificielle. Ces logiciels constituent la valeur ajoutée du *Cloud*. Ils demandent beaucoup d'investissements et d'innovation et sont au centre d'une compétition commerciale féroce, mais aussi – et peut-être surtout – d'une compétition pour le contrôle des données.

Alors que les réseaux de télécommunications sont déployés physiquement en Europe et sont en majorité opérés par des entreprises européennes, le *Cloud* est détenu et opéré pour environ 65 % par trois entreprises américaines : Google, Microsoft et Amazon. Certes, les centres de données peuvent être physiquement situés en Europe ou aux États-Unis. Mais les couches logicielles qui apportent la valeur ajoutée du *Cloud* restent contrôlées par ces entreprises de la *Big Tech*. L'Europe est aujourd'hui dépendante de celles-ci, comme des lois américaines auxquelles elles sont soumises.

Que se passerait-il si, demain, dans un moment de tension transatlantique, nous n'avions plus accès à nos données stockées dans *Google Cloud* ?

Si nos données de sécurité sociale confiées à Microsoft Azur n'étaient plus disponibles ?

Comment pourrait fonctionner la SNCF – dont le système d'information, d'une complexité analogue au système nerveux du corps humain, est placé sur le *Cloud* – ou le parc nucléaire français – dont les données de la maintenance des pièces d'usure ont été confiées au *Cloud* d'Amazon AWS ?

Alors que les réseaux de télécommunications sont déployés physiquement en Europe et sont en majorité opérés par des entreprises européennes, le *Cloud* est détenu et opéré pour environ 65 % par trois entreprises américaines :
Google, Microsoft et Amazon.

GILLES BABINET ET MILENA HARITO

Pour l'instant et malgré les récentes tensions commerciales avec les États-Unis, le scénario du pire d'un usage des services utilisant le *Cloud* comme moyen de coercition reste plus qu'hypothétique. Mais les scénarios de guerre ouverte – le président Trump se levant un matin et intimant aux grands acteurs numériques de couper les services numériques américains fournis à l'Union européenne – sont en fait moins inquiétant que des scénarios hybrides, beaucoup plus proches de nous et auxquels il faut se préparer : un conflit insidieux, fait de petits dysfonctionnements, astucieusement utilisés pour maintenir la pression – telle que l'interruption pendant plusieurs heures du système de communication par Satellite Starlink en Ukraine en octobre 2022 par exemple. Certains services de *Cloud* pourraient être réduits, voire même éteints, pendant de courtes périodes, en fonction du type d'acteur que l'on souhaite atteindre et du message que l'on souhaite véhiculer. Et cela serait possible avec ou sans la connivence du gouvernement américain.

Mettre l'infrastructure numérique au cœur de la défense européenne

Cette vulnérabilité massive du fonctionnement de nos entreprises et de nos institutions face aux géants du *Cloud* est la raison pour laquelle, dans son discours devant la Chambre et le Sénat italien le 18 mars 2025, traduit et commenté dans la revue, Mario Draghi avait plaidé pour inclure les dépenses concernant le *Cloud* et la cybersécurité dans les dépenses de la défense européenne.

Le marché européen du *Cloud* s'estime en 2024 autour de 110 milliards d'euros – soit environ deux fois et demie moins que le marché américain. Les trois opérateurs américains appelés « *hyperscalers* » – Amazon Web Services, Microsoft Azure and Google Cloud – en détiennent environ 65 % répartis dans le monde et en Europe. Ils fournissent généralement les solutions les plus complexes et à plus forte valeur ajoutée, qui sont aussi les plus difficiles à remplacer. Les principaux fournisseurs européens sont SAP, Deutsche Telekom et OVH avec environ 2 % de part de marché chacun. Ils sont suivis par Telecom Italia, Orange Business et une myriade de petits acteurs.

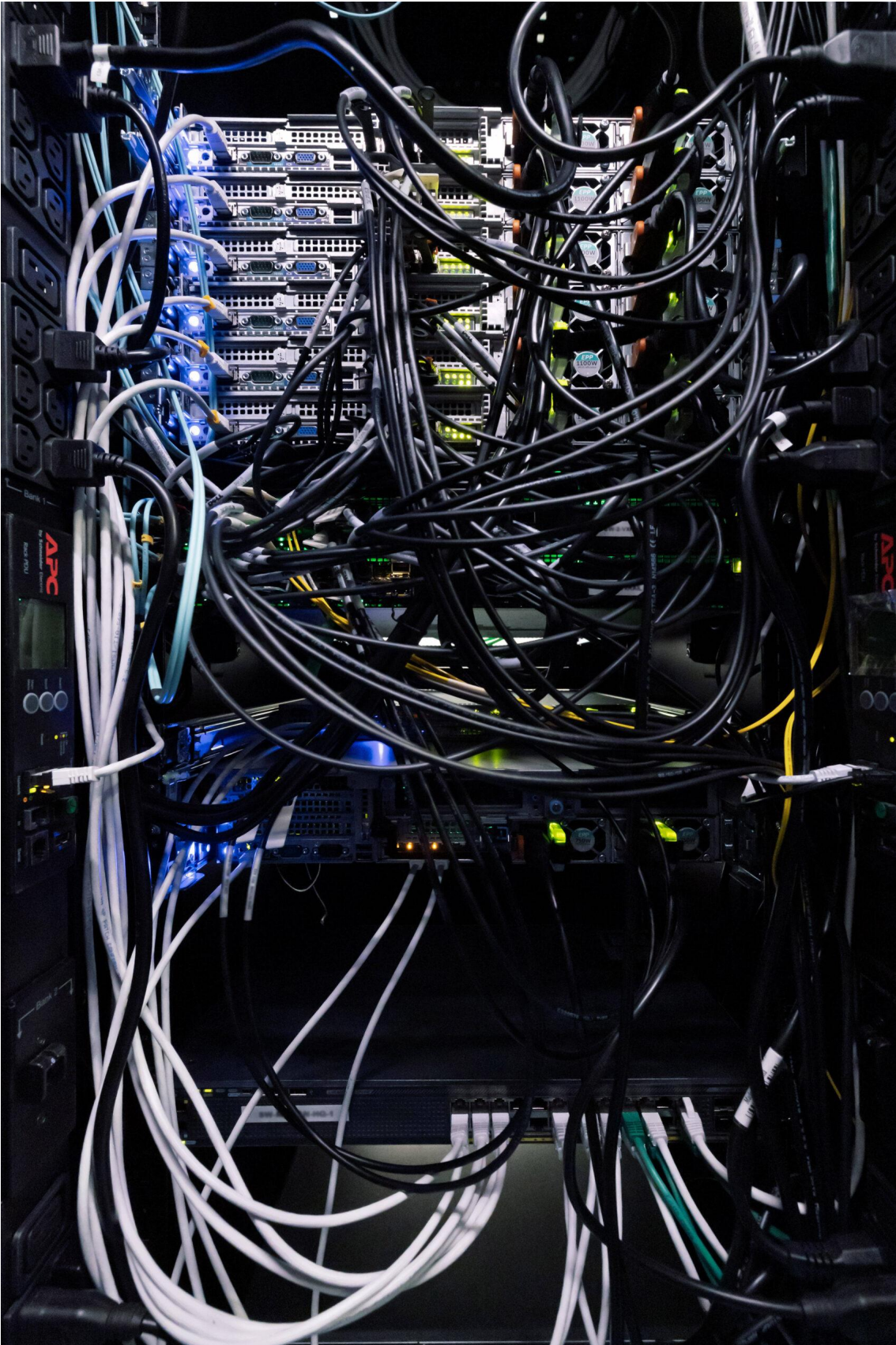
Il est crucial de comprendre ce qui est à l'origine de cette situation.

Elle est tout d'abord le résultat d'une culture américaine plus favorable à l'innovation, qu'il s'agisse du *venture capital* qui finance des startups développant des applications en *Cloud* ou des entreprises traditionnelles qui n'hésitent pas à adopter massivement de nouvelles pratiques beaucoup plus rapidement que les entreprises européennes ^③.

En second vient l'intégration du marché américain, qui permet à toute entreprise technologique de s'adresser sans nécessité d'adaptation et de traduction, et surtout sans adaptation réglementaire, à 350 millions de consommateurs potentiels. Cet avantage concurrentiel d'échelle est particulièrement important pour les services numériques, où les coûts sont en général fixes et donc où chaque client supplémentaire représente un coût quasi-nul ^④.



« Le marché européen du Cloud s'estime en 2024 autour de 110 milliards d'euros — soit environ deux fois et demie moins que le marché américain. »



« Les trois opérateurs américains appelés « hyperscalers » — Amazon Web Services, Microsoft Azure and Google Cloud — en détiennent environ 65%.»

Après le développement rapide des services propres d'Amazon, Google et Microsoft, et de l'infrastructure *Cloud* qui était d'abord nécessaire pour ces services, une intégration verticale a été mise en place par les acteurs nord-

américains. La rente obtenue par la position quasi-monopolistique dans les services numériques leur a permis d'étendre le *Cloud* et de le proposer à toutes les entreprises, et aux gouvernements, pour héberger leurs données et leur systèmes informatiques. C'est ainsi que s'est construite la position dominante des *hyperscalers*. Des pratiques de financement croisé monopolistiques, notamment mises en œuvre par Amazon, ont été pointées par un rapport du Congrès américain et par l'Autorité de Concurrence en France en 2023 – mais ces signalements sont restés sans conséquences.

D'énormes investissements disponibles ont permis aux géants *hyperscalers* de construire des avantages concurrentiels, puis graduellement de s'étendre à d'autres domaines annexes, afin de devenir encore plus puissants et indépendants : des câbles sous-marins aux *datacenters*, de l'énergie aux processeurs et aux modèles d'IA.

Mais pour l'heure, que ce soit à l'échelle nationale ou européenne, la riposte s'est exprimée essentiellement sur le plan réglementaire.

Les trois opérateurs américains appelés « *hyperscalers* » – Amazon Web Services, Microsoft Azure and Google Cloud – détiennent environ 65 % du marché du *Cloud* dans le monde et en Europe.

GILLES BABINET ET MILENA HARITO

En France, un ensemble de règlements récents vise à préserver la sécurité des systèmes d'information et des données qui recourent au *Cloud*.

C'est ainsi qu'ont été créés les standards de *Cloud de confiance* et, plus exigeant encore, de *Cloud souverain*. Ces derniers obligent les entreprises à héberger et à traiter les données dans l'Union européenne, par du personnel basé en Europe, évitant ainsi en théorie les risques liés aux lois extraterritoriales comme le *Cloud Act* américain.

Au niveau européen, différentes directives et règlements visent à ouvrir le marché, à éviter des concentrations et à promouvoir la concurrence, entre autres par des règles d'interopérabilité de données qui facilitent le changement de fournisseur – il s'agit des *Data Act*, *Data Governance Act*, et *Digital Markets Act*. Mais les discussions européennes sur la certification pour les services *Cloud* (EUCS) n'ont pas été concluantes depuis 2019.

En théorie toutes les données – y compris celles des systèmes informatiques complexes des entreprises américaines qui gèrent le *Cloud Souverain* – seraient donc hébergées et soumises aux lois européennes.

En pratique, en cas de tensions accrues, il pourrait en être autrement.

L'évolution et les mises à jour deviendraient compliquées, même au sein d'un *Cloud souverain*, tant les sous-éléments qui le composent ont été hégémonisés par les États-Unis – même les éléments décrétés *open source* peuvent ainsi être soumis à une licence régie par le droit américain ⁵.

Mais dans un contexte géopolitique de remise en question de la valeur des lois et de règles qui sous-tendaient jusqu'alors l'ordre international, on peut légitimement s'interroger : ces protections réglementaires, qui ont leur pertinence, fonctionneront-elles dans un monde impérial post-2025 ?

Une stratégie numérique pour l'Union face à l'Empire

Il ne s'agit plus de spéculer sur d'éventuels renoncements au droit de certains acteurs.

La menace est désormais avérée.

Le 27 janvier 2025 le président Trump a licencié les trois membres démocrates du *Privacy and Civil Liberties Oversight Board*, un organe clef du *Data Privacy Framework (DPF)*⁶ – texte imparfait qui permet toutefois à des milliers d'entreprises de transférer légalement les données des Européens aux États-Unis. Sa mission est de vérifier que le FBI ou la CIA respectent bien des principes de droit lorsqu'ils accèdent aux données personnelles des Européens (emails, messages...). La mainmise politique de l'administration Trump sur cet organisme laisse désormais entrevoir la possibilité que les États-Unis ne s'embarrassent plus de l'accord donné aux Européens.

Au-delà des réglementations de l'Union, des initiatives industrielles européennes visent à aller plus loin.

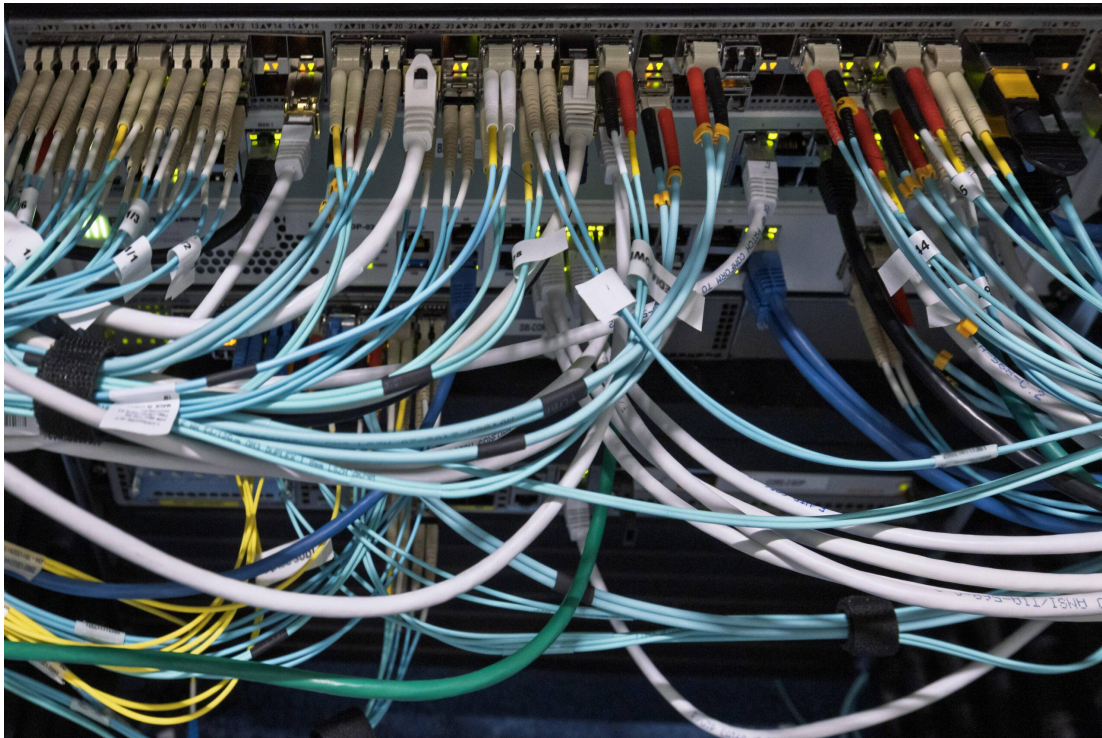
En France, il existe des consortiums de *Cloud Souverain* comme *Blue* (Orange, CapGemini) – qui sont toutefois bâtis sur des technologies Microsoft Azure. Il en est de même pour *S3ns* (Thales, Alphabet), avec la technologie Google. Le principe directeur est de faire en sorte que la gouvernance de ces infrastructures informatiques ne donne aucune prise en cas de requête d'une autorité américaine. Le code américain est licencié à une entité de droit français, dont la gouvernance est composée exclusivement de citoyens français.

La dépendance européenne aux entreprises de la Big Tech reste critique. Il est temps d'accélérer.

GILLES BABINET ET MILENA HARITO

L'initiative Gaia-X, lancée par la France et l'Allemagne, consiste quant à elle en une collaboration entre entreprises, gouvernements et universités pour mettre en place un ensemble de standards qu'adopteraient différents acteurs d'infrastructure européenne de données et de technologies souveraines. Elle permettrait de favoriser l'essor des acteurs européens existants et de réduire la dépendance vis-à-vis des acteurs non européens. La caractéristique centrale de Gaia-X consiste à standardiser les formats d'échanges pour favoriser le développement d'une constellation de *Clouds* inter-compatibles, et donc facilement interchangeables.

Pourtant, malgré ces initiatives, entre 2017 et 2022, la part de marché des fournisseurs européens a baissé de 27 % à 13 % – au bénéfice des trois *hyperscalers* mentionnés plus haut.



« Certains services de Cloud pourraient être réduits, voire même éteints, pendant de courtes périodes, en fonction du type d'acteur que l'on souhaite atteindre et du message que l'on souhaite véhiculer. Et cela serait possible avec ou sans la connivence du gouvernement américain. »

Les chiffres parlent d'eux-mêmes : la dépendance européenne aux entreprises de la Big Tech reste critique. Il est temps d'accélérer.

Nous estimons que plusieurs actions résolues sont nécessaires pour que l'Europe puisse tout à la fois restaurer son autonomie stratégique, sa compétitivité et sa capacité d'innovation, dans le champ du *Cloud* mais aussi de l'IA – qui reste pour l'instant très dépendante d'une infrastructure en *Cloud*.

Nous identifions trois priorités stratégiques :

1 — FAVORISER UNE PERSPECTIVE TECHNOLOGIQUE DE MOYEN TERME

Il ne suffira pas à l'Europe de se prémunir de la versatilité possible de ses partenaires technologiques : elle devrait aussi faire des paris technologiques de moyen terme.

En 2031, avec la croissance de la quantité de données due à l'IA et la rapidité des réseaux 5G, on estime que plus de la moitié des données pourraient être traitées plus efficacement en « périphérie », sans traverser des réseaux, en mode appelé « *Edge Computing* ». Contrairement au *Cloud*, pour lequel la domination des géants américains et chinois est déjà actée, le *Edge* reste un territoire à conquérir ⁽⁷⁾.

Alors que les objectifs numériques de l'Union prévoyaient 10 000 nœuds sécurisés et souverains en périphérie de réseaux en 2030⁽⁸⁾, uniquement trois étaient commercialement déployés en septembre 2024. Ces objectifs nécessitent une adaptation au nouveau contexte transatlantique, en mettant en œuvre une feuille de route de long terme qui identifie les composantes de la chaîne de valeur devant impérativement rester sous contrôle souverain.

S'il est irréaliste de produire des processeurs de taille de gravure inférieure à 4 nm en Europe, il n'en est pas moins inexcusable d'avoir délégué l'encryption de services critiques à des acteurs étrangers. Il convient donc de demander aux Organisations d'infrastructures vitales (OIV) de soumettre des feuilles de route comprenant un plan à la fois de remédiation en cas de panne d'un fournisseur logiciel d'un service essentiel, et d'autonomisation progressive sur une échelle de temps long.

2 — CRÉER LES CONDITIONS POUR ACCÉLÉRER LES INVESTISSEMENTS

Le rapport Draghi évoque un déficit cumulé d'investissements de l'Union par rapport aux États-Unis qui se chiffre en milliers de milliards d'euros – à titre d'exemple, dans le domaine du *Cloud*, Amazon AWS prévoit d'investir 100 milliards en infrastructure IA seulement en 2025.

Face à un tel constat, le tropisme européen s'exprime généralement par l'ambition, le plus souvent illusoire, de créer « le nouvel Airbus » – qu'il s'agisse des « microprocesseurs », « batteries », « chars de combat » ou « avions de chasse » – pour souvent constater, quelques années plus tard, un vaste gâchis d'argent public.

Il conviendrait donc selon nous de limiter autant que possible les politiques industrielles et de diriger l'investissement vers la synchronisation de la recherche à l'échelle européenne – rendant ici grâce aux *Advanced Research Projects Agency* (ARPA) américaines, à la *National Science Foundation* et à quelques autres organismes de financement de la recherche.

De même, on peut éviter l'investissement direct en capital, en privilégiant l'investissement en fond de *private equity* secondaire – une sorte de *venture capital* sous forme d'abondement maximisant l'effet de levier et minimisant le risque.

Le tropisme européen s'exprime généralement par l'ambition, le plus souvent illusoire, de créer « le nouvel Airbus » pour souvent constater, quelques années plus tard, un vaste gâchis d'argent public.

GILLES BABINET ET MILENA HARITO

L'accélération de l'Union de l'épargne et des investissements (UEI) devrait être une priorité, de sorte à mieux orienter l'épargne de l'Union vers des investissements productifs en général⁽⁹⁾. Comme le préconisaient les rapports Letta et Draghi en 2024, la nécessité d'avoir une Europe plus intégrée qui favorise les effets d'échelles est toujours d'actualité – et elle est sans doute plus importante encore dans le numérique que nulle part ailleurs.

Pour rationaliser les investissements dans le *Cloud* et le *Edge Cloud*, il est possible de favoriser des investissements communs et partagés entre acteurs européens, selon des modèles déjà connus pour les déploiements d'infrastructures numériques de fibre en France ou de réseaux mobiles en Europe.

Les plus grandes entreprises numériques de l'Union sont les opérateurs de télécommunications qui ont déployé en Europe une excellente infrastructure de fibres et de réseaux mobiles, basée sur une chaîne d'approvisionnement télécom également européenne. Ils ont la taille, l'organisation, les centres de traitements de données en périphérie de

réseaux et la 5G nécessaires pour les investissements massifs dans le *Edge Cloud* – bien sûr en coopération avec des partenaires spécialisés.

Toutefois, leur niveau d'investissement reste limité à cause du marché européen très fragmenté. On dénombre 34 groupes d'opérateurs mobiles en Europe là où, pour des marchés comparables, il y en a 3 ou 4 aux États-Unis ou en Chine. Il est nécessaire de bâtir sur la force de ces grands acteurs européens et de leur créer de nouvelles marges de manœuvre, en favorisant les fusions d'opérateurs pour leur donner les moyens d'investir, seuls ou en partenariats, dans le *Edge Cloud*.

Pour ce faire, un changement radical, bien identifié dans le rapport Draghi, est nécessaire : appliquer les règles de concurrence au seul niveau pertinent, qui est celui du marché européen dans sa totalité. Associer des engagements d'investissement forts, tout en permettant plus de fusions permettrait à des entreprises européennes de devenir des acteurs à l'échelle pertinente du *Cloud* – et de conduire vers une situation de marché européen plus équilibrée.

Enfin, il est nécessaire de souligner l'intérêt que pourrait avoir une logique de standards du système d'armement européen. À l'heure où il apparaît incontournable que l'IA contamine tous les domaines de défense, l'opportunité pour l'Europe de s'affranchir d'une logique atlantiste pour favoriser son propre modèle permettrait une forte mutualisation des investissements en R&D, dont les retombées civiles à moyen terme pourraient être considérables, en particulier sur les sujets d'IA, de *Cloud* et de technologies numériques au sens large.



« Dans le monde numérique, le pouvoir est désormais hyperconcentré. »



« Il va au-delà des gouvernements et il est en train d'échapper à la démocratie. »

3 — RENFORCER L'ACTION PUBLIQUE

À chaque étape, les politiques publiques jouent un rôle décisif. Or puisqu'il en est de même pour nos concurrents dans les autres parties du monde,

nous devons, comme les autres, faire un usage stratégique de notre puissance publique.

Pour sortir de la situation actuelle de verrouillage par les acteurs américains – ayant sans doute résulté d'un manque de vision de nombre d'acteurs – nous avons la possibilité de développer des standards et de l'interopérabilité pour ouvrir le marché ⁽¹⁰⁾.

Dans ce domaine, l'exemple de l'Inde est édifiant.

Le pays s'est attaché à recréer une dynamique de résilience numérique à travers la création des services numériques fondamentaux, de système de paiement ouvert, d'identité numérique biométrique et une importante initiative de *Cloud* destinée essentiellement à abriter les services publics numériques de l'Inde Fédérale, mais aussi des États indiens qui le souhaiteraient. Cette initiative, largement basée, sur de l'*open source* permet, en particulier en ce qui concerne le *Cloud*, de fédérer une large panoplie d'outils, sans reposer uniquement sur ceux des grands acteurs américains.

L'initiative prise par la direction du numérique en France (DINUM) en collaboration avec les autorités allemandes, consistant à développer une suite numérique *open source* pour le secteur public en tant qu'alternative à Microsoft Office, est emblématique de ce qu'il conviendrait de faire : utiliser la puissance publique pour susciter le développement de socles logiciels en source ouverte et favoriser la standardisation d'expériences utilisateurs alternatives aux services fournis par les grandes entreprises américaines.

À l'exception de l'accès aux terres rares et de la fabrication de microprocesseurs de pointe, les infrastructures informationnelles ne contiennent aucune technologie réellement inaccessible aux Européens.

GILLES BABINET ET MILENA HARITO

Il n'est pas réaliste d'espérer rattraper le niveau technologique des *hyperscalers*.

Mais en mutualisant les efforts et en démultipliant ce type d'approche, il est possible de parvenir sur une perspective de temps long à un niveau de qualité et d'innovation probablement équivalent – voire supérieur – à ce que font ces acteurs d'outre-Atlantique.

Bifurquer : il est encore possible de choisir la voie européenne

L'Europe a de nombreuses « cartes en main » pour gagner en autonomie dans son infrastructure numérique.

Il est faux d'affirmer que l'Europe serait condamnée à sortir de l'histoire, que son déclin technologique serait désormais irrémédiable et qu'il nous faudrait donc accepter de nous plier aux termes d'une « Pax Americana » au sein de laquelle l'usage des technologies informationnelles serait fatalement d'origine d'outre-Atlantique.

L'exemple des infrastructures informationnelles le montre bien : à l'exception de l'accès aux terres rares et de la fabrication de microprocesseurs de pointe, elles ne contiennent aucune technologie réellement inaccessible aux Européens. Il s'agit donc de créer les conditions qui permettraient aux consommateurs de bénéficier des avantages spécifiques à ces technologies – à commencer par leurs rendements croissants.

L'intégration des réglementations nationales et des marchés de capitaux à une échelle européenne doit être une priorité – qui a d'ailleurs été justement identifiée par le rapport Draghi. Reste à créer une culture et des compétences communes au niveau européen, un objectif probablement plus ambitieux, mais tout aussi nécessaire.

Enfin, il faut prendre garde pour éviter de tomber dans un piège trop commun : la volonté de rattraper plutôt que de créer sa propre voie.

On ne compte plus les plans de mise à niveau : leurs conséquences sont presque toujours décevantes. Il ne s'agit donc pas ici de faire ce que d'autres ont déjà fait, mais bien de préempter les besoins à venir. Il s'agit de faire des choix correspondant aux besoins des Européens, qui divergent de plus en plus de ceux des Américains, et finalement de permettre à des technologies adaptées à l'environnement européen d'advenir.

Dans le monde numérique, le pouvoir est désormais hyperconcentré.

Il va au-delà des gouvernements et il est en train d'échapper à la démocratie.

Pour protéger nos frontières, notre économie, notre mode de vie et nos valeurs, il faut agir vite.

SOURCES

- ① Florian Reynaud, Damien Leloup et Olivier Clairouin, « [Panne informatique mondiale : des aéroports, des hôpitaux et de nombreuses autres entreprises paralysés dans le monde entier](#) », Le Monde, live du 19 juillet 2024. ¹
- ② [The Draghi report on EU competitiveness](#), Commission européenne, septembre 2024. ¹
- ③ Daniela Mustatea, « [North America Vs Europe : Who Will Win the Race to Cloud Adoption ?](#) », BigStep, 19 janvier 2015. ¹
- ④ On résume généralement cette caractéristique par la théorie des rendements croissants (winner takes all) telle qu'elle a été énoncée par Brian Arthur dès 1996. Voir W. Brian Arthur, « [Increasing Returns and the New World of Business](#) », Harvard Business Review, Juillet-août 1996. ¹
- ⑤ [Understanding US export controls with open source projects](#), Linux Foundation, juillet 2020. ¹
- ⑥ Stéphanie Bascou, « [Transfert de données transatlantique : l'Europe annonce un nouveau Privacy Shield](#) », O1net, 10 juillet 2023. ¹
- ⑦ [Infrastructures numériques : un plan décisif](#), Institut Montaigne, mars 2025. ¹
- ⑧ [Europe's Digital Decade : digital targets for 2030](#), European Commission, septembre 2023. ¹
- ⑨ « [La Commission dévoile la stratégie de l'union de l'épargne et des investissements visant à améliorer les possibilités financières](#) », Communiqué de presse, Commission européenne, 19 mars 2025. ¹
- ⑩ « [Data Act enters into force : what it means for you](#) », Directorate-General for Communication, European Commission, 11 janvier 2024. ¹