ÉTUDE / Rapport

Numérique responsable, un levier stratégique de souveraineté numérique en France et en Europe

Avril 2026

ASSOCIATION green it

Auteur·rices

Étude : Numérique responsable : un levier stratégique de souveraineté numérique en France et en Europe

Version : 1.0
Date de publication : 1er avril 2026

Auteur·rices :

- Laure Dupin, Danù Green
- Laure Alfonsi, Zeb & Web

Contributeurs·rices :

- Frédéric Bordage, GreenIT.fr
- Anne Rabot, Enezann
- Xavier Prizé, Freelance

Contact :

Association Green IT
contact@greenit.eco
Téléphone : 06.09.62.22.51

Introduction

La souveraineté numérique comme capacité de maîtrise

La **souveraineté numérique** se définit comme la capacité d'un État, d'un territoire ou d'une organisation à **maîtriser ses infrastructures, ses données, ses technologies critiques et ses chaînes de valeur numériques**, afin de préserver son autonomie stratégique, sa sécurité et sa liberté de décision.

Elle ne se réduit pas à la localisation des serveurs ni à la nationalité des fournisseurs – c'est une réalité **systémique** qui mêle des enjeux technologiques, industriels, juridiques, énergétiques et géopolitiques. Par exemple, même des données hébergées sur le sol européen peuvent rester soumises à des lois extra-européennes telles que le **Cloud Act** américain, si l'opérateur est une entreprise de droit américain[1] ; un logiciel américain est soumis aux US Export Laws, et interdire son utilisation par certains collaborateurs selon leur nationalité, par exemple.[31]

La souveraineté numérique implique donc de **conserver le contrôle juridique et technique** de son écosystème numérique.

En Europe, de multiples signaux d'alarme ont été émis au cours des dernières années. Les rapports de la Commission européenne – notamment le bilan **State of the Digital Decade 2025** – ainsi que les travaux du Cigref (Club informatique des grandes entreprises françaises) et les analyses de l'ANSSI convergent vers un même constat[2,3] : la **dépendance aux acteurs extra-européens est devenue structurelle**. Plus de **la moitié des entreprises de l'UE utilisent désormais des services de cloud** nord-américains – une proportion atteignant *près de 85% pour les grandes entreprises*[4] – et cette part continue de croître (+7,4 points entre 2023 et 2025)[4]. Surtout, ces services cloud portent de plus en plus sur des fonctions critiques (bases de données managées, plateformes applicatives, analyse de données, intelligence artificielle).

Quelques fournisseurs mondiaux concentrent l'essentiel de ces services à forte valeur ajoutée, entraînant un **verrouillage progressif** : plus les volumes de données et d'usages augmentent, plus les organisations s'appuient sur des solutions propriétaires intégrées, et plus les coûts de réversibilité explosent. La dépendance devient alors *auto-entretenue*, inscrite au cœur même des architectures et contrats numériques. Notons que ce verrouillage progressif ne dépend pas d'une architecture technique. Ce mécanisme s'applique bien au-delà du *cloud*.

Face à cette situation, les réponses politiques se multiplient. L'Europe mise sur des stratégies de **substitution technologique** ambitieuses : développement de *clouds souverains* (initiatives du type GAIA-X, offre « Cloud de confiance » en France), renforcement d'une filière industrielle du numérique (par exemple via le **Chips Act** pour augmenter la part européenne dans la production mondiale de semi-conducteurs [5]) ou encore soutien massif à la fabrication locale de composants critiques. Ces efforts, bien que nécessaires, sont longs à déployer et limités quant à leurs aboutissements économiques et géopolitiques. Il suffit en effet qu'un seul composant, qu'une seule étape manque pour créer un Single Point of Failure dans cette recherche de souveraineté.

Dans ce contexte, **le numérique responsable apparaît comme un levier complémentaire, immédiatement activable, permettant de *réduire la dépendance avant même de la remplacer*.** Plutôt que de chercher uniquement à recréer des alternatives européennes à l'identique de ce qui existe ailleurs (approche défensive), il s'agit non seulement **d'agir sur la demande et les usages** pour alléger dès maintenant le fardeau de la dépendance ; mais aussi d'envisager un numérique hybride, associé à des technologies low-tech pour lesquelles la souveraineté est facile à atteindre.

Cette étude propose d'analyser en profondeur comment une démarche de **numérique responsable** – intégrant sobriété, écoconception, low-tech, slow-tech et IA frugale – peut renforcer la souveraineté numérique de la France et de l'Europe.

Nous commencerons par dresser les constats d'une **dépendance multidimensionnelle** (technologique, économique, industrielle, environnementale, juridique). Nous présenterons ensuite les **solutions et leviers** qu'offre le numérique responsable pour reconquérir des marges de manœuvre stratégiques. Une attention particulière sera portée aux recommandations opérationnelles pour les institutions, les entreprises et les citoyens, ainsi qu'à des **cas d'usage concrets** illustrant ces leviers en action. Enfin, nous conclurons par une vision stratégique : celle d'une souveraineté numérique « lucide », fondée sur la maîtrise et les choix éclairés plutôt que sur l'illusion d'une indépendance totale.

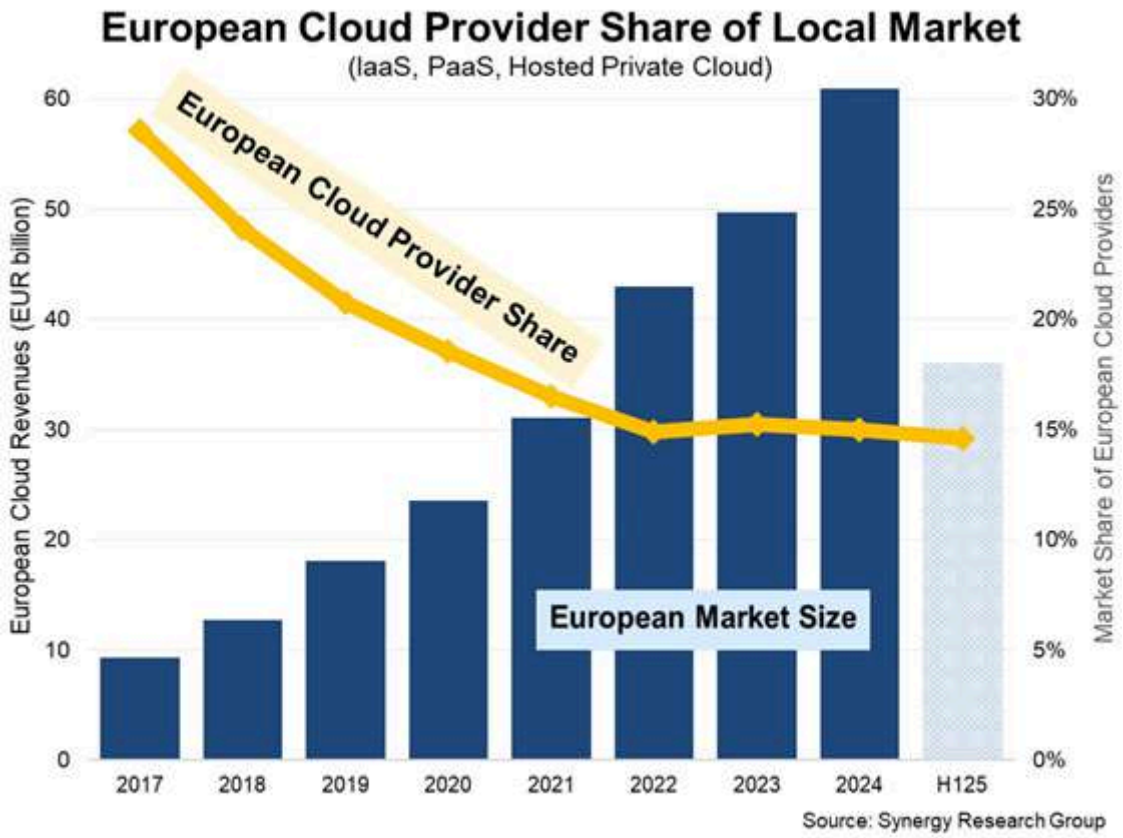
Les constats : une dépendance multidimensionnelle

Une dépendance technologique alimentée par l'augmentation des usages

La **dépendance numérique européenne** ne résulte pas uniquement d'un manque d'alternatives locales ; elle découle aussi de la croissance exponentielle des usages et des données. Comme indiqué, *52,7% des entreprises européennes utilisaient des services cloud payants en 2025*, contre 45% en 2023[4]. Cette moyenne cache de fortes disparités selon la taille : **84,7% des grandes entreprises** y recouraient en 2025[4].

D'autre part, le cloud s'infiltre désormais dans des domaines névralgiques : systèmes ERP, plateformes Big Data, services d'IA, etc. La Commission européenne souligne ainsi que la transformation numérique va de pair avec une montée en dépendance vis-à-vis d'un petit nombre d'**hyperscalers** , le plus souvent nord-américains, qui fournissent ces services de pointe.

Ce phénomène crée un **effet de verrouillage** : plus les organisations accumulent de données et de processus critiques dans des environnements cloud propriétaires, plus il devient coûteux et complexe d'en sortir. Les coûts de migration, les enjeux d'interopérabilité et la perte de fonctionnalités freinent toute réversibilité. À terme, la dépendance devient **structurelle**, inscrite dans l'architecture même des SI (systèmes d'information). Une étude du Cigref en 2025 a tenté de quantifier cette emprise : d'après leurs estimations, environ **83% du marché européen des logiciels et services cloud** est aujourd'hui capté par des acteurs américains, représentant un flux financier de **264 milliards d'euros par an** partant d'Europe vers les États-Unis[2]. Ce transfert massif de valeur contribue à financer **1,9 million d'emplois américains** dans le secteur du numérique, pendant que l'Europe perd en investissement, en innovation et en recettes fiscales sur son propre sol[2].



Evolution du marché du cloud en Europe : les fournisseurs non européens (majoritairement américains) captent environ 85% du marché en 2024, ne laissant que 15% aux acteurs européens[6]*. La domination des trois hyperscalers leaders (AWS, Microsoft, Google) s'établit à 70% de part de marché à elle seule*[6]*, reflétant un déséquilibre préoccupant pour la souveraineté numérique.*

Au-delà des chiffres, cette concentration pose un problème de **contrôle**. Elle expose les États et organisations européennes à plusieurs risques : risque juridique (soumission au droit étranger, voir l'exemple du Cloud Act évoqué en introduction), risque opérationnel (dépendance à la roadmap et aux décisions tarifaires d'un fournisseur unique), et risque stratégique (perte de compétences internes au profit d'une externalisation intégrale). Enfin, cette domination technologique s'accompagne d'une **dépendance en matière de cybersécurité** : les failles ou incidents majeurs affectant un acteur dominant (attaque d'un cloud provider, coupure d'un service SaaS critique, etc.) ont des impacts systémiques sur l'ensemble du tissu économique.

En synthèse, l'Europe s'est placée dans une situation où son **infrastructure numérique vitale** repose sur des piliers qu'elle ne maîtrise pas pleinement. Cette dépendance technologique est d'autant plus alarmante que les autres composantes de la chaîne de valeur numérique présentent, elles aussi, des fragilités structurelles pour la souveraineté.

Complexité logicielle et fragilité stratégique

La souveraineté numérique se joue aussi au niveau de la **maîtrise technique** des systèmes d'information. Héberger ses données en Europe n'est qu'un aspect du problème ; encore faut-il **comprendre, auditer et sécuriser** les logiciels et services que l'on utilise, savoir où sont réalisés les traitements faits sur les données. Or, depuis deux décennies, l'empilement des couches logicielles et la prolifération d'APIs et de services managés « boîtes noires » ont considérablement réduit la visibilité qu'ont les organisations sur leur propre informatique. L'utilisation de bibliothèques open source dont on ignore parfois la provenance exacte, l'usage de frameworks ou de microservices gérés par des tiers, du code déployé dans des conteneurs sur des orchestrateurs pilotés par d'autres, etc. Cette **complexité croissante** engendre une double fragilité : *dépendance technique* et *vulnérabilité en termes de sécurité*.

Le Cigref souligne que la **dépendance n'est pas que contractuelle, elle est aussi technique** [2] : même si l'on pouvait juridiquement se libérer d'un fournisseur, la complexité d'interconnexion des systèmes rend tout changement coûteux et risqué. Par exemple, une entreprise souhaitant migrer hors d'un grand cloud public peut se heurter à la difficulté de recréer en interne tous les services managés (bases de données scalables, fonctions serverless, IA as a service…) dont elle dépend. La **sortie** devient un casse-tête technique qui dissuade de bouger – c'est le fameux *vendor lock-in*.

Sur le plan de la **cybersécurité**, la complexité et l'opacité augmentent aussi la surface d'attaque et réduisent la capacité de réaction. Quand une chaîne applicative fait intervenir 5 ou 6 sous-systèmes différents issus de fournisseurs variés, une faille dans l'un (par ex. une bibliothèque open source vulnérable, comme l'épisode *Log4Shell*) peut compromettre l'ensemble, sans que l'organisation visée n'ait même conscience d'utiliser le composant en question. En outre, la **dépendance aux mises à jour** de sécurité fournies par des éditeurs externes place les utilisateurs en position d'attente : ils subissent un calendrier de correctifs qu'ils ne contrôlent pas. Si un éditeur cesse le support d'un produit, l'utilisateur est confronté à un dilemme : migrer (au prix fort) ou rester avec une solution obsolète et risquée.

Enfin, la tendance à externaliser de nombreuses fonctions **critiques** (authentification, paiement, cartographie, analytics, etc.) via des API tierces ou des modules « plug-and-play » pose la question de la **souveraineté des données** qui transitent par ces briques. Beaucoup d'applications envoient des données chez Google (via Firebase, Google Maps, etc.), Microsoft, Amazon ou d'autres simplement parce que les développeurs ont intégré des SDK ou services pratiques. L'organisation se retrouve alors *otage* de ces dépendances cachées : un changement de politique du fournisseur tiers (tarification, conditions d'utilisation, fermeture de l'API) peut mettre en péril une fonctionnalité de l'entreprise utilisatrice.

En résumé, la **perte de maîtrise technique** liée à la complexité logicielle affaiblit la souveraineté. Une architecture sur-complexe, aux dépendances multiples, est difficile à auditer, difficile à faire évoluer de façon autonome, et souvent liée à des éditeurs spécifiques. À l'inverse, **simplicité et transparence** sont des atouts stratégiques : un système d'information épuré, documenté, bâti sur des standards ouverts et du logiciel libre autant que possible, sera plus facile à contrôler et à faire évoluer en fonction des intérêts propres de l'organisation. Nous verrons plus loin comment l'écoconception et la low-tech peuvent contribuer à cette simplification.

Une dépendance industrielle aux semi-conducteurs et aux métaux critiques

Si le *soft* (logiciels et services) est largement importé, le *hard* l'est tout autant. Le numérique repose sur des infrastructures **matérielles** – serveurs, terminaux, réseaux – dont la fabrication et l'assemblage sont largement externalisés hors d'Europe. La production mondiale de composants essentiels, notamment les **semi-conducteurs**, est aujourd'hui ultraconcentrée en Asie de l'Est et aux États-Unis. L'Europe ne représente qu'environ **10% de la production mondiale** de semi-conducteurs, principalement sur des technologies intermédiaires ou matures[7]. Les puces les plus avancées (<5 nm) sont l'apanage quasi-exclusif de fonderies comme TSMC (Taïwan) ou Samsung (Corée du Sud), tandis que les États-Unis dominent la conception des circuits intégrés[7].

Consciente de cet écart, l'UE a lancé en 2022 le **European Chips Act** pour tenter de doubler la part européenne à *20% d'ici 2030*[6] – un objectif qui révèle l'ampleur du retard accumulé, sans résoudre le problème. La complexité actuelle des équipements rendra toujours nécessaire l'utilisation de composants non souverains. La souveraineté doit donc s'envisager de façon graduelle.

Par ailleurs, cette dépendance industrielle est indissociable de celle aux **matières premières critiques**. Nos équipements numériques contiennent de nombreux métaux et terres rares (lithium, cobalt, nickel, cuivre, indium, tantale, terres rares, etc.) dont l'extraction et le raffinage sont dominés par quelques pays (Chine, République démocratique du Congo, Chili, Australie, États-Unis…). D'après le rapport 2023 de la Commission européenne sur les matières premières critiques, l'UE dépend quasi intégralement des importations pour la plupart de ces ressources stratégiques. Or ces ressources ne sont pas infinies : une analyse récente de l'Association Green IT indique que les **réserves "rentables" disponibles (autrement dit le "fond de roulement") pour la majorité des métaux critiques du numérique se réduit de plus en plus, représentant moins de 10 ans de consommation courante pour la plupart d'entre eux**[8]. En clair, au rythme actuel de consommation, *la génération suivante pourrait faire*

face à des tensions sévères sur les marchés des métaux pour fabriquer les appareils high-techs, à moins d'une drastique inflexion.

Le **premier impact** de cette réalité est environnemental, car l'extraction de ces métaux est à la fois polluante, énergivore et destructrice pour les écosystèmes. Mais il est aussi géopolitique : un numérique avide en nouveaux équipements signifie une **dépendance accrue à des chaînes d'approvisionnement mondiales fragiles**. Tout choc (tension diplomatique, crise minière, protectionnisme) pourrait provoquer des ruptures d'approvisionnement. Rappelons que la fabrication des équipements représente aujourd'hui **la majeure partie de l'empreinte environnementale du numérique** en France et en Europe – jusqu'à 78% des émissions de gaz à effet de serre du secteur, contre 21% pour la phase d'usage [9]. Chaque cycle de renouvellement accéléré des smartphones, ordinateurs, objets connectés et serveurs vient ainsi *aggraver* l'empreinte carbone **et** renforcer la dépendance industrielle et géopolitique. Un numérique intensif en équipements ne peut être souverain s'il repose sur des matériaux dont l'accès n'est pas garanti à moyen terme.

En somme, la question des métaux critiques et des composants est plus que environnementale : elle est **stratégique**. **Qui contrôle la production des ressources physiques du numérique contrôle, en partie, l'avenir numérique**. L'Europe doit composer avec ce fait : elle ne dispose pas – ou plus – sur son sol des mines, des usines et des compétences suffisantes pour soutenir seule la demande. Cette vulnérabilité industrielle appelle des réponses urgentes en matière de circularité, d'innovation dans les matériaux et de maîtrise de la demande, que nous aborderons plus loin.

Une dépendance aux infrastructures réseau mondiales

La France repose sur **un maillage d'infrastructures globales** contrôlées pour beaucoup par des acteurs étrangers et par les GAFAM. Les câbles sous-marins, les points d'atterrissage (landing points), les points d'échange Internet (IXP) et les géants du CDN/DNS constituent les principaux vecteurs de dépendance.

Trains de trafic dominés par les GAFAM et les US

D'après l'Arcep, la catégorie *« GAFAM »* (Google, Amazon, Meta, Microsoft, Apple) représente environ **25 % du trafic Internet total en France**. En 2024, Amazon a généré 8,6 % du trafic, Google 7,3 %, Meta 5,4 %, tandis que Microsoft et Apple atteignent chacun ~1–1,6 %. Un indicateur similaire est avancé par Jean-Luc Vuillemin d'Orange : *« Aujourd'hui, 80 % du trafic généré par les internautes français part vers les États-Unis »*, soulignant que le réseau mondial est majoritairement centré sur les points d'échange et de peering américains. En clair, une majorité de nos flux transitent par les hubs américains (New York, Los Angeles, etc.) ou via des serveurs US des GAFAM. Cette

situation conforte la dépendance aux infrastructures et aux décisions politiques américaines. Par exemple, le débat sur la neutralité du Net, soutenu par La Quadrature du Net et les géoblocages concerne directement les opérateurs américains (Netflix, Google, etc.) qui maîtrisent les contenus et l'acheminement.

Contrôle des câbles sous-marins par les GAFAM

Les câbles sous-marins sont le fondement de l'interconnexion mondiale. Ces dernières années, les GAFAM sont devenus des acteurs majeurs de ces infrastructures. Les études montrent que les géants du web américains possèdent désormais près de **la moitié** des câbles sous-marins mondiaux les plus puissants. Google est emblématique : il détient 32 des ~500 câbles existants (dont la moitié en propre). Par exemple, le câble **Dunant** (Virginie – Bretagne) est la propriété exclusive de Google. L'opérateur français Orange n'y est présent que comme gestionnaire de l'atterrissement en France, pour deux paires de fibres. Cette concentration donne aux GAFAM un **pouvoir géostratégique** : théoriquement, un propriétaire de câble pourrait couper ou prioriser certains flux. Les acteurs non-Américains (opérateurs télécoms européens, asiatiques, chinois) restent cantonnés aux câbles plus anciens ou moins capacitaires. À noter qu'une analyse de l'Arcep indique que près de **40 % du trafic international à destination ou en provenance de France** transite par câbles sous-marins. Tout incident sur ces liaisons (coupure accidentelle, sabotage, Brexit impactant infrastructures partagées) aura donc un effet marqué sur la connectivité française. En effet, comme le relève Ophélie Coelho dans « Géopolitique du numérique » [30], la propriété des câbles sous-marins se révèle être un avantage stratégique majeur dès la première guerre mondiale. Elle permettra au gouvernement britannique à la fois d'isoler l'Allemagne en coupant ses communications à ses colonies, mais aussi d'intercepter des messages stratégiques.

Points d'atterrissage et peering

La France compte plusieurs points d'atterrissement majeurs, appelés IXP, (Brest, Marseille, Le Havre) où convergent les câbles (destinés notamment aux USA, au Brésil, à l'Afrique du Nord). En aval, les points d'échange Internet (France-IX, PARIX, Telehouse) concentrent le trafic inter-entreprises. Or les GAFAM sont massivement connectés à ces IXP : Google, Amazon, Meta ont leurs propres AS (systèmes autonomes) et serveurs dans les principaux IXP parisiens. Cela leur garantit des temps de transit minimaux et de l'autonomie. En pratique, cela signifie que même pour des flux intra-Européens, le routage peut passer par des équipements américains (ex. services Cloud de Microsoft Azure sont souvent hébergés aux US). Par ailleurs, de nombreux DNS publics (ex. Google Public DNS) et CDN (Akamai, Cloudflare) utilisés en France sont américains.

Risques associés

Cette configuration pose plusieurs risques majeurs pour la souveraineté :

- **Contrôle et interception** : les opérateurs étrangers (notamment américains) maîtrisent les points névralgiques de l'Internet. Ils peuvent légalement être contraints par leur État à intercepter ou censurer des données (CLOUD Act, Patriot Act). Par exemple, le fait qu'une grande partie du trafic français passe par des infrastructures US implique qu'il est soumis en partie au droit américain

- **Résilience fragilisée** : une coupure de câble (naturelle ou malveillante) ou un problème de transit international peut avoir un impact directement sur la France. L'absence d'alternatives souveraines sur certaines infrastructures est une source de fragilité. En cas de crise géopolitique, un opérateur étranger pourrait donner la priorité à son trafic national au détriment du trafic international.

- **Neutralité du réseau :** les accords commerciaux entre grands opérateurs peuvent biaiser la neutralité. Par exemple, certains accords de peering bilatéraux privilégiés (peering privé Google-France Télécom) peuvent contourner un Internet neutre. D'autres contenus européens peuvent pâtir d'une moindre capacité CDN.

- **Économique et politique :** ce modèle fragilise les modèles économiques. Par ailleurs, il limite les leviers de régulation français sur le numérique (puisque les serveurs et câbles critiques sont détenus par des sociétés hors de portée).

L'énergie et l'eau : des dépendances souvent invisibles

Souvent, le débat sur la souveraineté numérique met l'accent sur l'**électricité** et le **carbone**, notamment via le prisme des data centers. Si la France bénéficie d'un mix électrique relativement décarboné (grâce au nucléaire et aux renouvelables), il n'en demeure pas moins que **la croissance des usages numériques accentue la pression énergétique**. L'Agence Internationale de l'Énergie estimait qu'en 2023 les data centers consommaient mondialement environ 1 à 1,5% de l'électricité, et cette part pourrait doubler d'ici quelques années sous l'effet du boom de l'IA et du cloud[10]. Externaliser massivement ses infrastructures dans le cloud revient donc, pour un pays comme la France, à « importer » une demande électrique supplémentaire, souvent produite dans des pays au mix plus carboné (États-Unis, Asie) et à **déplacer une partie de la dépendance vers les énergies fossiles**. En d'autres termes, sans gouvernance, le cloud peut servir de **transfert de responsabilités** en matière énergétique : on profite ici des services numériques, mais l'énergie consommée pour les faire tourner est dépensée ailleurs, parfois avec du charbon ou du gaz.

Au-delà de l'électricité, un autre aspect est longtemps passé sous les radars : l'**eau**. Les data centers utilisent d'énormes volumes d'eau douce pour le refroidissement des serveurs, notamment lorsqu'ils fonctionnent avec des circuits de refroidissement par évaporation. Selon des analyses, **un centre de données de taille moyenne peut**

consommer autant d'eau qu'une petite ville, tandis que les plus gros « hyperscaler » nécessitent jusqu'à *5 millions de gallons d'eau par jour* (soit environ **19 millions de litres quotidiens**, équivalent à la consommation d'une ville de 50 000 habitants)[11]. Dans des régions déjà exposées au stress hydrique ou aux sécheresses, cette ponction sur les réserves locales d'eau douce entre en concurrence avec d'autres usages essentiels (agriculture, eau potable…). Ainsi, aux Pays-Bas, l'implantation de vastes data centers a suscité des controverses en raison des quantités d'eau prélevées dans les nappes phréatiques locales. Aux États-Unis, l'essor des fermes de serveurs pour l'IA se heurte à des préoccupations similaires, certaines installations ayant consommé plus de 80 millions de litres d'eau potable en un an[12,13] Nos usages numériques sont aussi indirectement à l'origine d'une autre consommation d'eau lors de la production d'énergie, nucléaire, par exemple. Le dernier rapport de France stratégie consacré à la demande en eau à horizon 2025 met en lumière cette double dépendance.[29]

Cette **dépendance hydrique** jusqu'alors peu débattue devient un enjeu de **résilience territoriale** : un numérique intensif en calcul est indirectement intensif en eau, ce qui pourrait fragiliser certaines régions en cas de sécheresse. De plus, ces consommations d'eau et d'énergie font courir un risque d'**acceptabilité sociale** : l'opinion publique peut se retourner contre des infrastructures perçues comme « gloutonnes » en ressources naturelles. Enfin, notons que l'empreinte environnementale globale du numérique (carbone, eau, matières) devient un enjeu de souveraineté en soi : dépendre d'un modèle numérique non durable, c'est s'exposer à des chocs futurs (réglementations climatiques, pénuries) qui limiteront brutalement nos marges de manœuvre.

L'IA : un accélérateur de dépendances

L'**intelligence artificielle**, notamment l'**IA générative**, accentue encore les dynamiques précédentes. Les modèles de pointe (GPT-4, PaLM, Llama 2…) requièrent des capacités de calcul colossales pour l'entraînement et l'inférence, capacités détenues quasi exclusivement par les grands acteurs mondiaux disposant de data centers gigantesques. Ainsi, se lancer dans l'IA avancée implique presque inévitablement de consommer des services cloud de Google, Amazon, Microsoft ou d'utiliser des API fournies par OpenAI, AWS, etc. Le risque est de voir émerger une **nouvelle couche de dépendance** : après l'infrastructure (IaaS) et les logiciels (SaaS), celle des *modèles d'IA* eux-mêmes, fournis en tant que service (*MLaaS* – Machine Learning as a Service).

L'adoption massive et peu sélective de ces IA externalisées renforce mécaniquement la **dépendance aux plateformes extra-européennes**, tout en posant des enjeux nouveaux. Sur le plan **sécurité**, l'ENISA (agence européenne de cybersécurité) et l'ANSSI alertent sur les vecteurs d'attaque spécifiques à l'IA[14,3] : injections de requêtes

malveillantes (*prompt injection*), empoisonnement de données d'entraînement, fuite de données confidentielles via les modèles, etc. Les organisations qui intègrent de l'IA génèrent souvent des flux de données sensibles vers les services d'IA (par exemple, un employé qui interroge ChatGPT avec du texte interne). Si ces services sont hors de leur contrôle, un risque de **perte de confidentialité** apparaît, sans parler de la difficulté d'auditer le comportement du modèle (*boîte noire*).

Par ailleurs, l'**empreinte énergétique et environnementale** de l'IA est très lourde. Selon l'étude de l'association Green IT sur les impacts de l'IA dans le monde, les projections prévoient que l'IA mondiale émettra en 2030 autant de gaz à effet de serre que la France entière. En phase d'entraînement, un modèle de langage peut consommer des mégawattheures d'électricité et des millions de litres d'eau pour refroidir les GPU qui effectuent les calculs [11][15]. En phase d'utilisation, une requête à un grand modèle nécessite bien plus de calcul qu'une requête web classique. Si une entreprise ou une administration externalise massivement ses traitements d'IA, elle externalise donc d'autant une consommation d'énergie (souvent carbonée) et d'eau associée. Cela **accentue la dépendance énergétique** évoquée plus haut, tout en créant un angle mort dans les bilans carbone (puisque l'énergie est consommée hors de ses murs, elle peut passer inaperçue dans ses propres comptes).

Enfin, sur le plan **réglementaire**, l'IA fait émerger un risque de dépendance aux cadres juridiques étrangers. Les questions d'éthique et de régulation de l'IA (biais algorithmiques, transparence, responsabilité en cas de dommages causés par une IA, etc.) sont débattues au niveau international. L'Europe a publié l'**AI Act** en juin 2024 [16], la première régulation globale sur l'intelligence artificielle, qui vise notamment à classer les systèmes d'IA par niveau de risque et à imposer des obligations de conformité pour les IA à risque élevé. Si les IA déployées en Europe proviennent majoritairement de fournisseurs non européens, il faudra s'assurer qu'elles respectent ce cadre. Sinon, on verra se reproduire la situation du RGPD vs les services cloud américains : une potentielle **incompatibilité juridique** entre des IA pensées ailleurs et les exigences européennes (par exemple en matière d'explicabilité ou de traitement des données personnelles).

En synthèse, l'IA agit comme un multiplicateur de dépendances. Sans stratégie, elle risque d'approfondir le sillon de l'importation de technologies non maîtrisées et d'en créer de nouvelles (dépendance aux modèles, aux bibliothèques d'IA, aux puces spécialisées type GPU/TPU dominées par Nvidia, Google, etc.). Conjuguée aux constats précédents (cloud, matériel, données, complexité), cette tendance plaide pour une réaction urgente : il s'agit de définir une approche de l'IA qui serve nos intérêts stratégiques, plutôt que d'en subir passivement les conséquences.

Les solutions : le numérique responsable comme stratégie de souveraineté

Face à des **dépendances technologiques, industrielles, énergétiques et juridiques** profondément ancrées, la réponse ne peut pas être uniquement *substitutive* ou purement industrielle. Nous n'achèverons pas en quelques années la relocalisation complète des usines de semi-conducteurs, ni la création d'un GAFAM européen couvrant tous les services numériques. Une stratégie de souveraineté efficace doit aussi être **structurelle**, c'est-à-dire agir sur la **réduction maîtrisée des besoins** et l'optimisation de l'usage des ressources. Autrement dit, la souveraineté numérique ne se construit pas seulement *en créant des alternatives* européennes, mais aussi *en réduisant la dépendance aux services et ressources non maîtrisés*.

C'est précisément là qu'intervient le **numérique responsable**. En intégrant des principes de sobriété, de frugalité, de durabilité et de maîtrise d'usage, il offre une voie pour *diminuer notre exposition* aux dépendances identifiées, tout en accélérant la transition écologique du numérique. Nous détaillons ci-après les leviers principaux d'une stratégie de numérique responsable au service de la souveraineté : **minimisation des volumes de données**, **prolongation de la durée de vie des équipements**, **écoconception**, approche **Slow Tech**, orientation **Low Tech**, **désescalade technologique** et, en dernier recours, **IA frugale**. Chacun de ces leviers s'accompagnera de recommandations concrètes et d'exemples illustrant son impact potentiel.

Réduire les volumes pour restaurer la marge de manœuvre stratégique

Étant donné que la dépendance est souvent proportionnelle aux volumes de données et de services consommés, **reprendre le contrôle sur la croissance des volumes** est une première action de souveraineté. Cela consiste à appliquer un principe simple : *moins de données stockées et échangées, c'est moins de dépendance*. Les travaux conjoints de l'ARCEP et de l'ADEME sur le numérique soutenable[17] montrent en effet que l'augmentation exponentielle des flux de données est un facteur central de l'empreinte environnementale du numérique, mais aussi de la pression sur les infrastructures cloud et réseau. En corollaire, plus nos organisations accumulent de données, plus elles s'en remettent à des solutions de stockage et traitement externes, ce qui renforce le verrouillage.

Pour **inverser la vapeur**, il est possible de s'inspirer d'un principe bien connu en protection des données personnelles : le principe de **minimisation** (inscrit dans le RGPD). Appliqué de manière générale, cela signifie : ne collecter et conserver que les données réellement nécessaires à la mission, éviter les duplications inutiles, *nettoyer les données dormantes*, et questionner systématiquement la *valeur ajoutée* de chaque usage analytique ou de chaque indicateur stocké. De nombreuses organisations seraient surprises de découvrir la quantité de données qu'elles stockent sans jamais les utiliser : selon une enquête mondiale, **60% des décideurs estiment qu'au moins la moitié des données de leur entreprise sont des "données sombres"** (dark data) non exploitées, et un tiers d'entre eux pensent même que plus de 75% des données stockées dorment inutilement[18]. Plus globalement, des analyses comparent ces *données inutilisées* à de la « matière noire » : elles occupent de l'espace, consomment de l'énergie de stockage, mais n'apportent aucune valeur car personne n'en fait rien[19]. Éliminer ou ne pas générer ces volumes superflus permettrait de **réduire les coûts, la consommation et l'exposition aux risques** (puisque toute donnée stockée peut faire l'objet d'une fuite ou d'une réquisition légale).

Concrètement, une politique de **sobriété des données** comporte plusieurs volets opérationnels :

- **Gouvernance des données** : instaurer des procédures de tri, d'archivage raisonné et de purge des données selon leur utilité et leur sensibilité. Par exemple, une administration pourrait décider de supprimer automatiquement certains logs techniques au bout de 6 mois si elles ne sont pas exploitées, là où auparavant elles étaient conservées indéfiniment « au cas où ».
- **Lutte contre les "dark data"** : mener des audits réguliers des stockages pour identifier les volumes orphelins ou redondants. Certaines grandes entreprises ont initié des programmes de *data cleaning* et ont découvert des teraoctets de vieux documents, backups ou datasets jamais utilisés. Gartner estime d'ailleurs que plus de 50% des données d'entreprise sont ainsi redondantes, obsolètes ou triviales[19] – un gisement de simplification non négligeable.
- **Minimisation dès la conception** : dans les nouveaux projets, questionner *en amont* les besoins en données. A-t-on besoin de suivre 100% des clics des utilisateurs sur un site web si cela n'est pas exploité ensuite ? Peut-on se contenter d'indicateurs agrégés plutôt que de stocker chaque enregistrement détaillé ? Cette approche rejoint l'écoconception (ne pas sur-spécifier les besoins).

On retrouve ces bonnes pratiques dans les référentiels d'écoconception tels que le RGESN ou le RWEB (référentiel web de Green IT). Les bénéfices d'une telle démarche de sobriété numérique sont multiples. Sur le plan *stratégique*, **moins de volumes signifie plus de réversibilité** : une base de données de 1 To sera plus facile à migrer ou rapatrier qu'un lac de données de 100 To. Sur le plan *juridique*, cela réduit l'exposition – par exemple, moins de données personnelles stockées signifie moins de surface pour des fuites et une conformité RGPD facilitée. Sur le plan *économique*, stocker et traiter moins de données peut réduire significativement les factures cloud (qui sont souvent indexées sur les volumes). Enfin sur le plan *écologique*, c'est autant d'énergie et de ressources économisées (serveurs, disques…) – ce qui, in fine, allège la pression sur la fabrication de nouveaux équipements. On peut ainsi résumer : **« Moins de données, c'est moins de dépendance »**.

En adoptant une telle stratégie de **sobriété numérique**, les organisations peuvent commencer à regagner de la marge de manœuvre indépendamment des avancées industrielles. C'est un premier pas vers une souveraineté choisie : éviter l'excès avant de combler le manque.

Allonger la durée de vie des équipements : réduire la dépendance aux métaux critiques

Si la fabrication des équipements est le talon d'Achille environnemental et stratégique du numérique, la **première solution** est d'en limiter le renouvellement. *Allonger la durée de vie* des terminaux (smartphones, ordinateurs, tablettes…), des serveurs et autres matériels permet de **différer l'extraction de nouveaux métaux** et de diminuer le volume d'équipements à produire sur une période donnée. Autrement dit, c'est gagner du temps sur l'épuisement des ressources et réduire la dépendance vis-à-vis des chaînes d'approvisionnement lointaines.

Selon l'ADEME, prolonger de 2 à 4 ans l'usage d'un équipement peut réduire de 50% son impact annuel (puisque l'impact de fabrication est « amorti » sur une plus longue période) [20]. C'est précisément la promesse de certains acteurs pionniers comme **Fairphone**. Ce constructeur européen de smartphones durables offre une garantie de 5 ans et un support logiciel d'au moins 8 à 10 ans sur ses modèles récents, soit **le double de la durée de support habituelle dans l'industrie**. Grâce à cette approche (matériel modulaire et réparable, logiciels mis à jour longtemps), Fairphone estime qu'un utilisateur peut réduire de **50% son empreinte environnementale liée au smartphone** par rapport à un cycle de renouvellement classique sur la même période [20, 21]. C'est un exemple concret où un design orienté long terme sert à la fois la **soutenabilité** et la **souveraineté** : un client Fairphone n'a pas besoin de racheter un appareil propriétaire non-européen tous les 2-3 ans, il conserve plus longtemps un appareil maîtrisé, dont les

pièces détachées sont disponibles et dont les données restent sous son contrôle plus longtemps.

À l'échelle d'une entreprise ou d'une administration, comment opérationnaliser l'allongement de la durée de vie ? Plusieurs **leviers** existent :

- **Politiques d'achat exigeantes** : intégrer des critères de durabilité, réparabilité et évolutivité dans les appels d'offres. Par exemple, exiger des garanties de 5 ans minimum, la disponibilité de pièces détachées pendant 7 ans, ou un indice de réparabilité élevé. Depuis 2021, la France impose un indice de réparabilité affiché sur les produits électroniques, ce qui facilite de tels choix. Certaines organisations ont même commencé à privilégier les fournisseurs offrant des modèles modulaires ou reconditionnables.

- **Développement du reconditionné** : au lieu d'acheter systématiquement du neuf, envisager le recours à des équipements reconditionnés de qualité. Le marché du reconditionné est en plein essor en Europe (smartphones, PC, serveurs d'occasion remis à neuf). Soutenir cette filière, c'est réduire la demande de nouveaux appareils et encourager une économie plus circulaire. De plus, cela développe des compétences locales (entreprises de reconditionnement, ateliers de réparation), participant à une **autonomie technologique locale**.

- **Maintenance et réparation** : investir dans la maintenance préventive et les formations pour réparer plutôt que jeter. De nombreuses DSI ont intérêt à prolonger leurs serveurs au-delà du cycle standard de 3-5 ans, surtout si les besoins de performance n'augmentent pas drastiquement. Sur les postes de travail, un programme de remplacement de composants (batteries, extension de RAM, SSD) peut redonner une seconde vie à un PC pour quelques années de plus, à coût modique.

- **Sobriété fonctionnelle** : *simplifier les logiciels* peut prolonger la vie du matériel. En effet, si l'on utilise des logiciels toujours plus gourmands, on est contraint de renouveler le matériel plus fréquemment. À l'inverse, un poste de travail équipé d'un système d'exploitation léger et d'applications sobres peut rester fluide plus longtemps. Certains organismes ont expérimenté l'installation de distributions Linux légères sur des PC qui ne supportent pas une nouvelle version d'OS (Windows 11, par exemple) pour éviter de les remplacer : cela répond aux besoins courants sans investissement matériel.

- **Réemploi interne** : organiser la rotation ou la seconde vie des équipements en interne. Par exemple, un ordinateur haut de gamme de développeur peut, après 4 ans, être réaffecté à un usage moins exigeant (bureautique simple) au lieu d'être mis au rebut. De même, les smartphones professionnels

restitués peuvent être remis à neuf et redistribués à des utilisateurs aux besoins basiques ou à des associations.

Les bénéfices stratégiques sont directs : *chaque année d'usage gagnée est une extraction évitée*. **Chaque équipement conservé est une dépendance différée**, un répit dans la consommation de métaux critiques. Sur le plan géopolitique, si l'Europe arrivait par exemple à prolonger de 30% en moyenne la durée de ses équipements numériques, l'effet serait équivalent à "supprimer" des millions de terminaux du flux d'importation chaque année, allégeant d'autant sa vulnérabilité aux pénuries. De plus, en stimulant le marché de la réparation et du reconditionnement, on **renforce un tissu industriel local** (PME du numérique responsable) et on crée des emplois non délocalisables.

Notons que le prolongement de la durée de vie rejoint aussi la dynamique réglementaire européenne : le **droit à la réparation** des équipements électroniques est de plus en plus promu (obligation de disponibilité des pièces, indices de réparabilité, projet d'indice de durabilité). La France a d'ores et déjà introduit l'indice de réparabilité, et un indice de durabilité est en préparation. Ces évolutions normatives soutiennent l'idée qu'un équipement doit pouvoir durer 5, 7, 10 ans, et plus seulement 2 ou 3 ans.

En somme, **"le meilleur déchet est celui qu'on ne produit pas"** : en évitant de transformer trop vite nos équipements en déchets électroniques, on évite aussi de devoir recourir trop vite à de nouvelles ressources. C'est un cercle vertueux qui renforce notre **résilience industrielle** autant qu'il sert l'environnement. À l'évidence, dans la compétition mondiale sur les ressources, l'Europe aura du mal à rivaliser sur l'extraction minière ; en revanche, elle peut innover dans la *sobriété matérielle* et devenir un champion de l'allongement de la durée d'usage. Cela contribuerait à une souveraineté "par le bas" : moins dépendre des flux de matières premières contrôlés par d'autres.

Écoconception et simplification des architectures

La **frugalité logicielle** est un autre pilier du numérique responsable pouvant soutenir la souveraineté. L'**écoconception des services numériques** vise à développer des applications plus sobres en ressources (CPU, mémoire, bande passante, stockage), sans compromis sur les besoins métiers essentiels. De nombreuses études et retours d'expérience montrent qu'il est souvent possible de réduire considérablement la consommation d'une application *à fonctionnalités constantes*. En optimisant le code, en éliminant les traitements redondants, en allégeant l'interface utilisateur, on obtient des logiciels plus légers et plus rapides, ce qui profite autant à l'utilisateur final qu'à l'infrastructure. Si on va un cran plus loin, en repensant les fonctionnalités et en se recentrant sur les besoins réels de l'utilisateur, les gains sont alors considérables.

En France, un référentiel public a été élaboré pour guider cette démarche : le **Référentiel Général d'Écoconception de Services Numériques (RGESN)**, publié par

la DINUM (Direction interministérielle du numérique). La version 2024 de ce référentiel comporte **78 critères d'écoconception répartis en 9 catégories** (stratégie, spécifications, architecture, UX/UI, contenu, frontend, backend, hébergement, algorithmie)[22]. Suivre ces bonnes pratiques permet de réaliser des gains significatifs. Par exemple, l'optimisation des images et du code d'un site web peut diviser par 2 ou 3 son poids et donc la donnée à transférer, sans changer le contenu. À plus forte raison, repenser une application métier lourde peut mener à des réductions d'empreinte de l'ordre de 30%, 50% voire davantage, comme le montrent des projets pilotes menés par diverses entreprises françaises et l'Association GreenIT (qui recense des *bonnes pratiques d'écoconception* éprouvées dans le RWEB)[23].

Quel rapport avec la souveraineté ? Un logiciel plus efficient offre en réalité plusieurs avantages stratégiques :

- D'abord, il peut tourner sur une infrastructure plus modeste. **Une application plus légère nécessite moins de puissance de calcul, moins de bande passante et moins de stockage**. Elle pourra potentiellement fonctionner sur des serveurs de taille inférieure, ou sur des machines plus anciennes, ou être hébergée localement plutôt que sur un cloud lointain. Ainsi, cela **élargit les options d'hébergement** : là où une application lourde force à aller chez un hyperscaler pour bénéficier de ses énormes ressources, une application optimisée pourrait, elle, tourner chez un hébergeur local ou sur un cloud souverain plus modeste. En rendant les services *moins dépendants de l'échelle*, on redonne de la **flexibilité** dans le choix des fournisseurs.

- Ensuite, un logiciel économe est souvent un logiciel **plus simple et mieux maîtrisé**. Le processus d'écoconception pousse à supprimer les fonctionnalités non essentielles, à rationaliser le code et l'architecture. In fine, le produit est moins complexe, donc plus facile à auditer et à maintenir. Cela rejoint le point précédent sur la complexité logicielle : *simplifier, c'est regagner de la souveraineté technique*. Une architecture épurée implique moins d'interconnexions obscures, moins d'APIs tierces, donc **moins de dépendances** à des modules externes.

- Par ailleurs, en étant moins gourmand, un service écoconçu peut rester utilisable même dans des conditions dégradées et plus longtemps sur un équipement existant, rejoignant notre objectif d'allongement de vie. Par exemple, une appli mobile optimisée pourra fonctionner sur un smartphone de 5 ans d'âge sans problème, alors qu'une appli mal optimisée rendrait l'appareil trop lent au bout de 2 ans, forçant l'utilisateur à le changer. Donc l'écoconception logicielle **complète la sobriété matérielle**.

- Enfin, la démarche d'écoconception s'accompagne généralement d'indicateurs de suivi (mesure de la consommation, tests de performance, etc.). Cette *culture de la mesure* peut aussi servir la sécurité et la qualité en général, renforçant la fiabilité du SI.

Pour faciliter l'adoption, des outils émergent : citons par exemple le site *EcoIndex* (qui note l'impact environnemental des pages web), ou les référentiels cités plus haut [24]. L'ANSSI elle-même encourage l'usage de logiciels épurés, notant qu'ils sont souvent plus sûrs car comportant moins de surface de vulnérabilité.

En un mot, **"Small is beautiful"** dans le numérique souverain : un logiciel frugal est un logiciel sous contrôle. À l'échelle de l'État, promouvoir l'écoconception (via des marchés publics adaptés, des incubateurs de services publics numériques responsables, etc.) pourrait permettre de développer une filière d'excellence française/ européenne en logiciels sobres. On pourrait imaginer un label pour les logiciels répondant à des critères de performance énergétique et de transparence, label soutenu par les pouvoirs publics et recherché par les organisations voulant allier responsabilité et indépendance.

Slow Tech : ralentir pour reprendre le contrôle

La démarche **Slow Tech** s'inspire du mouvement "Slow" appliqué au numérique : de même qu'on parle de Slow Food en opposition à la restauration rapide, la Slow Tech prône un **numérique plus réfléchi, maîtrisé et durable**, plutôt que la course effrénée aux dernières technologies. Concrètement, adopter la Slow Tech signifie *ralentir* le rythme d'adoption des nouveautés pour **privilégier la pertinence, la robustesse et la maîtrise** sur l'excitation de la nouveauté permanente.

Dans un contexte de souveraineté, la Slow Tech invite à plusieurs **réflexes salutaires** :

- **Questionner la nécessité** de chaque nouvel outil ou gadget : a-t-on vraiment besoin de ce nouvel outil collaboratif à la mode, de ce nouvel objet connecté, de cette nouvelle version majeure du logiciel, immédiatement ? Ne peut-on pas faire durer l'existant ou se contenter d'une version plus simple ? Une alternative non numérique n'est-elle pas possible ? Cette réflexion permet d'éviter l'*innovation pour l'innovation*, qui est parfois plus dictée par le marketing ou l'effet de mode que par un réel besoin métier.

- **Refuser l'innovation non maîtrisée** : ne pas céder aux sirènes de telle plateforme « gratuite » sans en évaluer les contreparties, de telle technologie propriétaire sans alternative, etc. Par exemple, de nombreuses écoles ou administrations en Europe ont récemment dû reconsidérer l'usage de suites bureautiques cloud américaines (comme Microsoft 365) suite aux alertes sur le Cloud Act et le non-respect du RGPD [25]. Plutôt que de foncer

sur ces solutions pour leur confort apparent, certaines ont fait le choix raisonné de **solutions alternatives souveraines** (par ex. migration vers *Nextcloud* couplé à OnlyOffice, ou adoption de suites collaboratives françaises)[25]. Ce ralentissement volontaire – le temps de trouver une alternative conforme et maîtrisée – s'est révélé payant en termes de souveraineté des données.

- **Privilégier les solutions sobres, robustes et pérennes** : la Slow Tech valorise la **Low Tech** (voir section suivante) et n'adopte la High Tech que lorsque c'est nécessaire. Par exemple, pour un besoin interne de messagerie instantanée, une organisation Slow Tech pourrait choisir une solution open source éprouvée (comme XMPP ou Matrix) plutôt qu'un énième nouvel outil à la mode, certes bourré de fonctionnalités mais propriétaire et dont la pérennité n'est pas garantie.
- **Intégrer systématiquement l'analyse de dépendances** avant d'engager un projet numérique : *si j'adopte cette technologie, quelles nouvelles dépendances vais-je créer (techniques, contractuelles, juridiques) et sont-elles acceptables ?* Ce questionnement, souvent absent dans l'urgence de la transformation digitale, est central en Slow Tech.

En pratiquant la Slow Tech, on redécouvre le **temps de l'arbitrage**. Ralentir n'est pas renoncer à l'innovation, c'est *reprendre la main sur son calendrier*. C'est éviter de se précipiter dans l'adoption d'une technologie que l'on ne saurait plus tard maîtriser ou substituer. **"Ralentir, c'est arbitrer"** : c'est choisir d'investir d'abord dans ce qui compte vraiment (sécurité, soutenabilité, souveraineté), quitte à ne pas avoir la toute dernière version clinquante du logiciel X dès sa sortie.

En un mot, la Slow Tech est un **outil de discernement souverain** dans la frénésie numérique actuelle. Alors que la pression concurrentielle pousse à adopter massivement le cloud et l'IA sans analyse stratégique approfondie, la Slow Tech propose de *retrouver le sens des priorités*. Et souvent, ces priorités nous ramènent à des choix plus sobres et plus locaux, ce qui est exactement l'objectif recherché.

Low Tech numérique : faire mieux avec moins

Parallèlement à l'approche Slow Tech (qui est temporelle et stratégique), l'approche **Low Tech** appliquée au numérique se concentre sur *la nature même des solutions techniques* que nous utilisons. Par **Low Tech numérique**, on n'entend pas un retour à la bougie ou l'abandon d'Internet 😉. Il s'agit de promouvoir des technologies **simples, robustes, réparables, compréhensibles et adaptées au besoin réel**. C'est l'opposé de la fuite en avant vers le toujours plus sophistiqué, toujours plus puissant, sans considération d'utilité.

Concrètement, une **démarche Low Tech numérique** cherche à :

- Concevoir des **architectures sobres** : par exemple, un site web statique plutôt qu'une usine à gaz dynamique pour une simple page d'information. Ou bien une application de collecte de données qui stocke localement puis synchronise quand nécessaire, plutôt qu'un streaming permanent des données vers le cloud.

- Utiliser des **outils interopérables et standards** : la low tech valorise ce qui est largement diffusé et maîtrisé. Par exemple, privilégier des formats ouverts et durables (CSV, TXT, etc.) plutôt que des formats propriétaires complexes. S'appuyer sur des protocoles éprouvés (SMTP pour le mail, RSS pour diffuser du contenu) plutôt que de réinventer la roue via des plateformes fermées.

- Choisir des **technologies éprouvées** : ce qui est "nouveau" n'est pas forcément mieux. La low tech n'a pas honte d'utiliser une techno des années 90 si elle fonctionne de manière efficace et maîtrisée. Par exemple, en cybersécurité, les systèmes "AirGap" (non connectés) ou le bon vieux SMS pour de l'authentification double facteur peuvent être préférés à des solutions plus high-tech mais plus fragiles (applis push sophistiquées).

- Favoriser des **systèmes maintenables localement** : un système low tech doit pouvoir être compris et maintenu par des équipes locales, sans dépendance à une armée d'experts extérieurs. Cela signifie éviter les *boîtes noires* ésotériques. Un bon test est : « en cas de crise, mes ingénieurs/techniciens seraient-ils capables de réparer ou remplacer ce système eux-mêmes ? ».

Adopter la low tech numérique, c'est souvent **limiter la dépendance aux composants exotiques et aux infrastructures surdimensionnées**. Par exemple, une collectivité locale qui souhaite mettre en place un portail citoyen pourrait choisir une solution open source simple, hébergée sur un serveur mutualisé local, plutôt que d'opter d'emblée pour un package "smart city" clef en main très sophistiqué vendu par un grand groupe. Certes, le second a plus de fonctionnalités, mais le premier sera bien plus autonome, compréhensible (et probablement suffisant pour le besoin réel).

En termes de souveraineté, la Low Tech apporte plusieurs bénéfices :

- **Autonomie opérationnelle accrue** : un système simple est plus facile à administrer par soi-même. On a moins besoin de consultants externes ou de support éditeur coûteux. Par exemple, une école qui utilise des PC sous Linux léger et des suites bureautiques open source n'est pas prisonnière des licences d'un grand éditeur et peut adapter elle-même son environnement.

- **Réduction de la complexité = réduction des failles** : moins de couches = moins de bugs potentiels = surface d'attaque réduite. Un **système simple est plus maîtrisable** qu'un système sophistiqué et opaque. Les experts en cybersécurité prônent souvent de "revenir aux bases" et de limiter les dépendances, ce qui rejoint l'esprit low tech.

- **Résilience renforcée** : en cas de crise (cyberattaque, panne internet, etc.), des solutions low tech peuvent continuer de fonctionner là où des solutions high tech complexes échouent. Par exemple, si un service cloud tombe, une solution locale simple peut prendre le relais temporairement. Ou si l'électricité est rationnée, un service optimisé pourra peut-être tourner sur un petit serveur basse conso alimenté par UPS, alors qu'une grosse infra high-tech ne tiendra pas.

- **Économies financières** : souvent, la low tech coûte moins cher (à l'achat et à l'usage). Ces économies peuvent être réinvesties ailleurs (par exemple dans la formation du personnel, qui renforce là aussi la souveraineté par les compétences).

La Low Tech n'est pas incompatible avec la modernité, au contraire elle peut être innovante. C'est plutôt un **changement de paradigme** : *faire mieux avec moins*. Un bel exemple est celui du **Minitel 2.0** : certains acteurs explorent l'idée de terminaux simples (faible puissance, juste l'essentiel) connectés à un réseau local pour des usages spécifiques, un peu à la manière du Minitel en son temps. L'idée n'est pas de revenir au Minitel en tant que tel, mais de s'inspirer de sa sobriété et de son intégration territoriale (fabrication française, réseau national) pour concevoir des solutions actuelles plus souveraines. De manière générale, la Low Tech encourage à **penser différemment le progrès** : au lieu de toujours ajouter des couches technologiques, se demander si l'on ne peut pas atteindre l'objectif par une solution plus légère, plus durable.

Un exemple concret de choix low tech : **remplacer un site web par un simple système d'alerte SMS ou email**. Frédéric Bordage (expert Green IT) cite ainsi le cas de certains projets où, au lieu de développer une énième plateforme web sophistiquée pour informer des usagers, il a recommandé d'envoyer de simples mails ou SMS d'alerte, ce qui *se substituait presque totalement au besoin du site web* [26]. Solution low tech par excellence : utilisation d'une techno simple (mail/SMS) fonctionnant sur n'importe quel téléphone, très peu coûteuse et ne nécessitant quasiment aucune maintenance, comparé à un site web complexe. Ce genre de réflexion devrait devenir un réflexe : *la solution la plus simple possible pour répondre au besoin, et pas au-delà*.

En adoptant largement la low tech numérique dans les services publics, les PME, etc., l'Europe pourrait réduire son appétit pour les technologies importées haut de gamme, et valoriser son ingéniosité pour des solutions sobres. C'est un choix de société autant

que technique : **privilégier l'utile au flashy, l'endogène à l'exogène**. Et en période de tension sur les ressources, c'est peut-être la seule voie soutenable à long terme (rappelons la question posée dans un article GreenIT : préfère-t-on continuer à agrandir indéfiniment les écrans TV dans nos salons, ou garder les dernières réserves de métaux pour les outils numériques vraiment critiques pour l'avenir ?[26]). La Low Tech nous pose cette question de fond, et y répondre est un acte de souveraineté.

Désescalade technologique : simplifier avant de substituer

Un concept lié à la Slow Tech et à la Low Tech est celui de **désescalade technologique**. Il part du constat qu'une **substitution frontale** des écosystèmes numériques (par exemple remplacer du jour au lendemain toutes les solutions américaines par des alternatives européennes) est souvent irréaliste, voire impossible à court terme. En revanche, on peut emprunter une trajectoire **progressive** : *diminuer d'abord la dépendance*, pour rendre une éventuelle substitution plus facile ensuite. En d'autres termes : **simplifier avant de remplacer**.

La désescalade technologique consiste à identifier tout ce qui, dans notre SI ou notre stratégie numérique, relève du "surplus" ou du "non essentiel" importé, et à le réduire, afin de **rendre l'écosystème plus léger, plus modulaire, donc plus facile à migrer le moment venu**. Cela recoupe plusieurs actions déjà évoquées :

- **Supprimer les usages à faible valeur ajoutée** : par exemple, une entreprise peut décider d'abandonner certains outils analytiques ou marketing secondaires qui la lient à des plateformes tierces sans bénéfice majeur. Moins d'outils = moins de dépendances.
- **Rationaliser les couches logicielles** : audit des applications redondantes, consolidation sur moins d'outils mais mieux maîtrisés, suppression des services techniques obscurs dont on pourrait se passer. Par exemple, si une DSI utilise 5 systèmes de gestion de contenu différents (suite à des héritages divers), en passer 4 sur 5 sur un seul standard open source rendra l'ensemble plus homogène et plus facile à contrôler.
- **Limiter l'usage des services avancés non essentiels** : par exemple, éviter de s'enfermer dans des services cloud propriétaires très spécifiques (ex : bases de données ultra-propriétaires, services d'IA hyper spécialisés) pour des usages qui pourraient être couverts de manière plus standard. Chaque service exotique adopté est une couche de dépendance en plus.
- **Réinternaliser certaines compétences clés** : ceci est crucial. La désescalade inclut l'idée de reconstruire en interne des aptitudes qu'on avait complètement externalisées. Par exemple, si tout le développement logiciel

a été confié à un prestataire externe, essayer de recruter progressivement des développeurs en interne pour monter en compétence, même si l'externalisation continue en parallèle. Idem pour l'hébergement : peut-être commencer par rapatrier un petit pourcentage des applications sur une infrastructure maison, pour réapprendre à gérer un data center, tout en gardant le gros sur le cloud public dans un premier temps. L'idée est de *recréer une culture technique interne*, sans attendre d'être capable de tout faire, mais en amorçant le mouvement.

Cette démarche de simplification/désescalade apporte des bénéfices **immédiats** : *réduction de coûts*, *réduction de complexité*, *réduction de la surface d'attaque*, etc. Elle redonne aussi de la **marge de manœuvre**. Une organisation allégée peut plus facilement pivoter ou intégrer de nouvelles briques souveraines. Par analogie, c'est plus facile de manœuvrer un bateau léger qu'un paquebot gigantesque. Si on rêve de sortir des eaux contrôlées par un fournisseur, mieux vaut d'abord diminuer son tirant d'eau numérique.

Un scénario concret : imaginons un ministère qui utilise massivement une suite bureautique/cloud non souveraine pour tous ses agents. Plutôt que d'annoncer abruptement « on bascule tout sur une solution française l'an prochain » (au risque de l'échec si la solution alternative n'est pas mûre ou les agents pas formés), une désescalade progressive serait de commencer par segmenter les usages : maintenir la suite non souveraine pour les fonctions où aucune alternative n'est prête (par ex macros Excel complexes), mais *en parallèle* déployer progressivement une suite alternative (LaSuite + stockage Nextcloud) pour les usages plus basiques, et former les utilisateurs. On pourrait décider que, d'ici 2 ans, 50% des documents internes simples doivent être produits avec l'outil souverain. Cela réduit la dépendance graduellement. Au bout de 2 ans, fort de l'expérience, on pourra pousser plus loin et peut-être viser 80%, etc., jusqu'à ce que la dépendance résiduelle soit marginale et qu'un débranchement complet devienne envisageable. Cette stratégie évite les écueils d'une migration brusque (rejet utilisateur, bugs non gérés, etc.) en **faisant de la souveraineté un chemin progressif** plutôt qu'un basculement brutal.

La désescalade technologique est en quelque sorte la mise en pratique orchestrée des principes de sobriété, slow et low tech. C'est un **plan d'action** pour sortir du piège sans sauter dans le vide. Elle pourrait même être encouragée par des politiques publiques : par exemple, imaginer un programme d'accompagnement des entreprises pour auditer leur SI et **identifier 10% de dépendances technologiques faciles à éliminer** la première année, puis 10% supplémentaires l'année suivante, etc. Cumulativement, en quelques années, on aurait réduit la voilure et créé un terrain bien plus favorable à l'adoption des solutions européennes en cours de développement.

En définitive, la désescalade rappelle que la souveraineté numérique n'est pas un état binaire (dépendant vs souverain) mais un continuum. Chaque pas pour *réduire* la dépendance est bon à prendre, même si on ne peut pas la supprimer totalement du jour au lendemain.

Une IA frugale et maîtrisée

Enfin, abordons le cas particulier de l'**IA frugale**. Comme discuté dans les constats, l'IA est un domaine où l'emballement peut vite nous piéger dans de nouvelles dépendances. Adopter une approche **frugale et sélective de l'intelligence artificielle** est donc crucial pour aligner le déploiement de l'IA avec nos objectifs de souveraineté.

Que signifie *IA frugale* en pratique ? C'est d'abord **réserver l'IA aux cas d'usage à forte valeur ajoutée**, qui répond à un vrai besoin et où aucune autre solution plus simple ne serait aussi efficace. Plutôt que de vouloir mettre des IA partout (par effet de mode), on cible les domaines où l'IA apporte un vrai plus et où cette plus-value justifie les ressources mobilisées et les risques induits. Par exemple, utiliser un modèle de vision par ordinateur pour détecter des anomalies médicales invisibles à l'œil humain, oui. Utiliser un chatbot GPT pour répondre à des questions simples auxquelles un bon vieux moteur de recherche ou une FAQ suffirait, non.

Ensuite, **privilégier des modèles spécialisés et de taille raisonnable plutôt que des modèles généralistes géants**. Les "petites IA" entraînées sur des périmètres ciblés peuvent souvent suffire et présentent l'avantage d'être *auto-hébergeables*. On voit émerger par exemple des modèles open source de traitement de texte ou d'image beaucoup plus légers que GPT-4, qui peuvent tourner sur un serveur standard. C'est moins puissant qu'un modèle géant, mais largement assez pour des besoins spécifiques, et surtout c'est **maîtrisable en interne**. De plus, un modèle plus petit est plus facile à auditer, à expliquer (on peut parfois inspecter ses règles décisionnelles), ce qui est un plus pour la conformité réglementaire future.

Une autre facette de l'IA frugale est de **réduire les volumes de données traitées**. Là encore, ne pas tout envoyer dans la moulinette IA "au cas où". Par exemple, pour entraîner un modèle, utiliser des datasets de taille raisonnable et bien calibrés plutôt que d'accumuler des pétaoctets de données brutes. Cela rejoint l'idée de dark data : inutile d'entraîner une IA sur des données dont 50% sont du bruit ou non pertinentes. Mieux vaut de *bonnes petites données* que de *grosses mauvaises données*. En exploitation, ça signifie aussi ne pas tout analyser en temps réel si ce n'est pas nécessaire (on peut imaginer des IA qui s'activent ponctuellement plutôt que 24/7 sur le flux complet).

Enfin, **favoriser des infrastructures maîtrisées pour faire tourner l'IA**. Si une organisation a un vrai besoin d'IA, elle peut envisager d'investir dans du matériel dédié (serveurs GPU en propre, ou cloud souverain spécialisé) plutôt que d'utiliser sans réflexion les grands clouds publics d'IA. Certes, cela peut coûter plus cher ou être plus

complexe au départ, mais pour certains usages sensibles ça en vaut la peine. Par exemple, une collectivité traitant des données de santé pourrait opter pour une plateforme IA hébergée dans un cloud de confiance (certifié SecNumCloud en France) pour s'assurer que les données ne sortent pas du cadre juridique national.

Techniquement, des **solutions existent pour "alléger" l'IA** : on parle de techniques de *distillation de modèles* (comme DistilBERT chez Hugging Face qui divise la taille d'un modèle BERT par deux tout en conservant l'essentiel de ses capacités [27]), de *quantification* (réduire la précision des calculs pour accélérer et consommer moins), ou d'architectures *fédérées* (entraîner un modèle de manière décentralisée sur les équipements locaux pour éviter de tout remonter dans un data center central). Ces innovations permettent d'envisager une IA plus locale et moins énergivore. D'ailleurs, l'**AFNOR** a publié en 2023 un référentiel de bonnes pratiques pour une IA frugale [28], signe que le sujet est pris au sérieux en France. Ce référentiel encourage la mesure de l'impact environnemental des IA et la mise en place d'objectifs de réduction. L'équipe de Green IT a sorti la première version de son référentiel IA début 2026. Au niveau européen, l'AI Act pourrait aussi inciter indirectement à la frugalité en imposant des contraintes (par exemple transparence sur l'empreinte carbone des grands modèles, ce qui pousserait à la réduire pour des questions d'image et de conformité).

En cultivant une **IA maîtrisée**, on limite plusieurs risques de dépendance : *géopolitique* (on peut s'appuyer plus sur des solutions locales ou open source que sur les big tech), *énergétique* (on évite l'explosion de la consommation électrique/eau évoquée), *juridique* (les données restent plus souvent dans notre giron, et les modèles alignés sur nos valeurs). En outre, on **renforce la capacité d'audit et de sécurisation** des IA déployées, condition indispensable pour les utiliser en contexte critique (défense, santé, justice…).

En résumé, il faut substituer à l'actuel slogan implicite "There's an AI for that" une approche plus raisonnée : "Y a-t-il *vraiment* besoin d'une IA pour ça ? Et si oui, laquelle et dans quelles conditions ?". Cette question doit être intégrée dès la conception des projets. Une IA frugale bien ciblée deviendra un allié, là où une débauche d'IA mal maîtrisée nous aliénerait.

Conclusion – De la sobriété à la souveraineté

La souveraineté numérique, on l'aura compris, ne peut se résumer à une politique industrielle de substitution ou à des déclarations de principe. Ce n'est pas uniquement en construisant des data centers nationaux ou en subventionnant des champions technologiques européens que l'on regagnera la maîtrise. Certes, ces initiatives sont importantes, mais elles doivent s'inscrire dans une **politique de maîtrise globale** de notre destin numérique.

Le **numérique responsable**, enrichi des principes de **Slow Tech** et de **Low Tech**, offre précisément cette trajectoire de maîtrise. Il nous invite à *réduire les volumes*, *prolonger la durée de vie des équipements*, *simplifier les architectures*, *arbitrer les usages*, *privilégier la robustesse sur l'accélération perpétuelle*. En adoptant ces principes, on touche simultanément aux volets stratégique, économique, juridique et environnemental de la souveraineté :

- Stratégiquement, moins dépendre des ressources externes (qu'il s'agisse de cloud, de composants, d'énergie) signifie **renforcer sa résilience** face aux aléas et pressions extérieures.
- Économiquement, consommer moins et localement revient à **réorienter la valeur** : plutôt que d'alimenter un exode de capitaux technologiques (les fameux 264 milliards annuels vers l'étranger[7]), on investit dans des filières internes (réparation, reconditionnement, logiciels locaux). C'est un choix de balance commerciale autant que de modèle de développement.
- Juridiquement, la sobriété numérique réduit l'exposition aux cadres extraterritoriaux (moins de données sensibles dans des clouds soumis à des lois étrangères, moins d'usage de solutions non conformes au RGPD, etc.). C'est **moins de faiblesses exploitables**.
- Environnementalement, c'est évident : sobriété rime avec moindre impact. Et un numérique durable est un numérique qui pourra *continuer d'exister demain*, alors qu'un numérique hors-sol écologiquement est condamné à terme (par épuisement des ressources ou rejet sociétal).

Dans un univers technologique mondialisé, interconnecté, construit sur des chaînes d'approvisionnement globales, il serait illusoire de prétendre atteindre une **souveraineté numérique absolue**. Aucun pays, aucune région ne peut espérer maîtriser de A à Z l'ensemble des composants, ressources, technologies et infrastructures numériques contemporaines. La question devient alors : *quel niveau de souveraineté relative voulons-nous atteindre, et dans quels domaines ?* Autrement dit, **quelles dépendances sommes-nous prêts à accepter, et lesquelles devons-nous impérativement réduire** ? Il s'agit de hiérarchiser : protéger en priorité nos fonctions critiques, sécuriser nos actifs les plus précieux, garantir une capacité d'action en cas de crise.

Cette démarche est éminemment politique et stratégique. Elle nécessite d'**assumer des choix** : par exemple, peut-être accepter d'utiliser des composants asiatiques grand public (non critiques), mais refuser de dépendre d'un cloud non-européen pour des données de santé. Ou encore, consentir à ne pas avoir le dernier iPhone à la mode si cela signifie relancer une filière de téléphone européen plus basique mais souverain. Ce sont des arbitrages qui doivent être éclairés par le débat public.

Dans cette perspective, on voit que le numérique responsable n'est pas un "supplément d'âme" éthique ou un simple outil de RSE pour les entreprises. Il est un **véritable instrument opérationnel** pour ajuster le curseur de dépendance, renforcer la résilience et restaurer des marges de manœuvre. Il donne corps à une *souveraineté lucide*, c'est-à-dire une souveraineté consciente de ses interdépendances mais décidée à les encadrer et les limiter au nécessaire.

En conclusion, **moins de dépendance commence par moins de dépendance aux volumes et aux excès**. **Moins de complexité, c'est plus d'autonomie.** Et finalement, **une souveraineté lucide vaut mieux qu'une souveraineté proclamée** : plutôt que de clamer "nous allons tout faire nous-mêmes", il vaut mieux agir concrètement, pas à pas, pour **réduire l'emprise subie** et regagner la maîtrise sur l'essentiel. C'est le chemin que propose le numérique responsable.

Nous terminerons par une série de recommandations opérationnelles à destination des différents acteurs – institutions publiques, organisations/entreprises, et citoyens – afin de traduire ces orientations en actions concrètes.

Nos recommandations pour une souveraineté numérique lucide

Pour les institutions (État, collectivités, régulateurs) :

1. **Fixer un seuil de "dépendance acceptable" et le mesurer** – Par exemple, réduire de X% en 5 ans la part des dépenses numériques publiques stratégiques captées par des solutions non souveraines. Cet indicateur pilotera les actions (soutien aux offres locales, clauses de réversibilité obligatoires dans les marchés, etc.) pour *restaurer la marge de manœuvre stratégique* de la France et de l'Europe.

2. **Allonger la durée de vie du parc IT public** – Intégrer des objectifs précis : exiger au moins 5 ans d'usage pour les smartphones des agents, 7 ans pour les PC, etc. Soutenir les filières de reconditionnement via les marchés publics (inclure du matériel reconditionné). Chaque année de vie gagnée réduit la dépendance aux métaux critiques et aux importations d'équipements.

3. **Créer une filière d'excellence en écoconception, slow tech et low tech** – Par des financements, des labels, des programmes de recherche. Il s'agit de

structurer un écosystème réunissant startups, PME, laboratoires autour du **numérique frugal**. L'objectif : que la France/Europe devienne une référence en solutions numériques sobres et souveraines (services numériques écoconçus, matériels modulaires, etc.). Cela passe aussi par la formation (développer l'intégration de ces notions dans les cursus IT).

4. **Orienter les financements publics vers les IA frugales et maîtrisées** – Conditionner les subventions et appels à projets IA à des critères de frugalité (modèles open source, faibles besoins, cas d'usage à impact positif et maîtrisé). Créer un cloud public de calcul haute performance *souverain* dédié à l'entraînement de modèles IA d'intérêt général, pour offrir une alternative aux clouds privés, tout en imposant des règles éthiques et environnementales.

5. **Encourager la désescalade technologique dans les administrations** – Auditer les SI publics pour identifier les dépendances excessives. L'État pourrait émettre une circulaire demandant à chaque ministère de présenter un plan de simplification de son patrimoine applicatif, avant de solliciter toute nouvelle solution étrangère. De plus, renforcer les effectifs internes DSI, cyber, data… pour regagner en compétences clés (réinternalisation progressive des savoir-faire techniques).

6. **Maintenir les versions non-numériques des services essentiels** – Pour l'ensemble des services essentiels fournis par l'État, s'assurer qu'une version non numérique est maintenue en condition de fonctionnement. Ceci permet de freiner le recours au tout numérique et de permettre de continuer à fonctionner en cas de rupture de continuité de service

7. **Soutenir des projets de câbles alternatifs** (e.g. liaison directe Europe–Amérique du Nord indépendante), participer à des consortiums de câbles reliant Afrique/Europe (diversification des routes). Développer une filière de CDNs ou edge clouds européens. Intensifier les investissements publics (via plans France/UE numériques) pour héberger des data centers souverains en Points de Peering stratégiques.

Pour les organisations et entreprises :

1. **Mesurer et réduire la part du numérique "non souverain" dans l'activité** – Par exemple, cartographier les fournisseurs et outils critiques et évaluer leur niveau de maîtrise (localisation, contrat, alternatives). Sur cette base, définir une feuille de route pour diminuer la dépendance : migrer certaines charges vers des solutions européennes, exiger des clauses Cloud Act-free, diversifier les fournisseurs au lieu du tout-GAFAM, etc.

2. **Allonger la durée de vie des équipements professionnels** – Inciter les employés à garder leur matériel plus longtemps (via des incitations, un choix de terminaux durables). Mettre en place un système de reprise interne du matériel en fin de premier usage (reconditionnement pour d'autres besoins en interne ou via un partenaire). Adopter une politique "BYOD durable" sécurisée peut aussi être une voie (utiliser son appareil perso plus longtemps avec support IT, plutôt que renouveler un parc entier fréquemment).

3. **Privilégier les solutions souveraines et écoconçues** – Intégrer dans les schémas directeurs IT un principe de préférence pour : le logiciel libre, l'open source, les solutions locales. Expérimenter des outils alternatifs (suite bureautique Open Source, hébergement chez des acteurs cloud locaux certifiés). Même si ce n'est pas généralisé tout de suite, se familiariser en interne avec ces solutions crée un terrain propice pour l'avenir. Soutenir aussi, en tant qu'entreprise utilisatrice, les éditeurs européens vertueux en leur faisant confiance pour des projets pilotes.

4. **Former et sensibiliser à la "veille lucide"** – C'est un aspect souvent négligé : développer en interne une culture de la **Slow Tech**. Par des formations, communiquer aux équipes que l'innovation doit être alignée avec la stratégie et non suivie aveuglément. Valoriser les réussites de projets où on a su dire "non" à une techno inadaptée. Inclure dans les comités d'architecture une étape "A-t-on envisagé plus simple/alternatif ?". En cybersécurité, inclure la question des dépendances tierces dans l'analyse des risques.

5. **Organiser la désescalade technologique** – Lancer un programme interne de simplification du SI : par exemple, objectif de réduire de 20% le nombre d'applications d'ici 3 ans, par consolidation. En profiter pour éliminer les doublons et les "shadow IT" non maîtrisés. Instaurer des processus de fin de vie pour les outils obsolètes, au lieu de tout accumuler. Ce nettoyage permanent évite l'effet "passoire" et *prépare* les migrations futures en assainissant le terrain (simplifier avant de substituer, comme évoqué). Par ailleurs, sur l'IA, mettre en place un comité d'éthique & sobriété : valider les cas d'usage IA selon des critères de valeur ajoutée et d'empreinte, afin d'éviter la prolifération non contrôlée de projets IA coûteux et dépendants.

Pour les citoyens :

1. **Épurer son environnement numérique personnel** : Réduire le nombre d'équipements numériques utilisés au strict nécessaire. Par exemple, tout le monde n'a pas besoin d'une tablette *en plus* d'un smartphone et d'un ordinateur. Moins d'équipements signifie moins de ressources consommées et moins de dépendance aux fabricants mondiaux. De même, faire le tri dans

ses applications et services en ligne – désinstaller celles qui ne servent pas, limiter les sollicitations inutiles (notifications, cloud drive pléthorique…).

2. **Faire durer et donner une seconde vie aux appareils** : Au lieu de changer de smartphone tous les 2 ans par habitude, viser 4 ou 5 ans. Utiliser une coque, réparer l'écran cassé plutôt que remplacer l'appareil, changer la batterie en boutique (de plus en plus de modèles le permettent, encouragé par la loi). Pour les ordinateurs, envisager une extension de RAM ou passer à un disque SSD pour lui redonner un coup de jeune plutôt que le remplacer complètement. Et lorsqu'un équipement n'est plus adapté à ses besoins, le **revendre ou le donner** (économie de l'occasion, associations) plutôt que le laisser dormir dans un tiroir ou le jeter – cela réduit la pression sur la production de neufs.
3. **Choisir des solutions éthiques, respectueuses et locales dès que possible** : Par exemple, opter pour un fournisseur d'email européen respectueux de la vie privée au lieu d'un webmail gratuit intrusif. Utiliser un moteur de recherche éthique (comme Qwant) plutôt que de nourrir systématiquement les géants qui profilent les données. Préférer un smartphone durable (Fairphone ou équivalent) ou un téléphone reconditionné plutôt qu'un modèle dernier cri issu de pratiques discutables. De manière générale, **accepter de payer pour des services en échange de garanties** (respect des données, absence de publicité, hébergement local) – cela vaut bien souvent mieux que le "tout gratuit" qui se finance en exploitant nos données. Par exemple, un cloud photo payant chez un acteur français ou européen offrira plus de contrôle qu'un service gratuit illimité basé à l'étranger. Ayons en tête que "quand c'est gratuit, c'est nous le produit".
4. **S'informer et soutenir les initiatives de numérique responsable** : Un citoyen souverain est aussi un citoyen éclairé. Apprendre à utiliser des alternatives (Linux, LibreOffice, Firefox…), c'est se donner du choix et ne pas être enfermé dans un seul écosystème. Participer à l'économie circulaire du numérique (Repair Café, ateliers de sensibilisation avec la Fresque du Numérique ou Latitudes) aide à faire évoluer les mentalités. Soutenir par son vote et sa voix les politiques publiques qui vont dans le sens d'une économie numérique durable et souveraine (par ex. réglementations sur l'obsolescence programmée, protection des données) est également essentiel.

En adoptant ces comportements, les citoyens deviennent **acteurs** de la souveraineté numérique : leurs choix de consommation et d'usage envoient un signal au marché (si la demande pour le durable et local augmente, l'offre s'adaptera) et réduisent la pression sur les ressources globales. L'addition de millions de micro-décisions individuelles peut considérablement influencer l'orientation du système numérique dans son ensemble.

Conclusion

En conclusion de cette analyse, nous avons mis en évidence qu'**un numérique plus responsable – sobre, éthique, durable – peut être un formidable levier de souveraineté** pour la France et l'Europe. Loin d'être contradictoires, transition écologique du numérique et autonomie stratégique se renforcent mutuellement. En réduisant nos gaspillages numériques, en valorisant la qualité sur la quantité, en reprenant la maîtrise de nos choix technologiques, nous posons les bases d'un écosystème numérique plus résilient, plus respectueux et plus libre.

La route vers la souveraineté numérique est un chemin de long terme, qui demandera volonté politique, innovation industrielle et évolution culturelle. Mais chaque pas compte. Dès aujourd'hui, institutions, entreprises et citoyens peuvent s'engager sur cette voie en appliquant les principes et recommandations évoqués. Il en va non seulement de notre **indépendance technologique**, mais aussi de notre capacité à définir le numérique que nous voulons : un numérique au service du bien commun, aligné sur nos valeurs et nos intérêts, plutôt qu'un numérique subi.

Moins subir pour mieux choisir, telle pourrait être la devise de la souveraineté numérique responsable. Puissions-nous collectivement la mettre en pratique, afin que le numérique reste un outil d'émancipation et de progrès, et non une nouvelle forme de dépendance. Le défi est grand, mais l'enjeu est crucial : c'est une part de notre liberté moderne qui se joue, dans chaque octet, chaque clic et chaque ligne de code. À nous de la préserver.

Annexes

Sources

1- Wikipédia - Cloud Act

https://fr.wikipedia.org/wiki/CLOUD_Act

2- Cigref – La dépendance technologique aux softwares & cloud services américains : une estimation des conséquences économiques en Europe - Cigref

https://www.cigref.fr/la-dependance-technologique-aux-softwares-cloud-services-americains-une-estimation-des-consequences-economiques-en-europe

3- ANSSI – Recommandations de sécurité pour l'IA
https://www.ssi.gouv.fr/actualite/intelligence-artificielle-et-cybersecurite/

https://cyber.gouv.fr/enjeux-technologiques/intelligence-artificielle/

4- Cloud computing - statistics on the use by enterprises - Statistics Explained – Eurostat
https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises

5- European Chips Act | Shaping Europe's digital future

https://digital-strategy.ec.europa.eu/en/policies/european-chips-act

6- European Cloud Providers' Local Market Share Now Holds Steady at 15% | Synergy Research Group

7- Semiconductors: can European industry regain ground?

https://www.polytechnique-insights.com/en/columns/industry/semiconductors-can-europe-regain-ground/

https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15

8- Allons-nous manquer de métaux d'ici 20 ans ? - Green IT

https://www.greenit.fr/2025/10/06/allons-nous-manquer-de-metaux-dici-20-ans/

9- Numérique : quel impact environnemental ? - ADEME Infos

https://infos.ademe.fr/magazine-avril-2022/faits-et-chiffres/numerique-quel-impact-environnemental/

10- Energy demand from AI – Energy and AI – Analysis - IEA

https://www.iea.org/reports/energy-and-ai/energy-demand-from-ai#abstract

11- Data Centers and Water Consumption | Article | EESI

https://www.eesi.org/articles/view/data-centers-and-water-consumption

12- Drought-stricken Holland discovers Microsoft data center slurped ...

https://www.datacenterdynamics.com/en/news/drought-stricken-holland-discovers-microsoft-data-center-slurped-84m-liters-of-drinking-water-last-year/

13- L'utilisation de l'eau dans les centres de données reste cachée - DCD

https://www.datacenterdynamics.com/en/analysis/data-center-water-usage-remains-hidden/

14- ENISA – Threat Landscape for AI
https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges

15- Understanding the energy-AI nexus – Energy and AI – Analysis - IEA
https://www.iea.org/reports/energy-and-ai/understanding-the-energy-ai-nexus

16- Commission européenne – AI Act
https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

17- ARCEP & ADEME – Pour un numérique soutenable (2022)
https://www.arcep.fr/cartes-et-donnees/nos-publications-chiffrees/impact-environnemental/enquete-annuelle-pour-un-numerique-soutenable-edition-2022.html

18- Qu'est-ce que les Dark Data ? | IBM
https://www.splunk.com/fr_fr/form/the-state-of-dark-data.html

19- Dark Data: Concept, Challenges, and Ways to Manage It
https://atlan.com/dark-data-101/

20- ADEME – Impact environnemental du numérique en France (2023)
https://librairie.ademe.fr/changement-climatique/7880-evaluation-de-l-impact-environnemental-du-numerique-en-france.html

21- Voici le Fairphone 5, un smartphone équitable, réparable et avec 8 ans de support logiciel

https://www.journaldugeek.com/2023/08/30/voici-le-fairphone-5-un-smartphone-equitable-reperable-et-avec-8-ans-de-support-logiciel/

22- RGESN

https://ecoresponsable.numerique.gouv.fr/publications/referentiel-general-ecoconception/

23- référentiels et outils Green IT

https://greenit.eco/nos-outils-et-referentiels/

24- Ecoindex

https://www.ecoindex.fr/

25- Le conflit USA UE: Cloud et la souveraineté numérique

https://beenari.com/project/article-conflit-usa-eu-cloud-it/

26- Pour une low-tech numérique - Green IT

https://www.greenit.fr/2019/09/24/%EF%BB%BFpour-une-low-tech-numerique/

27- Hugging Face – Model Distillation
https://huggingface.co/docs/transformers/model_doc/distilbert

28- AFNOR - Référentiel IA frugale
https://www.boutique.afnor.org/fr-fr/norme/afnor-spec-2314/referentiel-general-pour-lia-frugale-mesurer-et-reduire-limpact-

29- France Stratégie - Rapport - La demande en eau - Prospective territorialisée à l'horizon 2050

https://www.strategie-plan.gouv.fr/publications/demande-eau-prospective-territorialisee-lhorizon-2050

30- Géopolitique du Numérique, Ophélie Coelho

https://editionsatelier.com/boutique/accueil/511-geopolitique-du-numerique--9782708295384.html

31- US export laws

https://uslawexplained.com/export