Souveraineté numérique : quand l'État bâtit d'une main et détruit de l'autre.
Souveraineté numérique : quand l'État bâtit d'une main et détruit de l'autre.

Bernard Sfez - 2026-02-15 12:15

Si un pays comme la France dispose aujourd'hui d'un arsenal complet pour reconquérir sa souveraineté numérique, entre les lois votées et les bons de commande signés, un fossé persistant interroge la crédibilité de toute la démarche. Analysons comment l'État et l'Éducation nationale gèrent ou subissent leur relation aux géants technologiques américains. Du côté gouvernemental, des avancées tangibles cohabitent avec des renoncements difficiles à justifier. Du côté scolaire, la situation est plus préoccupante encore : c'est dès le plus jeune âge que se construit, année après année, une accoutumance aux écosystèmes fermés avec l'argent du contribuable.

Entre initiatives prometteuses et contradictions flagrantes, nous analysons ce qui fonctionne, ce qui bloque, et pourquoi la cohérence reste le maillon faible d'une stratégie par ailleurs ambitieuse. Car les alternatives souveraines existent et font leurs preuves. Reste à trouver la volonté politique de les généraliser, de la salle de classe au datacenter.

Le gouvernement face aux GAFAM : entre volonté politique et inertie structurelle

Des signaux politiques réels

Il serait injuste de dire que rien ne bouge. Depuis 2017, la France porte au niveau européen l'idée d'une autonomie stratégique numérique, et les dernières années ont vu une accélération notable. Toutefois, les spécialistes de l'information, du renseignement, de la cybersécurité et les consultants (indépendants ou aux services de l'État) s'accordent pour souligner la lenteur et parfois les contradictions des politiques publiques en la matière — manque de suivi, incohérences entre les discours et les actes, absence de constance dans l'exécution.

En juin 2025, lors d'un Conseil des ministres dédié, le gouvernement a officiellement reconnu la gravité de la situation : 83 % des dépenses numériques européennes sont dirigées vers des acteurs extra-européens, représentant un flux estimé à 264 milliards d'euros par an selon l'étude Asterès pour le Cigref (avril 2025). Un chiffre qui traduit non pas une simple préférence de marché, mais une dépendance structurelle — que le Cigref compare désormais à la facture énergétique de l'UE (360 milliards d'euros en 2024).

La réponse politique s'est articulée autour de plusieurs axes concrets :

La création de l'Observatoire de la souveraineté numérique

Officiellement lancé le 26 janvier 2026 sous la direction du Haut-commissariat à la Stratégie et au Plan. Sa mission : cartographier les dépendances, produire des indicateurs exploitables et orienter la commande publique. Ses premières analyses sont attendues au printemps 2026.

La doctrine « Cloud au centre »

Lancée en 2021 et actualisée par circulaire en mai 2023. En résumé, l'État impose que tout nouveau projet numérique des administrations utilise le cloud comme mode d'hébergement par défaut.

La qualification SecNumCloud

Pour les données sensibles — sécurité nationale, santé publique, données personnelles critiques — l'hébergeur retenu doit impérativement être qualifié SecNumCloud, un visa de sécurité délivré par l'ANSSI (Agence nationale de la sécurité des systèmes d'information). Concrètement, cette qualification garantit non seulement un haut niveau de cybersécurité (basé sur ISO 27001), mais surtout une immunité aux lois extraterritoriales — c'est-à-dire que le fournisseur ne peut pas être contraint par un gouvernement étranger (typiquement les États-Unis via le Cloud Act ou le FISA) à accéder à vos données. À ce jour, l'ANSSI recense une dizaine de prestataires déjà qualifiés SecNumCloud et 14 autres en cours de qualification — un écosystème en croissance, mais encore très modeste face aux hyperscalers.

Le plan France 2030

Un plan qui a mobilisé des milliards d'euros pour soutenir les technologies stratégiques — cloud, IA, cybersécurité, quantique. En avril 2025, un appel à projets spécifique au « Renforcement de l'offre de services cloud », doté de plusieurs dizaines de millions d'euros et opéré par Bpifrance, a été lancé pour soutenir l'émergence d'offres cloud IaaS/PaaS françaises compétitives, notamment pour l'IA.

Ces initiatives sont réelles et constituent sans doute déjà une reconnaissance concrète du problème — voire des problèmes. Elles méritent d'être saluées. Mais elles se heurtent à un problème structurel que nous allons examiner.

Le paradoxe de la commande publique

Le détail des chiffres de la commande publique cloud révèle un paradoxe saisissant. Selon la DINUM (mars 2025), cette commande a crû de 50 % entre 2023 et 2025 pour atteindre 52 millions d'euros, dont 75 % orientés vers des acteurs européens. C'est encourageant. Mais un tiers seulement de ces dépenses concerne des solutions labellisées SecNumCloud — le reste bénéficie largement aux hyperscalers américains.

Autrement dit, l'État demande à ses administrations de choisir souverain... tout en finançant massivement les alternatives non souveraines. Le marché français des solutions qualifiées SecNumCloud ne pèse que 18 millions d'euros — une goutte d'eau dans un océan dominé par AWS, Microsoft Azure et Google Cloud, qui contrôlent entre 70 et 80 % du marché cloud en France. Et comme nous l'avons détaillé dans notre article précédent, ces entreprises qui sont soumises au droit américain, Cloud Act, FISA et Patriot Act, peuvent être contraintes de livrer les données de leurs utilisateurs, ou de couper l'accès à leurs services, sur simple injonction de la

justice américaine.

Ce paradoxe est donc criant : l'État exhorte ses administrations à la souveraineté tout en injectant des millions dans les coffres de ceux qui la compromettent. La commande publique française finance massivement les entreprises prédatrices américaines et l'État ne se contente pas de subir une dépendance : il l'entretient activement, infligeant un véritable coup de poignard dans le dos des entreprises et acteurs européens qui, eux, assument sans broncher les coûts supplémentaires liés à la transformation pour une indépendance numérique.

La part des acteurs européens dans le marché du cloud a d'ailleurs connu une baisse constante depuis 2017, tombant à environ 13 % selon la Direction Générale des Entreprises (chiffre repris par EY dans son analyse de l'écosystème cloud européen). Les GAFAM eux, ont investi plus de 800 milliards de dollars dans leurs infrastructures depuis 2010. Le tout en répétant inlassablement le même boniment : « Nos serveurs sont en Europe, vous n'avez rien à craindre ». Et nous justifierons l'utilisation du terme « boniment » dans le paragraphe suivant.

Une asymétrie structurelle est aujourd'hui clairement identifiable : les moyens mobilisés en France et en Europe ne sont pas du même ordre de grandeur que ceux des acteurs outre-Atlantique.

Le Cloud Act et le FISA : les éléphants dans la salle des serveurs

Au-delà des parts de marché, c'est la dimension juridique qui devrait alarmer tout décideur. Le Cloud Act (2018) et la section 702 du FISA ainsi que sa réforme de 2024 permettent aux autorités américaines d'exiger l'accès aux données stockées par des entreprises soumises à leur juridiction — y compris lorsque ces données se trouvent physiquement en Europe.

Ce n'est pas de la théorie. En juin 2025, lors d'une audition au Sénat français le 11 Juin 2025, répondant à une question du rapporteur M. Dany Wattebled, Pierre Lagarde, directeur technique du secteur public de Microsoft France, a reconnu ne pas pouvoir garantir que les données des citoyens français hébergées dans des centres de données Microsoft situés en France ne seraient jamais transmises au gouvernement américain sans l'accord de Paris. Cette déclaration devrait figurer en lettres capitales dans chaque appel d'offres public impliquant un hébergeur américain.

Un avis juridique commandé par le ministère allemand de l'Intérieur a confirmé ce risque : la localisation des données dans l'UE ne suffit pas à garantir leur souveraineté dès lors que le fournisseur est soumis au droit américain. Ce n'est pas la géographie qui fait foi, mais la juridiction. Concrètement, que vos données soient stockées à Paris, Francfort ou Amsterdam, si elles le sont chez un fournisseur américain, elles sont juridiquement accessibles aux agences de renseignement américaines.

Le RGPD exige que les individus soient informés de l'accès à leurs données et impose la transparence, tandis que le FISA et le Cloud Act peuvent imposer cet accès sous le sceau du secret (gag orders), rendant même le signalement de l'accès impossible au regard de la directive NIS2. On se retrouve donc dans une situation kafkaïenne : un accès aux données imposé par la loi américaine peut constituer une violation du droit européen, mais la loi américaine interdit de le signaler. Contradiction frontale, et pourtant l'État continue de signer des contrats avec ces mêmes fournisseurs.
De nombreuses sources et analyses confirment ces faits :

- Section 504 du FRRA / élargissement ECSP dans le RISAA : analyse claire du cabinet ZwillGen.
- Texte final du RISAA (H.R.7888)

Le problème ne se limite pas au cloud. Le renouvellement du FISA en 2024 et les projets de réforme (section 504 du FRRA) pourraient étendre l'obligation de communication des données aux équipementiers, au-delà des seuls opérateurs de cloud. L'enjeu ne cesse de s'élargir.

Étendre l'obligation aux équipementiers, au-delà des seuls opérateurs de cloud

La nouvelle définition du RISAA couvre désormais tout « service provider who has access to equipment that is being or may be used to transmit or store wire or electronic communications ».

Concrètement, au-delà des opérateurs cloud, cela peut inclure :

- Les data centers / hébergeurs d'infrastructure (colocation, housing) — même s'ils ne gèrent pas le contenu.
- Les fournisseurs de services managés (MSP/MSSP) — infogérance, supervision réseau.
- Les équipementiers réseau et télécom — fabricants/opérateurs de routeurs, switches, firewalls (Cisco, Juniper, etc.).
- Les fournisseurs de CDN (content delivery networks).
- Les prestataires de maintenance IT ayant un accès physique ou logique aux équipements.
- Les fournisseurs d'accès Wi-Fi (explicitement mentionné dans l'analyse IRSEM, bien que les logements et restaurants soient exclus).
- Les éditeurs de logiciels SaaS hébergeant des communications (messagerie, visioconférence, outils collaboratifs).

L'IRSEM note que la définition est jugée « trop large » par l'industrie elle-même et que « simplement fournir une connexion Wi-Fi » pourrait théoriquement tomber dans le champ d'application.

Pour les organisations qui souhaitent aligner leurs pratiques avec ces réalités juridiques, un accompagnement en cybersécurité et en gestion d'infrastructure souveraine peut faire la différence entre conformité théorique et protection effective.

Des initiatives européennes à accélérer

La France n'est pas seule dans cette démarche. Au niveau européen, un arsenal réglementaire sans précédent est désormais opérationnel. Le DSA (Digital Services Act), pleinement applicable depuis février 2024, encadre les plateformes en ligne pour lutter contre les contenus illicites et imposer de la transparence — avec une première amende de 120 M€ infligée à X en décembre 2025, et une enquête ouverte en janvier 2026 sur son chatbot Grok.

Le DMA (Digital Markets Act) cible les « contrôleurs d'accès » (''gatekeepers'') et leurs pratiques anticoncurrentielles, avec de nouvelles procédures engagées contre Google en janvier 2026 pour ouvrir Android aux IA concurrentes. La directive NIS 2 renforce les obligations de cybersécurité des infrastructures critiques. Et le Data Act, applicable depuis septembre 2025, encadre l'accès aux données générées par les objets connectés, impose l'interopérabilité des services cloud et s'attaque au verrouillage technologique (vendor lock-in) pratiqué par les hyperscalers.

Mais ces instruments réglementaires ont leurs limites. Les amendes infligées aux GAFAM, même lorsqu'elles se chiffrent en milliards d'euros, restent absorbées comme un coût d'activité : les

sanctions DMA d'avril 2025 contre Apple (500 M€) et Meta (200 M€) ne représenteraient à peine que 0,5 % de leurs bénéfices annuels. Et les tensions géopolitiques s'intensifient : Washington perçoit ouvertement le DSA et le DMA comme des barrières non tarifaires, l'administration Trump ayant lancé en février 2025 un examen officiel de ces règlements qu'elle juge « discriminatoires » envers les champions américains.

Face à ces pressions, l'initiative franco-allemande a marqué un tournant. Annoncée en juin 2025, formalisée au sommet de Toulon en août, elle a abouti le 18 novembre 2025 au Sommet de Berlin sur la souveraineté numérique européenne, co-présidé par le Président de la République Française M. Macron et le Chancelier Allemand M. Merz devant 900 décideurs. Résultat : plus de _*12 milliards d'euros de promesses d'investissement privé*_, le lancement d'une « Digital Sovereignty Task Force » franco-allemande chargée de définir des indicateurs de souveraineté pour le cloud, l'IA et la cybersécurité (résultats attendus au Conseil des ministres franco-allemand 2026), le soutien à un consortium européen de communs numériques, et — fait notable — la reconnaissance explicite de l'open source comme pilier stratégique, le chancelier Merz révélant que la suite OpenDesk est déjà utilisée à la Chancellerie fédérale.

Des signaux encourageants. Mais l'enjeu reste autant culturel que politique :
Tant que les décideurs publics et privés européens considéreront les GAFAM comme le choix « par défaut », aucun cadre réglementaire ne suffira.

<?xml version="1.0" encoding="UTF-8"?>  FEU VERT ! 2013 Loi ESR — Logiciels libres en priorité Art. L.123-4-1 — Éducation FEU VERT ! PANNE D'ESSENCE !  2015 Partenariat Microsoft Éducation — 13 M€ Mécénat - Licences gratuites PANNE D'ESSENCE ! LIMITE DE VITESSE ! 50 2021 Doctrine Cloud au Centre — DINUM Office jugé non conforme LIMITE DE VITESSE ! STOP ! STOP 2022 Interdiction Office 365 et Google — Écoles Question Latombe — JO STOP ! ACCIDENT ! MARS 2025 Accord-cadre Microsoft 152 M€ 4 ans — sans concurrence ACCIDENT ! CREVÉ ! MARS 2025 Polytechnique → Microsoft 365 Données défense exposées CREVÉ ! ESSENCE !  JUIN 2025 Conseil des ministres souveraineté numérique 264 Mrd€/an de dépendance ESSENCE ! INCREVABLE ! ★ 2024 GendBuntu — 97% 103 164 postes Linux BOTTE SECRÈTE INCREVABLE ! ROULEZ ! JAN 2026 Observatoire de la souveraineté numérique Clément Beaune ROULEZ ! © 2026 OpenSourceSolutions.pro — Inspiré du jeu des 1000 Bornes®

Un terrain miné par les contradictions

Si la dépendance numérique de l'État est préoccupante, celle de l'Éducation nationale est proprement vertigineuse et bien plus lourde de conséquences à long terme. Car l'école ne se contente pas d'utiliser des outils : elle forme des habitudes, des réflexes, des dépendances cognitives.

Le sujet n'est pas nouveau. Dès 2015, la signature d'un partenariat entre le ministère de l'Éducation nationale et Microsoft avait provoqué une levée de boucliers des associations du logiciel libre et des syndicats enseignants. L'ADULLACT (Association des Développeurs et Utilisateurs de Logiciels Libres pour les Administrations et les Collectivités Territoriales) alertait déjà que chaque élève et chaque enseignant contraint de disposer d'un compte Microsoft verrait se créer un « lien de dépendance durable ».

En 2022, le ministère a officiellement demandé l'arrêt du déploiement d'Office 365 et de Google Workspace dans les établissements scolaires, au motif que ces solutions ne sont conformes ni au RGPD ni à la doctrine « Cloud au centre ». La CNIL a recommandé le recours à des suites collaboratives hébergées en UE par des prestataires soumis exclusivement au droit européen Trois ans plus tard, la réalité sur le terrain est tout autre.

Mars 2025 : le renouvellement qui a tout remis en question

Le 14 mars 2025, un avis publié au Bulletin officiel a révélé l'attribution d'un accord-cadre de quatre ans portant sur des licences Microsoft, pour un montant maximal de 152 millions d'euros. En pleine période de tensions transatlantiques, au moment même où le gouvernement multipliait les discours sur la souveraineté numérique, l'Éducation nationale renouvelait son « open bar » Microsoft.

Le CNLL (Conseil National du Logiciel Libre) a dénoncé un marché « attribué sans mise en concurrence réelle », aggravant une dépendance technologique qualifiée d'« excessive et dangereuse ». Le député Philippe Latombe a demandé à la ministre de l'Éducation de dénoncer le contrat, rappelant que la circulaire de la DINUM interdit le déploiement d'Office 365 dans les administrations françaises.

Parallèlement, la direction de l'École polytechnique — fleuron sous tutelle du ministère des Armées dont les recherches irriguent nos secteurs les plus critiques (militaire, cyber, quantique) — a acté, sans concertation, la migration de ses données vers Microsoft 365. Le CNLL dénonce une « mise en danger délibérée des données sensibles de l'établissement », y compris celles relevant de la sécurité nationale. Rester factuel devient ici un exercice de haute voltige : pour n'importe quel expert du secteur, le constat est sans appel, on marche sur la tête !

L'ironie est amère : le même État qui crée un Observatoire de la souveraineté numérique finance par ailleurs, sur fonds publics, l'approfondissement de sa dépendance à Microsoft.

La gratuité comme cheval de Troie

Le mécanisme est bien rodé. Microsoft et Google proposent des offres « gratuites » aux établissements scolaires — Office 365 pour l'un, Google Workspace for Education pour l'autre. Cette gratuité n'est évidemment pas désintéressée. Comme le soulignait le député Latombe, elle

s'apparente à une forme de dumping et de concurrence déloyale : aucun appel d'offres n'est lancé pour des offres gratuites, ce qui élimine mécaniquement les concurrents européens.

L'effet est systémique et parfaitement calculé. Un élève qui utilise Word et Excel pendant treize ans de scolarité n'envisagera pas spontanément LibreOffice en entreprise. Un enseignant formé sur Google Classroom ne migrera pas volontairement vers Moodle. La gratuité initiale se transforme en rente de dépendance : les licences personnelles, les abonnements cloud, les certifications professionnelles Microsoft ou Google. Tout l'écosystème commercial en aval profite de cette imprégnation précoce.
Il s'agit, en termes marketing, d'une stratégie de « land and expand » appliquée à un public captif de mineurs. L'école devient le premier maillon d'une chaîne de verrouillage qui se poursuit dans l'enseignement supérieur, la vie professionnelle et jusqu'aux usages personnels.

Et que dire des données ? Les informations collectées pendant toute la scolarité — résultats, comportement, absences, compétences acquises ou non, implication parentale, handicaps — constituent un profilage détaillé de millions de mineurs, accumulé sur au minimum treize ans.

Les rangs bougent parfois. Précisons et donnons tout de même des éléments concret.
Des solutions comme Pronote (Index Éducation, hébergement qualifié SecNumCloud sur datacenter propriétaire en France) ou École Directe (Aplim, hébergement en France sur infrastructure OVHcloud) montrent qu'il est parfaitement possible de gérer la vie scolaire avec des solutions françaises souveraines. Mais ces logiciels de vie scolaire coexistent au quotidien avec des suites bureautiques et collaboratives américaines, ainsi c'est dans Google Drive que les élèves et les professeurs partagent leurs travaux, dans Teams que les enseignants organisent leurs visioconférences, que des tablettes Chromebook ou iPad sont déployées.

La souveraineté des outils de gestion masque la dépendance des outils pédagogiques alors que le modèle alternatif existe déjà et nous allons en parler.

Les alternatives existent — et fonctionnent

Le discours selon lequel il n'existerait pas d'alternative crédible aux GAFAM dans l'éducation est factuellement faux.

Le Socle Interministériel des Logiciels Libres (SILL), maintenu par la DINUM, référence à ce jour plus de 530 solutions matures (ce chiffre augmente régulièrement) pour chaque usage et voici quelques exemples: LibreOffice pour la bureautique, Tiki Wiki pour la collaboration et la gestion de contenu, Nextcloud pour le partage de fichiers, Moodle pour le LMS, Thunderbird ou Tiki Wiki pour la messagerie, Jitsi Meet pour la visioconférence et jusqu'aux outils d'infrastructure : gestion de serveurs, supervision, analytics de trafic web, tout l'empilement technique dispose d'équivalents open source éprouvés en production.

Des hébergeurs français qualifiés SecNumCloud — OVHcloud, Cloud Temple, Outscale — peuvent accueillir les données éducatives dans un cadre juridiquement sécurisé, à l'abri des lois extraterritoriales américaines. Le surcoût estimé de 15 à 20 % par rapport aux hyperscalers est le prix de la souveraineté, mais c'est un investissement dans l'indépendance, pas une dépense superflue. Rappelons que Pronote, le logiciel de vie scolaire utilisé par la majorité des établissements secondaires français, a obtenu la qualification SecNumCloud : la preuve qu'un éditeur français peut atteindre le plus haut niveau d'exigence.

La Gendarmerie nationale a montré la voie à grande échelle. Depuis 2008, elle a progressivement migré l'ensemble de son parc avec quelque 70 000 postes en 2008 (le chiffre de 103 000 soit 97 % du parc est souvent donné pour 2024 sans source officielle) sous GendBuntu (sa propre distribution Ubuntu) avec LibreOffice, Firefox et Thunderbird. Résultat : une économie récurrente de plus de 700 000 licences et une baisse du coût total de possession de l'ordre de 40 % (chiffre régulièrement donné, sans source officielle), sans impact sur la productivité opérationnelle.

Une politique volontariste permettrait de généraliser des solutions open source matures comme Tiki Wiki, Odoo ou Moodle, de s’appuyer sur le catalogue du Comptoir du Libre de l’ADULLACT, de déployer les outils de LaSuite Numérique de la DINUM, et plus largement de mobiliser un écosystème riche de solutions libres et souveraines.. Il ne manque qu'un maillage structuré de conseillers numériques open source publics capables d'accompagner chaque établissement, chaque commune, chaque municipalité, musée, etc. vers des solutions souveraines, interopérables et hébergées localement, en faisant vivre un tissu de prestataires open source de proximité.

Et; les textes le prévoient déjà. La loi sur l'enseignement supérieur et la recherche de 2013 demande que « les logiciels libres soient utilisés en priorité » dans le service public de l'enseignement supérieur (article L.123-4-1 du code de l'éducation). La loi pour une République numérique de 2016 encourage l'utilisation des logiciels libres dans l'ensemble du secteur public. Ces textes existent. Ils sont simplement ignorés.

Former à la souveraineté, pas seulement à l'outil

L'enjeu éducatif dépasse la question des logiciels. C'est la culture numérique elle-même qui doit être repensée. Apprendre à un élève à utiliser Word, c'est former un consommateur. Lui apprendre à comprendre ce qu'est un format de fichier, pourquoi l'interopérabilité compte, comment fonctionnent les données personnelles, c'est former un citoyen.

Selon l'enquête internationale TALIS 2018, seuls 34 % des enseignants du premier degré avaient participé à une formation relatif au numérique dans l'année écoulée. Ce déficit est une opportunité : former les formateurs non pas sur un produit commercial spécifique, mais sur des compétences transversales et des outils ouverts, c'est investir dans l'autonomie à long terme.

Le programme européen Erasmus+ et le Digital Education Action Plan 2021-2027 soutiennent déjà cette vision. Des initiatives comme les résidences d'artistes numériques en collège ou les ateliers de pensée critique face à la désinformation montrent qu'il est possible d'enseigner le numérique sans se soumettre aux plateformes qui en monopolisent l'accès.

Pour engager cette transition, les établissements et organisations peuvent s’appuyer sur différents acteurs spécialisés. Open Source Solutions fait partie de ces acteurs et propose |un accompagnement technique structuré en souveraineté numérique, depuis l’audit jusqu’à la migration vers des solutions libres et souveraines permettant de transformer l'intention en réalité opérationnelle.

L'appel à la cohérence

La souveraineté numérique ne peut pas être un objectif du matin et une contradiction de l'après-midi. On ne peut pas créer un Observatoire de la souveraineté numérique en janvier 2026 et avoir

signé un accord-cadre Microsoft de 152 millions d'euros dix mois plus tôt. On ne peut pas interdire Office 365 dans les administrations et le financer dans les écoles. On ne peut pas légiférer sur la protection des données tout en confiant celles de 12 millions d'élèves à des entreprises soumises au Cloud Act.

La cohérence n'est pas un luxe. C'est la condition de la crédibilité. Et cette crédibilité déterminera si la France et l'Europe parviendront à transformer leurs ambitions en infrastructure réelle — ou si elles continueront d'écrire des feuilles de route sur des serveurs américains.

L'Observatoire, confié au Haut-commissariat à la stratégie et au plan, doit livrer ses premières analyses au printemps 2026. Il pourrait constituer un tournant — à condition que ses conclusions se traduisent en décisions concrètes de commande publique, en critères d'exclusion dans les marchés sensibles, et en feuilles de route de migration pour les administrations les plus dépendantes. Surtout, cette cohérence doit s'appliquer du début à la fin de la chaîne : les entreprises et les simples utilisateurs doivent être inclus dans cette marche vers l'autonomie numérique.

Les outils existent.
Les compétences existent.
Le cadre juridique existe.
Ce qui manque, c'est la volonté de passer du discours aux actes — décision par décision, marché public par marché public, salle de classe par salle de classe. Faire de l'éducation numérique le point de départ de la désaccoutumance, c'est reconnaître que la souveraineté se construit dès le plus jeune âge.

Dans notre troisième et (sans doute) dernier article de cette série, nous aborderons les solutions concrètes à l'échelle des organisations. Nous détaillerons comment une PME, une collectivité ou un établissement peut, dès aujourd'hui, reprendre le contrôle de son infrastructure numérique en s'appuyant sur des alternatives souveraines et opérationnelles.