Tribune

Cybersécurité : la France peut-elle encore prétendre à la souveraineté numérique ?

Par Philippe Folliot, sénateur du Tarn

Membre de la Commission des affaires étrangères, de la défense et des forces armées Membre de la Délégation sénatoriale aux outre-mer Président de l'Alliance Centriste

« 70 % de nos données sont contrôlées par des géants américains. Jusqu'à quand ? »

Le 4 novembre dernier, en commission des Affaires étrangères, de la Défense et des Forces armées au Sénat, j'ai interpellé MM. Nicolas Roche (**SGDSN** – Secrétariat Général de la Défense et de la Sécurité Nationale), Vincent Strubel (**ANSSI** – Agence Nationale de la Sécurité des Systèmes d'Information) et Marc-Antoine Brillant (**Viginum** – Service de vigilance et de protection contre les ingérences numériques étrangères) sur un sujet qui devrait nous alarmer tous : **70 % du marché français de l'hébergement des données** est aujourd'hui contrôlé par trois entreprises américaines – **Amazon, Google et Microsoft**, toutes soumises à l'**extraterritorialité du droit américain**.

Malgré l'existence d'une doctrine française de souveraineté numérique, incarnée par la qualification **SecNumCloud** (qualification de sécurité pour le cloud souverain) de l'ANSSI, et malgré des exemples inspirants comme les choix de la Gendarmerie nationale, certains ministères, à l'image de celui de la Santé avec le **F-Data Club** (nom de l'initiative de gestion de données de santé), continuent d'externaliser des données sensibles vers des prestataires étrangers. Mais la menace la plus sournoise vient peut-être des offres hybrides, comme **BLEU** (coentreprise entre Microsoft, Orange et Capgemini) ou **S3NS** (coentreprise entre Google et Thales).

Ma question était simple, et je la repose aujourd'hui : « Est-ce que l'ANSSI s'apprête à valider ces offres hybrides, ce qui, à certains égards, remettrait en cause la souveraineté et surtout les perspectives de solutions alternatives totalement nationales ou européennes ? » Cette question n'est pas technique. Elle est profondément politique. Elle interroge notre capacité collective à défendre nos intérêts face à une puissance étrangère qui, elle, ne fait aucun compromis et agit avec une détermination sans faille.

L’arsenal juridique américain : une prédation organisée et méthodique

L'affaire **Alstom**, sous la pression du **FCPA** (*Foreign Corrupt Practices Act*), est devenue l'emblème d'une stratégie d'extraterritorialité analysée avec acuité par Frédéric Pierucci dans *Le Piège Américain*. Onze ans plus tard, le constat est toujours aussi accablant : les États-Unis ont durci et élargi leur arsenal juridique. Le **Cloud Act** (*Clarifying Lawful Overseas Use of Data Act*), le **FISA** (*Foreign Intelligence Surveillance Act*), le **Patriot Act** (loi antiterroriste élargissant les pouvoirs de surveillance) ou encore la réglementation **ITAR** (*International Traffic in Arms Regulations*) leur permettent de contraindre les entreprises étrangères. Il suffit d'un simple courriel transitant par un serveur américain, ou d'une opération financière libellée en dollars, pour placer une entreprise européenne sous leur coupe, au nom de la sécurité nationale ou de la lutte contre la corruption.

Ce qui est encore plus préoccupant, c’est que ces textes donnent aux autorités américaines un accès quasi systématique à nos données, et ce sans que nous en ayons toujours conscience. Le FISA, par exemple, autorise la **National Security Agency (NSA)** à consulter les informations des entreprises étrangères dès lors qu’elles transitent par les États-Unis ou qu’elles sont hébergées par une société de droit américain, comme Microsoft, Google ou Amazon. Le Cloud Act va encore plus loin : il oblige ces mêmes entreprises à transmettre aux autorités américaines toutes les données qu’elles détiennent, même si elles sont stockées en Europe. En 2014, Microsoft a dû remettre des emails hébergés en Irlande aux États-Unis, malgré l’opposition de l’Union européenne. La Cour suprême américaine a alors tranché sans ambiguïté : peu importe où sont les données, si l’entreprise est américaine, Washington y a accès.

Malgré les exigences de la jurisprudence Schrems II de la Cour de justice de l’UE, le Data Privacy Framework (DPF) signé en 2023 s’apparente à une illusion de protection, car la réalité est que Washington n'a pas réformé ses lois d'accès. Le Cloud Act et le FISA restent intacts.

Ces instruments ne visent pas uniquement la sécurité nationale. Ils servent aussi à protéger les intérêts économiques américains, un concept que Washington interprète de manière très extensive. L’exemple du conflit **Airbus-Boeing** est, à ce titre, édifiant. Non seulement les États-Unis n’ont pas hésité à pratiquer de l’espionnage ciblé – comme les écoutes de la chancelière allemande **Angela Merkel** révélées en 2013 – mais ils ont également pris des mesures de rétorsion commerciales brutales (taxes sur le vin, le Roquefort) pour affaiblir Airbus sur le marché mondial. L’**intelligence économique** est une arme de guerre commerciale, et les GAFAM en sont, par la contrainte légale, les relais les plus efficaces, transformant chaque donnée européenne hébergée chez eux en potentiel avantage concurrentiel pour les États-Unis.

Pourtant, la France a tenté de réagir : loi Sapin II, création du **SISSE** (Service de l’Information Stratégique et de la Sécurité Économiques), et la tenue de **commissions**

d'enquête sur les ingérences étrangères à l'Assemblée nationale et au Sénat. Mais ces mécanismes restent défensifs, fragmentés et insuffisants. Pendant ce temps, les États-Unis étendent leur emprise, dans la droite ligne du slogan « America First » : être dominant ou être dominé. La question est simple : de quel côté voulons-nous être ?

Les offres hybrides : une souveraineté numérique en trompe-l'œil

La doctrine SecNumCloud, portée par l'ANSSI, prouve que des alternatives 100 % françaises ou européennes existent bel et bien. La Gendarmerie nationale l'a compris en choisissant des solutions souveraines pour ses propres besoins. Pourtant, des ministères comme celui de la Santé, via le F-Data Club, ou des entreprises stratégiques comme EDF, avec son choix récent de **BLEU**, continuent de s'appuyer sur des infrastructures contrôlées par des acteurs américains.

Pourquoi est-ce un problème majeur ? Parce qu'une offre hybride comme BLEU ou S3NS, même labellisée SecNumCloud, conserve une dépendance structurelle aux États-Unis. Microsoft et Google restent en effet soumis au Cloud Act et au FISA. Une seule brique américaine dans une infrastructure suffit à soumettre l'ensemble au droit étranger, et donc à exposer nos données les plus sensibles.

Prenons l'exemple de BLEU, qui propose les services **Microsoft 365** et **Azure** dans un « cloud français ». En réalité, Microsoft garde la main sur les couches logicielles critiques, comme les mises à jour ou la sécurité. Résultat : nos données restent accessibles à Washington, malgré les serveurs situés en France et les promesses de souveraineté.

Autre exemple, S3NS, qui associe Google et Thales. Pourtant, Google reste une entreprise américaine, soumise aux mêmes obligations légales que Microsoft.

Ces partenariats ne font pas qu'étouffer les vraies alternatives européennes (**OVHcloud, Mistral AI, Qarnot**) ; ils financent notre propre dépendance. Nous payons pour des solutions présentées comme souveraines, alors qu'elles conservent une porte dérobée vers les États-Unis. C'est une illusion dangereuse, et nous ne pouvons plus nous permettre de fermer les yeux.

Les données : la ressource stratégique du XXIe siècle

Après le charbon, le pétrole, l'électricité et les microprocesseurs, les **données sont devenues la ressource clé du XXIe siècle**. Elles alimentent nos intelligences artificielles, optimisent nos industries, protègent nos citoyens et déterminent la compétitivité de nos entreprises. Pourtant, nous continuons de les confier massivement à des acteurs étrangers, comme si nous n'avions pas conscience des risques encourus.

Les conséquences de cette dépendance sont lourdes et multiples. D'abord, il y a la **perte de souveraineté** : nos secrets industriels, nos algorithmes, nos dossiers médicaux peuvent être réquisitionnés par une puissance étrangère sans que nous puissions rien y faire. Ensuite, il y a un **risque économique majeur** : comme pour Alstom ou Airbus, nos champions industriels pourraient être affaiblis par des fuites de données ou des pressions extérieures. Enfin, il y a une **menace sur notre capacité d'innovation** : les données sont le carburant de l'intelligence artificielle, et les laisser entre les mains des GAFAM, c'est renoncer à notre compétitivité sur le long terme.

Une commission d'enquête pour sortir de l'illusion et agir concrètement

Face à cette prédation organisée, une **commission d'enquête parlementaire** s'impose plus que jamais. Son rôle serait d'abord d'auditer les risques auxquels nous sommes confrontés : quelles données sensibles sont déjà exposées ? Quels secteurs, comme la santé, l'énergie ou la défense, sont les plus vulnérables à ces ingérences ? Ensuite, il faudrait mesurer les pertes que nous avons déjà subies, que ce soit en termes d'emplois, de brevets ou de parts de marché, comme ce fut le cas pour Alstom ou Airbus. Enfin, il serait crucial d'identifier les vulnérabilités de notre appareil d'État et de nos entreprises : quels ministères ou quelles sociétés utilisent encore des clouds américains ou hybrides, mettant ainsi en péril notre sécurité nationale ?

Mais une commission d'enquête ne doit pas se limiter à un simple constat. Elle doit aussi proposer une réponse politique et stratégique coordonnée. Cela passe d'abord par l'**interdiction des offres hybrides** pour les données sensibles, afin de garantir que nos infrastructures critiques ne soient plus exposées aux lois américaines. Ensuite, il est impératif de **réserver les marchés publics aux solutions 100 % européennes**, comme OVHcloud ou Mistral AI, pour soutenir nos champions technologiques. Par ailleurs, la création d'un **fonds souverain** permettrait de racheter et de protéger nos pépites technologiques, comme Exaion, aujourd'hui menacée par une vente à un acteur américain. Enfin, il faut **renforcer le label SecNumCloud** en excluant toute participation américaine, pour s'assurer que nos données restent vraiment souveraines.

Cette commission doit impulser une réaction politique forte et coordonnée, comme le propose le projet que je soutiens. Son objectif est clair : **comprendre pour protéger, et protéger pour garantir notre indépendance économique, technologique et démocratique**. Nous n'avons plus le choix : soit nous agissons maintenant, soit nous acceptons de devenir un protectorat numérique.

Un choix de civilisation pour la France et l'Europe

La **souveraineté numérique** n'est pas une option parmi d'autres. C'est une nécessité absolue. Nous avons aujourd'hui un choix à faire : soit nous continuons comme hier, en acceptant que nos données soient espionnées, que nos entreprises soient affaiblies, et que notre souveraineté soit bradée ; soit nous agissons sans délai pour bannir les clouds américains pour les données critiques, financer nos champions technologiques, et imposer une doctrine de souveraineté numérique sans compromis.

En commission, j'ai rappelé que la Gendarmerie nationale a montré la voie en choisissant des solutions souveraines. Il est temps que l'État suive cet exemple. **Les données sont le nouveau pétrole.** La France ne peut pas se permettre de les brader, ni de les laisser entre les mains de ceux qui en feront une arme contre nous

Philippe FOLLIOT