Sujet élaboré par une cellule pédagogique nationale

CONCOURS INTERNE ET 3ème CONCOURS D'ATTACHÉ TERRITORIAL

SESSION 2026

ÉPREUVE DE RAPPORT AVEC SOLUTIONS OPÉRATIONNELLES

ÉPREUVE D'ADMISSIBILITÉ :

CONCOURS INTERNE : Rédaction, à l'aide des éléments d'un dossier, d'un rapport faisant appel à l'esprit d'analyse et de synthèse du candidat, à son aptitude à concevoir et à mettre en place une application automatisée dans une collectivité territoriale.

3ème CONCOURS : Rédaction, à partir des éléments d'un dossier, d'un rapport faisant appel à l'esprit d'analyse et de synthèse du candidat, à son aptitude à concevoir et à mettre en place une application automatisée dans une collectivité territoriale.

Durée : 4 heures
Coefficient : 4

SPÉCIALITÉ : ANALYSTE

À LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET :

- Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom ou un nom fictif, ni initiales, ni votre numéro de convocation, ni le nom de votre collectivité employeur, de la commune où vous résidez ou du lieu de la salle d'examen où vous composez, ni nom de collectivité fictif non indiqué dans le sujet, ni signature ou paraphe.
- Sauf consignes particulières figurant dans le sujet, vous devez impérativement utiliser une seule et même couleur non effaçable pour écrire et/ou souligner. Seule l'encre noire ou l'encre bleue est autorisée. L'utilisation de plus d'une couleur, d'une couleur non autorisée, d'un surligneur pourra être considérée comme un signe distinctif.
- Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.
- Les feuilles de brouillon ne seront en aucun cas prises en compte.

Ce sujet comprend 35 pages.

Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué
S'il est incomplet, en avertir le surveillant

Vous êtes attaché territorial, chargé de mission « transformation numérique » auprès de la direction générale des services de la commune d'Admiville (150 000 habitants).

Dans un contexte de tensions géopolitiques et de compétition technologique accrue, la souveraineté numérique est devenue un enjeu majeur de compétitivité, de sécurité et de résilience.

Depuis plusieurs années, les collectivités sont de plus en plus concernées par ces questions. Elles ont en effet recours aux outils informatiques extra-européens, notamment en matière de bureautique, d'infrastructure informatique, de sécurité, de stockage et plus récemment d'intelligence artificielle.

Dans ce contexte, la directrice générale des services (DGS) vous demande de rédiger à son attention, un rapport portant sur les enjeux liés à la souveraineté numérique de la commune d'Admiville assorti de solutions opérationnelles.

Vous rédigerez ce rapport à l'aide des éléments du dossier et en mobilisant vos connaissances.

Liste des documents :

Document 1 : « Cloud Act : définition et implications » - *Datalegal* - 6 octobre 2025 - 1 page

Document 2 : « Renforcez votre souveraineté numérique avec La Suite territoriale » - *La Suite territoriale* - 15 octobre 2025 - 3 pages

Document 3 : « Les collectivités se mobilisent pour la souveraineté numérique » - *Intercommunalités de France* - 11 avril 2025 - 2 pages

Document 4 : « Comment se passer de Microsoft Office 365 et migrer vers ONLYOFFICE » (extraits) - *ITPME* - novembre 2025 - 5 pages

Document 5 : « Reprendre le Contrôle de son Destin Numérique : Le Virage Linux des Administrations Territoriales, enjeux de souveraineté numérique » (extraits) - *ITPME* - 29 septembre 2025 - 3 pages

Document 6 : « Souveraineté numérique : un défi concret pour les acteurs publics » (extraits) - *easiware.com* - 12 novembre 2025 - 4 pages

Document 7 : « Souveraineté numérique : les collectivités locales se libèrent des GAFAM grâce à l'open source » (extraits) - *rwx-g.fr* - 3 juillet 2025 - 7 pages

Document 8 : « Les enjeux au long cours de la souveraineté en matière d'IA » - *Banque des territoires* - 11 juillet 2025 - 3 pages

Document 9 : « SecNumCloud : certification française pour le cloud souverain » (extrait) - *performance marketing expert* - 25 décembre 2025 - 1 page

Document 10 : « Investissement et souveraineté numérique : le défi de 2026 » - *Aqui.fr* - 24 mai 2026 - 4 pages

Documents reproduits avec l'autorisation du CFC

Certains documents peuvent comporter des renvois à des notes ou à des documents non fournis car non indispensables à la compréhension du sujet.

Dans un souci environnemental, les impressions en noir et blanc sont privilégiées. Les détails non perceptibles du fait de ce choix reprographique ne sont pas nécessaires à la compréhension du sujet, et n'empêchent pas son traitement.

datalegal

DOCUMENT 1

Cloud Act : définition et implications

06/10/2025

Définition et portée juridique

Le **Cloud Act** (abréviation de **Clarifying Lawful Overseas Use of Data Act**) est une loi fédérale américaine adoptée en 2018 qui modifie certaines dispositions du **Stored Communications Act**. Son objectif légal principal est de préciser la capacité des autorités américaines à obtenir des données détenues par des fournisseurs de services électroniques soumis à la juridiction des États-Unis, y compris lorsque ces données sont stockées à l'étranger. Le texte introduit également un mécanisme d'**accords exécutifs** qui permet au gouvernement américain de conclure des accords bilatéraux pour l'accès transfrontalier aux données avec des pays partenaires répondant à des critères de protection des droits fondamentaux.

Principaux mécanismes et garanties

Concrètement, le **Cloud Act** autorise les autorités à délivrer des **mandats** ou autres instruments légaux à des fournisseurs américains pour obtenir des communications ou des métadonnées indépendamment du lieu de stockage. Le texte prévoit toutefois des voies de contestation : un fournisseur peut demander au tribunal d'examiner une demande lorsqu'elle entre en conflit avec une loi étrangère applicable ou si l'exécution porterait atteinte aux droits d'une personne. Les **accords exécutifs** comportent des conditions sur les garanties procédurales et la supervision judiciaire des demandes.

Points de tension avec le RGPD et le droit international

Le **Cloud Act** peut engendrer des conflits de lois juridiques et opérationnels, en particulier avec le **RGPD**. Par exemple, une entreprise américaine qui stocke des données de citoyens européens peut être légalement contrainte de divulguer ces données aux autorités américaines, situation potentiellement incompatible avec les obligations de protection et de notification imposées par le droit européen. Les tribunaux et régulateurs européens recommandent d'évaluer au cas par cas les demandes et d'utiliser les mécanismes de contestation prévus par le texte. (…)

Mesures pratiques de conformité et recommandations

- Évaluer la domiciliation juridique des fournisseurs et la présence opérationnelle aux États-Unis (**fournisseurs américains**).
- Mettre en place un **chiffrement** avec contrôle des clés par le client pour minimiser l'exposition aux demandes de divulgation.
- Prévoir des clauses contractuelles et des procédures internes pour traiter les demandes gouvernementales et activer les recours judiciaires prévus par le **Cloud Act**.
- Consulter la DPO et les services juridiques pour analyser les risques de **conflit de lois** avec le RGPD avant tout transfert ou externalisation.

DOCUMENT 2

Renforcez votre souveraineté numérique avec La Suite territoriale

Publié le 15 octobre 2025

Traitement de texte, messagerie, stockage de documents... Les outils numériques utilisés par les collectivités territoriales sont encore largement d'origine extra-européenne. Ces usages interrogent la souveraineté numérique, impliquant des coûts élevés, des limites en matière de sécurité et des coûts de transition vers des outils souverains importants. La Suite territoriale constitue une alternative publique souveraine pour les plus petites collectivités.

La souveraineté numérique en quatre points clés

La *souveraineté numérique* vise à réduire la dépendance de la France à l'égard de puissances extra-européennes. Elle repose sur quatre axes principaux :

- Le renforcement de la **cybersécurité** des infrastructures et des systèmes d'information
- L'**hébergement des données sur une infrastructure** européenne sécurisée
- L'adoption de **solutions numériques européennes et *open source***
- La **maîtrise des coûts** liés à cette adaptation

Pourquoi les collectivités territoriales sont-elles concernées par ces enjeux ?

Parce qu'elles manient les données personnelles de leurs habitants ainsi que des fonds publics, les collectivités territoriales sont les premières concernées par les enjeux de souveraineté numérique. Or, elles rencontrent **d'importantes difficultés** :

- Les collectivités territoriales font face à l'aggravation de la cybermenace : selon une étude de cybermalveillance.gouv, **une collectivité sur 10 a été victime d'une cyberattaque en 2024**, **entraînant un arrêt temporaire d'activité pour un tiers d'entre elles**. Ces menaces touchent également les habitants des collectivités quand celles-ci ne sont pas clairement identifiables sur internet. Or, **seules 19% des communes françaises sont conformes aux critères de sécurité dans leur communication en ligne** selon l'Observatoire de la présence numérique des territoires.

- La majorité des collectivités territoriales utilise des solutions propriétaires extraeuropéennes qui présentent un risque pour la souveraineté des données, ainsi que des enjeux d'utilisation des données des utilisateurs à des fins commerciales. Ces solutions entraînent également une forme de captivité de l'utilisateur dans la mesure où leur interopérabilité avec des solutions tierces est limitée - la collaboration entre services et avec d'autres structures est alors réduite. Selon le Labo Société Numérique, **moins d'une collectivité sur deux favorise l'utilisation de solutions françaises et seules 7% privilégient l'*open source*.**

- L'hébergement des données des collectivités territoriales n'est pas nécessairement souverain ou sécurisé : **86% des communes utilisent des centres de données ne disposant pas du label *SecNumCloud*,** lequel garantit la robustesse du service face aux cyberattaques.

- Enfin, le numérique représente un poste budgétaire important pour les collectivités.
    - D'un côté, face à un budget contraint, les collectivités territoriales les plus fragiles ne sont pas nécessairement en mesure d'adopter les solutions adaptées à leur besoin en outillage numérique de base ou spécifiques à la cybersécurité. **73 % des petites et moyennes collectivités ont un budget informatique annuel de moins de 5 000 euros. En moyenne 2000€ par an sont alloués à la cybersécurité** selon Cybermalveillance.gouv. Certaines petites communes ne disposent ainsi pas de la capacité budgétaire d'absorber le coût de l'adaptation à la menace cyber, et adoptent en conséquence des solutions peu onéreuses mais non souveraines.
    - D'un autre côté, ces dépenses liées au numérique représentent déjà un coût important pour toutes les collectivités, notamment du fait de leur dépendance à des solutions propriétaires et payantes. **Selon le président des Interconnectés, les dépenses publiques du bloc local pour l'utilisation de produits et services numériques extraeuropéens représentent 1,5 milliard d'euros par an, soit 42 900€ en moyenne par collectivité**. C'est notamment pour réduire cette dépendance, synonyme de déperditions d'argent public, que Les Interconnectés et certaines collectivités de taille importante ont lancé l'initiative Tie Break en avril 2025.

La Suite territoriale permet de renforcer la souveraineté numérique des collectivités territoriales

Issue d'un partenariat entre l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et l'Agence nationale de la cohésion des territoires (ANCT), **la Suite territoriale vise à renforcer la cybersécurité des systèmes d'information des petites collectivités territoriales *via* notamment la mise à disposition d'un socle de solutions simples, souveraines et *open source*.**

- En mettant à disposition un nom de domaine institutionnel minimal pour toutes les communes qui en sont dépourvues et en permettant de s'authentifier *via* un identifiant et un mot de passe uniques ProConnect, la Suite territoriale est la solution minimale permettant **aux collectivités les plus vulnérables de réduire drastiquement le risque de cyberattaques auquel elles font face.** Elle permet, dans un premier temps, d'être conforme aux critères d'hygiène numérique de base en matière de communication en ligne (domaine, courriel, site web) grâce au Référentiel de la présence numérique des territoires.

- La Suite territoriale est entièrement développée sur la base de solutions *open source,* **son développement a été réalisé par les opérateurs français nationaux que sont l'ANCT et l'ANSSI.** La transparence offerte par l'*open source* protège les collectivités des différents risques des solutions sous licence. La publication du code permet son appropriation par n'importe qui favorise l'interopérabilité avec d'autres logiciels, et permet à l'ensemble de l'écosystème, public et privé, de coopérer sur un objet commun. Par ailleurs, les outils de La Suite territoriale ont été pensés pour être

simples d'utilisation afin de **pallier les difficultés liées à l'adoption et au changement d'outil.**

- L'hébergement de toutes les données de nos outils est assuré *via* **des hébergeurs et centres de données sécurisés et européens**, en cours de **labellisation *SecNumCloud***.

- Enfin, grâce au développement public, à la mutualisation des coûts *via* les structures de mutualisation présentes sur le territoire et à la coopération entre l'État, les opérateurs publics de services numériques et les collectivités territoriales elles-mêmes, **les solutions de La Suite territoriale sont accessibles à un coût réduit** voire mises à disposition à titre gracieux pour les plus vulnérables d'entre elles. Les outils ne comprennent par exemple ni d'abonnement, ni de fonctionnalité payante, ni de mode *premium*. **La Suite territoriale répond ainsi d'une mission de service public** : outiller les collectivités avec un socle minimal de services numériques, afin de permettre aux agents et élus de travailler de manière sécurisée, sans condition de ressource humaine ou financière.

INTERCOMMUNALITÉS DE FRANCE

DOCUMENT 3

Les collectivités se mobilisent pour la souveraineté numérique

Publié le 11/04/2025

Le 9 avril, les élus et membres de la commission numérique des Interconnectés, France urbaine et Intercommunalités de France se sont réunis à Paris (Station F) pour lancer la démarche « TIE BREAK » des collectivités territoriales en faveur d'une Trajectoire d'Indépendance numérique Européenne.

Réagir face à la dépendance des systèmes d'information des collectivités

Président des Interconnectés, Franckie Trichet a ouvert la conférence de presse en appelant à « *sortir d'une forme de déni* » face à la dépendance du bloc local à des technologies extra-européennes : « *Avec 22 métropoles, 101 départements, 18 régions, 1254 Intercos, 35 000 communes, nous parlons a minima de 1,5 milliard d'euros dépensés chaque année auprès d'acteurs économiques qui ne sont pas européens* ».

Face à une sédimentation technologique vieille de plusieurs décennies, il a insisté sur l'importance de prendre le temps nécessaire pour construire collectivement une stratégie en plusieurs étapes pour que chaque collectivité reprenne en main son destin numérique.

Un premier outil de diagnostic du niveau de dépendance des systèmes d'information dévoilé

A la suite du forum des Interconnectés qui s'est tenu à Rennes les 10 et 11 mars derniers, un groupe pilote de 11 collectivités a engagé une démarche commune pour mesurer le niveau de dépendance de leur système d'information à des technologies extra-européennes. Cet outil permet d'établir une cartographie précise des domaines concernés, ainsi que des éléments concrets et actionnables dont chaque collectivité peut s'emparer, comme le niveau de criticité des incidents numériques.

Conseiller à la métropole de Montpellier, Manu Reynaud a présenté le diagnostic mis en œuvre dans cette dernière, en insistant sur le caractère crucial des typologies de stratégie définies et de la formation auprès des directions des systèmes d'information (DSI) pour faire vivre la démarche.

Conçu pour être partagé et ouvert, l'outil de diagnostic sera enrichi par le travail collectif de plusieurs collectivités volontaires, afin de stabiliser un cadre commun. La prochaine étape visera à proposer une bibliothèque d'alternatives fiables et efficaces aux collectivités, pour établir un espace numérique plus souverain.

S'emparer des enjeux soulevés par la cybersécurité

Cette démarche s'inscrit dans une montée en compétences sur les enjeux numériques, particulièrement ceux liés à la cybersécurité.

Vice-présidente de l'Eurométropole de Strasbourg, Caroline Zorn a rappelé qu'en 2024, 10% des collectivités territoriales ont été victimes d'une ou plusieurs cyberattaques, mais 45% d'entre elles n'en connaissaient pas la cause.

Au-delà de la nécessaire sensibilisation sur le sujet, l'enjeu réside également dans l'élaboration d'une nouvelle politique industrielle, davantage tournée vers les acteurs européens, en s'appuyant particulièrement sur la cryptographie. Elu à la communauté urbaine d'Arras, Mickaël Audegond a expliqué que la directive européenne NIS 2 en matière de cybersécurité doit être regardée par les collectivités comme l'opportunité d'enclencher une réflexion systémique, pour mieux adapter leurs politiques aux besoins des entreprises.

A l'échelle des collectivités, c'est le levier de la commande publique qui est appelé à être davantage mobilisé pour favoriser un numérique souverain et aussi responsable.

Mobiliser l'échelle européenne

Pour bâtir ces alternatives, la dimension européenne est cruciale, comme l'a montré la convergence de vue des acteurs locaux réunis au Forum digital d'Eurocities qui s'est tenu à Bordeaux du 2 au 4 avril derniers. Laurent Watrin, adjoint au maire de Nancy et président de la Commission « Europe et participation citoyenne » de l'Association Française du Conseil des Communes et Régions d'Europe (AFCCRE), a d'ailleurs rappelé que les retours d'expériences des territoires sont précieux pour l'élaboration des normes de l'Union européenne, à l'image du règlement sur l'interopérabilité des services publics numériques. Celui-ci vise à faciliter l'échange transfrontalier de données dans le domaine de la santé, des transports ou encore des formalités administratives, pour rendre accessibles l'ensemble des services publics essentiels de l'Union européenne d'ici à 2030.

Pour Delphine Jamet, conseillère à la métropole de Bordeaux déléguée au numérique, l'Europe doit être « un rempart à l'heure de la guerre commerciale », ce qui suppose d'accompagner davantage les agents publics et les citoyens pour faire évoluer leurs pratiques numériques. « Il faut sensibiliser et former pour ne pas céder à la facilité des outils extra-européens » a renchéri Dominique Marty, conseiller de la communauté d'agglomération du Sicoval en charge de la transformation numérique.

Affermir le dialogue entre acteurs publics et privés

Outre les associations d'élus, l'Agence nationale de la cohésion des territoires (ANCT), la direction interministérielle du numérique (DINUM), la Banque des territoires ainsi que plusieurs institutions et entreprises étaient également présentes à Bordeaux pour marquer ce tournant stratégique.

Toutes ont fait part de leur volonté de travailler plus étroitement avec les collectivités et les agences de l'Etat, qu'il s'agisse du développement de jeunes champions européens du secteur dans les territoires, de la construction de communs numériques ou encore de la transition écologique.

En appelant à une mobilisation locale, nationale et européenne, les collectivités territoriales démontrent leur volonté politique de participer activement à l'édification d'une véritable souveraineté numérique, pour protéger et servir les citoyens.

DOCUMENT 4

Comment se passer de Microsoft Office 365 et migrer vers ONLYOFFICE

ITPME 11/2025

Microsoft Office 365 domine le marché des suites bureautiques depuis des décennies, mais son modèle d'abonnement et ses coûts récurrents poussent de nombreux utilisateurs et entreprises à explorer des alternatives viables. ONLYOFFICE émerge comme une solution crédible, offrant compatibilité, fonctionnalités collaboratives et une approche plus flexible en termes de déploiement et de coût.

Cette transition peut sembler intimidante, mais avec une planification adéquate et une compréhension des différences entre les deux plateformes, le passage à ONLYOFFICE peut s'effectuer en douceur tout en préservant votre productivité.

Comprendre ONLYOFFICE : Une alternative complète

ONLYOFFICE est une suite bureautique open-source qui propose des éditeurs pour documents texte, feuilles de calcul et présentations. Contrairement à Microsoft Office 365, ONLYOFFICE offre plusieurs options de déploiement : cloud, auto-hébergé ou version desktop.

Les avantages principaux d'ONLYOFFICE

Compatibilité des formats : ONLYOFFICE excelle dans la gestion des formats Microsoft Office (DOCX, XLSX, PPTX), offrant une compatibilité souvent supérieure à d'autres alternatives comme LibreOffice. Les documents conservent leur mise en forme, réduisant considérablement les problèmes de conversion.

Coût maîtrisé : Contrairement au modèle d'abonnement mensuel d'Office 365, ONLYOFFICE propose une version gratuite pour les particuliers et des licences perpétuelles pour les entreprises, permettant un meilleur contrôle budgétaire.

Contrôle des données : L'option d'auto-hébergement offre une souveraineté totale sur vos documents, un atout majeur pour les organisations soucieuses de confidentialité ou soumises à des réglementations strictes comme le RGPD.

Collaboration en temps réel : ONLYOFFICE intègre nativement des fonctionnalités collaboratives comparables à celles d'Office 365, avec édition simultanée, commentaires et suivi des modifications.

Évaluer vos besoins avant la migration

Avant d'entamer la transition, une analyse approfondie de votre utilisation actuelle d'Office 365 s'impose.

Inventaire des fonctionnalités utilisées

Identifiez quelles applications Office 365 votre organisation utilise réellement. Si vous dépendez uniquement de Word, Excel et PowerPoint, la migration sera simple. En revanche, si vous exploitez intensivement Outlook, Teams, SharePoint ou Power BI, vous devrez trouver des solutions complémentaires.

Identification des dépendances critiques

Certaines fonctionnalités avancées comme les macros VBA complexes, les tableaux croisés dynamiques élaborés ou les intégrations spécifiques peuvent nécessiter des adaptations. Testez vos documents les plus complexes dans ONLYOFFICE pour identifier les éventuels problèmes de compatibilité.

Évaluation de l'infrastructure

Pour une installation auto-hébergée, vérifiez que votre infrastructure IT peut supporter ONLYOFFICE. Les prérequis incluent un serveur Linux ou Windows avec des ressources suffisantes et, idéalement, une intégration avec votre solution de stockage cloud existante.

Choisir la version d'ONLYOFFICE adaptée :

ONLYOFFICE se décline en plusieurs versions répondant à différents besoins.

ONLYOFFICE Desktop Editors

Version gratuite installable sur Windows, Linux et macOS, idéale pour les utilisateurs individuels ou les petites équipes. Elle permet de travailler hors ligne avec une excellente compatibilité Office, mais sans fonctionnalités collaboratives natives.

ONLYOFFICE Docs (auto-hébergé)

Solution pour entreprises souhaitant garder le contrôle total de leurs données. Nécessite une infrastructure serveur mais offre toutes les fonctionnalités collaboratives. Disponible en version communautaire gratuite ou Enterprise avec support professionnel.

ONLYOFFICE Workspace

Plateforme cloud complète incluant éditeurs de documents, gestion de projets, CRM et messagerie. Alternative tout-en-un pour les organisations cherchant à remplacer plusieurs services Microsoft simultanément.

(…)

Remplacer les autres services Office 365

La suite Office représente seulement une partie de l'écosystème Office 365. Voici comment remplacer les autres composants.

Alternative à Outlook

Pour la messagerie, plusieurs options s'offrent à vous : Thunderbird (gratuit et open-source), Evolution sous Linux, ou la solution intégrée d'ONLYOFFICE Workspace. Ces clients supportent les protocoles standards IMAP/SMTP et peuvent se connecter à Exchange si nécessaire.

Remplacement de Teams

Pour la communication d'équipe, explorez Rocket.Chat, Mattermost ou Slack selon votre budget et vos besoins de confidentialité. ONLYOFFICE s'intègre avec plusieurs de ces plateformes, maintenant un workflow unifié.

Substitut à OneDrive/SharePoint

Nextcloud et ownCloud offrent des fonctionnalités de stockage cloud auto-hébergé avec une excellente intégration ONLYOFFICE. Synology Drive constitue une option pour les organisations utilisant des NAS Synology.

Gestion de projet sans Microsoft Planner

ONLYOFFICE Workspace inclut un module de gestion de projets. Alternativement, Taiga, OpenProject ou Redmine proposent des solutions robustes, particulièrement pour les équipes techniques.

(…)

Gérer la compatibilité et la collaboration externe

L'un des défis majeurs concerne l'interaction avec des partenaires utilisant encore Office 365.

Assurer la compatibilité bidirectionnelle

ONLYOFFICE maintient une excellente compatibilité avec les formats Microsoft, mais certains éléments complexes peuvent différer. Pour les documents externes critiques, conservez une instance Office 365 minimale ou utilisez Office Online (version gratuite web) pour les vérifications finales.

Collaborer avec des utilisateurs externes

ONLYOFFICE permet de partager des liens d'édition collaboratifs fonctionnant dans n'importe quel navigateur, sans nécessiter de compte Microsoft. Vos partenaires peuvent éditer vos documents directement sans installation logicielle.

Pour les échanges de fichiers, privilégiez les formats standards et testez systématiquement le rendu dans Office avant d'envoyer des documents importants à des clients utilisant Microsoft.

(…)

Calcul du retour sur investissement

La décision de migration doit reposer sur une analyse économique rigoureuse.

Comparaison des coûts

Office 365 Business Standard coûte environ 12€/utilisateur/mois, soit 144€/an. Pour 50 utilisateurs, cela représente 7 200€ annuels. ONLYOFFICE Desktop Editors est gratuit, tandis qu'ONLYOFFICE Docs Enterprise coûte environ 1 500€ pour 50 connexions simultanées (licence perpétuelle).

Sur cinq ans, Office 365 coûterait 36 000€ contre environ 3 000€ pour ONLYOFFICE (licence + infrastructure), représentant une économie potentielle de 90%.

Coûts cachés à considérer

N'oubliez pas les coûts de migration : formation, temps d'adaptation, éventuelle assistance technique externe. Pour un déploiement auto-hébergé, ajoutez les coûts d'infrastructure et de maintenance IT.

Cependant, ces investissements initiaux sont généralement amortis en moins de deux ans pour des organisations de taille moyenne.

(…)

Surmonter les obstacles à l'adoption - Malgré les avantages, certaines résistances sont prévisibles

Résistance au changement

La familiarité avec Office est un frein majeur. Impliquez les utilisateurs dès la phase de test, valorisez les champions du changement et communiquez clairement sur les bénéfices plutôt que sur les contraintes techniques.

Fonctionnalités manquantes

ONLYOFFICE ne dispose pas de toutes les fonctionnalités avancées d'Office. Pour les cas d'usage spécifiques nécessitant absolument ces fonctions, envisagez une approche hybride avec quelques licences Office maintenues pour les utilisateurs power.

Support technique

Contrairement à Microsoft, le support d'ONLYOFFICE communautaire repose sur forums et documentation. La version Enterprise offre un support professionnel, mais prévoyez des ressources IT internes pour la maintenance courante.

(…)

Se passer de Microsoft Office 365 n’est plus un sacrifice en termes de fonctionnalités. ONLYOFFICE offre une alternative mature, compatible et économique, particulièrement adaptée aux organisations soucieuses de maîtriser leurs coûts et leurs données.

La migration nécessite une planification minutieuse et un accompagnement des utilisateurs, mais les bénéfices financiers et stratégiques justifient cet investissement. Que vous soyez une PME cherchant à réduire ses coûts, une organisation valorisant la souveraineté numérique, ou simplement un utilisateur lassé des abonnements récurrents, ONLYOFFICE mérite votre attention.

Le moment idéal pour migrer est celui où vous questionnez la valeur apportée par votre abonnement actuel. Avec une approche méthodique et progressive, et l’accompagnement d’experts comme ITPME, la transition vers ONLYOFFICE peut s’effectuer en douceur, ouvrant la voie à une productivité bureautique libérée des contraintes d’abonnement.

DOCUMENT 5

Reprendre le Contrôle de son Destin Numérique : Le Virage Linux des Administrations Territoriales, enjeux de souveraineté numérique

ITPME – 29/09/2025

Dans un contexte géopolitique tendu et face à une dépendance technologique croissante, les collectivités locales françaises se trouvent à un tournant historique. La dépendance des collectivités aux solutions extra-européennes est évaluée à 1,5 milliard d'euros annuels, un montant considérable qui questionne à la fois la souveraineté numérique nationale et la gestion responsable des deniers publics.

La ville de Lyon lance un vaste chantier de **transformation numérique** pour réduire sa dépendance aux logiciels américains en misant sur l'open source, une démarche suivie par de nombreuses autres collectivités. Plus récemment, la région Île-de-France a abandonné Microsoft pour des solutions françaises, migrant vers le **cloud souverain** de Leviia. Ces exemples illustrent un mouvement de fond qui dépasse la simple question technique pour toucher aux fondements mêmes de l'autonomie stratégique de nos territoires.

(…)

Linux : La Solution Technique au Service de la Souveraineté

Pourquoi Linux est la Réponse Adaptée aux Collectivités

Les administrations publiques bénéficient d'une grande flexibilité avec Linux, qui peut être personnalisé, favorisant ainsi la souveraineté technologique des institutions publiques. Mais au-delà de cette flexibilité, Linux présente des avantages structurels uniques :

1. Un Système Libre et Open Source

Linux est un système d'exploitation open-source disponible gratuitement pour tout le monde, permettant aux utilisateurs de personnaliser et de modifier le système selon leurs besoins. Concrètement, cela signifie :

- **Transparence totale** : Le code source est auditable par n'importe quel expert, garantissant l'absence de portes dérobées ou de fonctionnalités cachées
- **Pérennité** : Aucun éditeur ne peut décider d'arrêter le support ou de forcer une migration coûteuse
- **Adaptabilité** : Les collectivités peuvent modifier le système pour répondre précisément à leurs besoins métier spécifiques
- **Indépendance technologique** : Pas de vendor lock-in (enfermement propriétaire) qui piège les administrations dans des écosystèmes fermés

2. Des Économies Budgétaires Substantielles

Les avantages de l'open source incluent notamment un coût largement inférieur à celui des logiciels propriétaires. Pour une collectivité, les économies se déclinent à plusieurs niveaux :

- **Licences** : Élimination des coûts de licences Microsoft Windows (environ 150-300€ par poste) et Microsoft Office 365 (60-150€/utilisateur/an)
- **Maintenance** : Un ordinateur de bureau sous OS open source industrialisé constitue un puissant levier pour la gouvernance informatique, réduisant les frais liés à la gestion
- **Matériel** : Linux fonctionne efficacement sur du matériel ancien, prolongeant la durée de vie des équipements de 3 à 5 ans supplémentaires
- **Formation** : L'écosystème open source favorise la mutualisation des compétences entre collectivités

Exemple concret : Une collectivité de 500 agents peut économiser entre 100 000€ et 200 000€ par an en passant à Linux, soit 500 000€ à 1 million d'euros sur un mandat municipal.

3. Sécurité Renforcée et Souveraineté des Données

Linux est réputé pour sa robustesse en termes de sécurité. Cette réputation repose sur plusieurs facteurs techniques :

- **Architecture sécurisée nativement** : Séparation stricte des privilèges, système de permissions robuste
- **Réactivité face aux failles** : La communauté open source corrige les vulnérabilités en quelques heures, contre plusieurs jours ou semaines pour les éditeurs propriétaires
- **Moins de malwares** : 95% des malwares ciblent Windows ; Linux reste largement épargné
- **Mises à jour maîtrisées** : L'administration contrôle le calendrier et le contenu des mises à jour, sans dépendre des décisions unilatérales d'un éditeur

4. Interopérabilité et Standards Ouverts

Linux respecte et promeut les standards ouverts (formats de fichiers, protocoles de communication), garantissant :

- L'échange fluide de données entre administrations
- La pérennité des documents sur le long terme
- La compatibilité avec l'écosystème numérique européen et national
- L'absence de dépendance à des formats propriétaires

(…)

Exemples Inspirants de Collectivités Ayant Franchi le Pas

Lyon : Pionnière de la Souveraineté Numérique Territoriale

La Ville de Lyon s'est engagée dans une transformation majeure de ses outils numériques pour ne plus être dépendante des solutions logicielles états-uniennes et acquérir une véritable souveraineté numérique. Cette démarche ambitieuse comprend la migration vers des solutions libres et la création d'une suite collaborative open source.

Résultats attendus :

- Économies budgétaires significatives
- Protection renforcée des données des Lyonnais

- Exemplarité en matière de souveraineté numérique

L'Île-de-France : Abandon de Microsoft pour le Cloud Souverain

La région a migré vers le cloud souverain de Leviia, dont les data centers sont situés entre Marseille et Lyon, garantissant un contrôle total des données avec la plateforme sécurisée MonLycée.net. Cette décision stratégique concerne des centaines de milliers de lycéens et enseignants.

La Gendarmerie Nationale : Référence Historique

La Gendarmerie a migré 72 000 postes vers Ubuntu dès 2005, démontrant la faisabilité à grande échelle et générant des économies de plusieurs millions d'euros annuels.

(…)

Conclusion : L'Urgence d'Agir pour la Souveraineté Numérique

Les élus ont lancé le projet Trajectoire d'indépendance européenne numérique (Tie Break) pour évaluer leur niveau de dépendance numérique et créer une bibliothèque de solutions souveraines. Cette initiative collective témoigne d'une prise de conscience nationale.

Face aux enjeux de souveraineté, de sécurité et d'économie budgétaire, la migration vers Linux n'est plus une option pour les collectivités locales, c'est une nécessité stratégique. Chaque mois de retard représente des centaines de milliers d'euros versés à des entreprises extra-européennes, des données sensibles potentiellement exposées et une dépendance technologique renforcée.

La transition vers Linux demande certes un investissement initial en formation et en accompagnement au changement, mais les bénéfices à moyen et long terme sont considérables : économies substantielles, sécurité renforcée, autonomie stratégique et contribution à un écosystème numérique européen souverain.

Les exemples de Lyon, de l'Île-de-France et de nombreuses autres collectivités démontrent que cette transition est non seulement possible, mais souhaitable. Il est temps pour les collectivités françaises de reprendre le contrôle de leur destin numérique et de construire un service public résilient, souverain et au service de l'intérêt général.

easiware

DOCUMENT 6

Souveraineté numérique : un défi concret pour les acteurs publics

Publié le 12 novembre 2025

Avec une écrasante majorité des technologies et des infrastructures numériques qui sont aux mains d'acteurs non européens, les institutions publiques françaises et européennes sont confrontées à un véritable dilemme, celui de la souveraineté numérique. Une question se pose notamment : comment garantir l'indépendance, la sécurité et la maîtrise des outils numériques tout en assurant une bonne qualité de service pour les citoyens ?

Loin d'être cantonnée à un débat technico-politique, la souveraineté numérique est devenue un impératif stratégique, auquel sont liées la protection des données, la continuité des services publics et la préservation de l'intérêt général. Mais entre les pressions économiques, les enjeux de cybersécurité et les attentes en matière d'inclusion numérique, les défis à relever sont nombreux.

1. Qu'est-ce que la souveraineté numérique, enjeu stratégique pour les services publics ?

A. La souveraineté numérique, une question de contrôle et d'indépendance

Selon le Sénat, la souveraineté numérique est la capacité d'un État ou d'une organisation à manœuvrer librement dans le cyberespace, sans subir d'influence ou de contrainte extérieure. Elle s'articule autour de deux piliers fondamentaux :

- L'indépendance technologique, c'est-à-dire la faculté de déployer des ressources, des logiciels, des infrastructures ou des services numériques sur lesquels l'État conserve un contrôle direct, sans dépendre d'acteurs étrangers.
- Le contrôle des données, qui implique de savoir où elles sont stockées, qui y a accès, et sous quelle juridiction elles sont placées.

B. Une dépendance aujourd'hui trop importante

Le constat est ainsi relativement préoccupant en Europe, car, d'après des chiffres du Gouvernement, 83 % des dépenses numériques profitent aujourd'hui à des entreprises non européennes, avec une dépendance économique et technologique particulièrement marquée vis-à-vis de géants du numérique américains ou chinois. Cette situation compromet la souveraineté des décisions étatiques, la sécurisation des données, et le développement de politiques publiques indépendantes.
(…)

C. Un défi d'ampleur pour les services publics

Les services publics sont en première ligne de ce combat pour la souveraineté numérique. Ils doivent assurer la continuité des services essentiels, garantir la protection des données sensibles, et préserver l'intégrité des politiques publiques.

Les administrations doivent en plus composer avec des cadres juridiques qui peuvent être conflictuels, à l'exemple du Cloud Act américain qui autorise les autorités des États-Unis à exiger l'accès à des données stockées par des entreprises américaines, même si celles-ci sont hébergées en dehors du territoire national. Cette extraterritorialité du droit s'accompagne d'un risque majeur pour la confidentialité et la souveraineté des informations publiques.

(…)

2. Comprendre la souveraineté numérique

A. Notions et principes

La souveraineté numérique implique des principes fondamentaux, qui sont étroitement liés aux enjeux de maîtrise technologique, de sécurité des données et de conformité réglementaire. Pour les acteurs publics, comprendre et intégrer ces notions est indispensable afin de bâtir une stratégie numérique indépendante et pérenne.

– Réduire la dépendance aux géants du numérique

Le premier enjeu consiste à disposer d'alternatives nationales ou européennes aux services numériques jugés critiques, comme les solutions de cloud computing, les messageries collaboratives ou les plateformes d'**IA**. Aujourd'hui, une grande partie de ces outils sont fournis par des acteurs américains (GAFAM) ou chinois (BATX), ce qui expose les organisations publiques à une perte de contrôle sur leurs infrastructures, et les rend vulnérables en cas de tensions géopolitiques ou de restrictions commerciales. (…)

– Le contrôle et la localisation des données

Aussi, la maîtrise des données inclut en premier lieu de savoir précisément où elles sont stockées, sous quelle juridiction, et quelles sont les conditions pour y accéder. Pour les administrations, cela signifie être en mesure d'héberger les informations sensibles (données de santé, données fiscales, infrastructures critiques, etc.) dans des environnements sécurisés, gérés par des entités soumises au droit national ou européen. (…)

– Un cadre juridique qui se renforce en Europe

Pour faire face à ces enjeux, l'Union européenne a engagé un vaste chantier de régulation dont l'objectif est de renforcer sa souveraineté numérique. Plusieurs mesures et textes clés soutiennent cette stratégie :

- Le **RGPD (Règlement général sur la protection des données)**, qui impose des standards élevés en termes de protection des données personnelles ;
- Le DSA (Digital Services Act) et le DMA (Digital Markets Act), qui ont pour but de mieux encadrer les plateformes numériques et de garantir une concurrence équitable ;
- Le Data Act, en cours d'entrée en vigueur, qui a pour ambition de clarifier les droits d'accès et de partage des données industrielles. (…)

B. Enjeux spécifiques pour les services publics

Les principes de la souveraineté numérique s'appliquent à tous les secteurs d'activité, mais les services publics, en raison de leur rôle central dans la vie des citoyens et de la nature sensible des données qu'ils manipulent, sont confrontés à des enjeux particuliers. Garantir leur autonomie s'impose donc comme une condition essentielle pour assurer la stabilité, la sécurité et l'équité des politiques publiques.

– Protéger les données et les infrastructures critiques

Les administrations et opérateurs publics gèrent des flux massifs de données sensibles, qui peuvent être des dossiers médicaux, des informations fiscales, des documents juridiques ou encore des bases de données relatives à la sécurité nationale. Toute compromission de ces données pourrait avoir des conséquences graves sur la continuité des services, la confiance des citoyens, voire la stabilité de certaines institutions. (…)

– Garantir l'égalité d'accès aux services numériques

L'universalité de l'accès aux services publics est un véritable fondement de l'action publique. Cette égalité est cependant fragilisée si certaines zones géographiques, notamment rurales ou isolées, dépendent d'infrastructures numériques trop éloignées ou gérées par des acteurs étrangers. (…)

– Soutenir la compétitivité et l'innovation publique

La capacité d'innovation des services publics dépend de leur maîtrise technologique. En conservant la main sur leurs outils numériques et en investissant dans des solutions souveraines, les institutions consolident leur agilité, leur réactivité, et leur aptitude à proposer de nouveaux services adaptés aux besoins des usagers. (…)

– Préserver la sécurité nationale

Certains secteurs d'activité qui sont gérés ou régulés par les pouvoirs publics, comme la santé, l'énergie, la justice ou la défense, sont concernés par des enjeux de sécurité particulièrement élevés. Toute faille dans les systèmes d'information utilisés par ces secteurs peut avoir des répercussions considérables, qui vont de la désorganisation des services à des actes de malveillance comme l'espionnage, le sabotage ou encore la manipulation des données. (…)

– Cultiver la confiance des citoyens

La transformation numérique des services publics ne peut s'avérer efficace qu'avec l'adhésion des citoyens. Cependant, cette confiance dépend en grande partie de la transparence quant à la gestion des données personnelles, au respect des règles éthiques, et à la garantie que les services numériques sont conçus dans l'intérêt général. (…)

3. Les défis concrets pour les acteurs publics

A. Dépendance aux solutions extraterritoriales

L'un des principaux obstacles à la souveraineté numérique est la forte dépendance des acteurs publics vis-à-vis de fournisseurs étrangers. Une grande majorité des data centers en Europe sont aujourd'hui détenus et gérés par des entreprises non européennes, qui sont donc soumises à des cadres juridiques extérieurs. Cela remet en cause la capacité des États à disposer d'un contrôle total sur les données et les infrastructures numériques essentielles.

Réduire cette dépendance implique alors d'identifier les services critiques concernés, ainsi que de développer des alternatives souveraines crédibles, ce qui suppose des investissements importants à l'échelle nationale et européenne.

B. Trouver le bon équilibre entre efficience, sécurité et sobriété

Les administrations doivent faire face à un triple impératif :

- déployer des solutions numériques efficaces,
- garantir leur sécurité,
- intégrer les exigences en matière de sobriété énergétique et environnementale.

Elles se confrontent néanmoins à de fortes contraintes budgétaires, qui rendent souvent difficile la conciliation de ces objectifs.

(…)

C. Prioriser les projets et encadrer l'usage de l'IA

En raison de la multiplication des besoins numériques, les acteurs publics sont contraints de hiérarchiser les projets à mettre en œuvre. Il leur faut trouver les aptitudes pour innover avec discernement, notamment en sélectionnant les outils qui apportent une réelle valeur ajoutée au service rendu aux citoyens.

La démocratisation de l'utilisation de l'intelligence artificielle dans les services publics soulève par ailleurs des questions sur les plans éthique et opérationnel. Il est primordial d'encadrer son déploiement, de veiller à la transparence des algorithmes, et de s'assurer que son usage est compatible avec les principes d'équité, de neutralité et d'intérêt général.

D. Développer la cybersécurité

L'augmentation de la récurrence des cyberattaques contre les institutions publiques impose une réponse systémique. Les systèmes centraux ne sont pas les seuls à devoir être protégés, et c'est l'ensemble de la chaîne qui doit être sécurisé, des grandes administrations aux plus petites collectivités locales, souvent moins armées face aux risques. (…)

E. Simplifier les démarches tout en garantissant l'inclusion

Dans leur volonté de moderniser les services, les administrations doivent veiller à ne pas complexifier davantage les démarches pour les usagers. La simplification passe par une transformation profonde des process internes, soutenue par des outils numériques ergonomiques, interopérables, et conçus pour tous les profils d'utilisateurs, y compris ceux qui sont moins familiers avec le numérique.

(…)

Pour conclure :

La souveraineté numérique est plus que jamais une nécessité opérationnelle, stratégique et démocratique pour les services publics. Face à la complexité des environnements numériques, à la dépendance aux acteurs extraterritoriaux et à l'évolution rapide des usages, il devient impératif pour les institutions publiques de reprendre la maîtrise de leurs outils, de leurs données, et plus globalement du champ du numérique.

(...)

DOCUMENT 7

Souveraineté numérique : les collectivités locales se libèrent des GAFAM grâce à l'open source

03/07/2025

Un véritable mouvement de fond s'observe depuis peu : de plus en plus de collectivités locales (villes, régions…) en France et en Europe disent adieu aux logiciels des géants du numérique américains (les GAFAM) pour adopter des solutions **open source**. Ce virage n'est pas anodin : il répond à des enjeux stratégiques de **souveraineté numérique**, de sécurité des données et d'indépendance technologique. La ville de Lyon, par exemple, a annoncé en juin 2025 une transformation majeure de ses outils numériques afin de **ne plus dépendre des solutions logicielles états-uniennes**. Cette tendance touche aussi d'autres acteurs publics (ministères, régions) et même des entreprises privées soucieuses de reprendre le contrôle de leurs données. Pourquoi un tel **exode loin des GAFAM** ? Comment ces organisations parviennent-elles à basculer vers l'open source ? Quels **gains** en retirent-elles et quels **risques** doivent-elles anticiper ? Nous vous proposons un tour d'horizon détaillé et technique de cette évolution.

Pourquoi abandonner les solutions des GAFAM ?

Souveraineté, loi et contrôle des données

Le premier moteur de ce « désengagement » est la quête de **souveraineté numérique**. En utilisant des logiciels propriétaires américains (Microsoft 365, Google Workspace, etc.), les organisations européennes s'exposent à la **juridiction extraterritoriale** des États-Unis. En effet, des lois comme le Cloud Act ou le FISA (héritier du Patriot Act) permettent aux autorités américaines d'accéder aux e-mails, documents et bases de données d'une organisation française hébergés sur des serveurs Microsoft, Google ou autres, **sans recours possible de la France**. Cela pose un sérieux problème de **confidentialité** et de **souveraineté des données** : des informations sensibles (données personnelles de citoyens, documents stratégiques, recherches) pourraient être consultées par un gouvernement étranger sans autorisation. Pour une collectivité ou une entreprise traitant des données critiques, c'est inacceptable.

Au-delà du risque juridique, dépendre de suites américaines signifie **perdre la maîtrise de l'infrastructure et du stockage**. Où sont hébergées nos données ? Qui y a accès ? En choisissant des alternatives open source hébergées localement ou sur des clouds souverains, les collectivités s'assurent de **décider où et comment leurs données sont stockées et protégées**. Par exemple, le Land allemand du Schleswig-Holstein a entrepris de migrer ses données vers un cloud public allemand plutôt que d'utiliser les services de Microsoft ou Google. Cet enjeu de contrôle a été mis en lumière par les tensions géopolitiques récentes : les relations UE–USA, la guerre en Ukraine, etc., ont rappelé l'importance de ne pas dépendre d'acteurs étrangers pour des ressources stratégiques (énergie hier, numérique aujourd'hui).

Enfin, les pouvoirs publics cherchent à **garantir la conformité au RGPD** et aux doctrines nationales de sécurité. En France, la doctrine Cloud de l'État exige que les données sensibles des administrations soient hébergées par des solutions certifiées SecNumCloud (sécurisées et

hors portée juridique non-UE). Or, les suites collaboratives américaines ne respectent pas ce critère de « cloud de confiance ». Passer à des logiciels libres ou des clouds européens permet de mieux se conformer à ces exigences légales et de **protéger la vie privée des citoyens**.

Indépendance technologique et économique

Le deuxième grand motif, c'est de **sortir d'une dépendance technico-économique** de plus en plus contraignante. Les GAFAM pratiquent le *vendor lock-in* : une fois qu'une organisation a adopté leur écosystème (Windows + Office + Teams, ou Google Docs + Gmail, etc.), **s'en affranchir semble complexe et coûteux**. Les outils sont interconnectés, les données piégées dans des formats propriétaires… Cette captivité numérique peut durer des années si l'on ne fait rien, avec à la clé une **dépendance subie aux décisions du fournisseur**.

Dépendre d'un seul éditeur présente aussi un **risque financier**. Microsoft, pour ne citer que lui, profite de sa position dominante pour augmenter régulièrement ses tarifs en Europe. Dernièrement, l'intégration de fonctionnalités d'IA a servi de prétexte à une hausse de prix pouvant aller **jusqu'à +43 % sur l'abonnement Microsoft 365**. À chaque nouvelle version, certaines options gratuites disparaissent, poussant les administrations à payer toujours plus. Ces hausses imprévues pèsent sur les budgets publics, comme l'a souligné un expert : « Les administrations se retrouvent parfois prises à la gorge » par les coûts des licences propriétaires. Au contraire, les logiciels libres n'imposent pas de licence payante par poste ; les dépenses se limitent au support, à la maintenance et à la formation, ce qui s'avère bien souvent **moins coûteux sur le moyen terme**. Le Land de Schleswig-Holstein anticipe ainsi **plusieurs dizaines de millions d'euros d'économies** en passant à l'open source.

Au-delà des coûts, il y a aussi un **risque géopolitique** à cette dépendance. En cas de tensions internationales ou de changement de politique aux États-Unis, un éditeur comme Microsoft pourrait restreindre l'accès à ses services, ou appliquer des conditions désavantageuses aux clients européens. Ce scénario peut sembler extrême, mais il est évoqué sérieusement depuis le retour de Donald Trump à la Maison Blanche en 2025. Dans ce contexte, de nombreuses collectivités préfèrent **prendre les devants** : ne plus mettre tous leurs œufs dans le même panier technologique et **diversifier leurs outils**. Cela s'inscrit d'ailleurs dans une dynamique européenne plus large : l'Union européenne encourage le développement de capacités numériques souveraines et la réduction de la dépendance aux fournisseurs extra-européens. L'Agence nationale de la cohésion des territoires en France finance par exemple des suites collaboratives libres pour les collectivités afin de **stimuler une offre locale** et indépendante.

Sécurité, transparence et innovation

Contrairement à une idée reçue, les logiciels libres offrent des garanties en matière de **sécurité et de transparence**. Le code source étant ouvert et auditable, une communauté d'utilisateurs et de développeurs peut repérer et corriger rapidement les failles, assurant une protection robuste de l'outil. Pour les collectivités, cette transparence est un **gage de confiance** vis-à-vis des citoyens : une ville qui passe à des logiciels libres **offre à ses habitants une visibilité sur les algorithmes utilisés** dans les services publics. Cela rejoint un impératif démocratique : expliquer les traitements automatisés et algorithmes qui prennent des décisions (par exemple dans l'attribution de prestations sociales, le calcul des impôts, etc.). Avec du code ouvert, il devient possible de vérifier le fonctionnement des logiciels publics, ce qui **renforce la confiance et la redevabilité**.

L'open source rime aussi avec **interopérabilité** et **pérennité**. Les formats ouverts garantissent un accès à long terme aux documents et données, sans risque de se retrouver avec des fichiers illisibles suite à l'abandon d'un logiciel propriétaire. Pour l'archivage historique des collectivités, c'est un atout important : conserver la maîtrise de ses données sur des décennies, voire plus, en pouvant toujours relire les contenus car on dispose du code source et des formats ouverts nécessaires. De plus, une collectivité peut mutualiser ses efforts avec d'autres autour d'un même outil libre : par exemple développer en commun une application qui servira à plusieurs villes (portail citoyen, système de délibérations, etc.), ce qui **répartit les coûts et profite à tout un réseau d'utilisateurs**.

Enfin, adopter les logiciels libres encourage l'**innovation locale**. Plutôt que d'acheter une solution clé-en-main à un géant étranger, les collectivités qui investissent dans l'open source collaborent souvent avec des PME locales, des éditeurs nationaux ou la communauté open source. Cela développe les **compétences internes** (on devient acteur du logiciel, pas simple client passif) et soutient l'**écosystème numérique local**. La France et l'Europe ne manquent pas de talents dans le domaine : en privilégiant ces solutions, le secteur public agit comme un moteur pour faire émerger des alternatives compétitives. D'ailleurs, l'État français a lancé **La Suite Numérique**, un projet collaboratif open source à destination des agents publics, montrant bien la volonté d'offrir une **alternative souveraine** aux outils collaboratifs privés. De même, l'Allemagne a voté une loi imposant aux administrations fédérales de **privilégier le logiciel libre** dans leurs achats informatiques, et la Suisse exige désormais que tout nouveau logiciel développé pour l'État voie son code source publié (sauf exception de sécurité). Ces exemples soulignent que le logiciel libre est désormais considéré comme un pilier stratégique de la souveraineté numérique en Europe.

Comment opérer la transition vers l'open source ?

Convaincre de la nécessité de changer est une chose, **passer à l'acte** en est une autre ! Migrer tout un parc informatique et des milliers d'utilisateurs vers de nouveaux outils représente un **défi technique et humain**. Cependant, plusieurs collectivités pionnières ont montré la voie, fournissant des **retours d'expérience** précieux sur le « comment ».

Choisir des alternatives libres performantes et compatibles

La première étape est d'identifier les **solutions open source équivalentes** pour chaque usage aujourd'hui couvert par un logiciel propriétaire. Bonne nouvelle : en 2025, il existe des alternatives libres matures pour **tous les besoins courants** :

- **Systèmes d'exploitation** : Remplacer Windows par une distribution Linux adaptée. Par exemple, la ville de Lyon a commencé à déployer Linux sur les postes de travail municipaux à la place de Windows. En Allemagne, le Land de Schleswig-Holstein prévoit également d'abandonner Windows pour Linux d'ici quelques années, après une phase initiale centrée sur la bureautique.
- **Suite bureautique (Office)** : Remplacer Microsoft Office (Word, Excel, PowerPoint…) par une suite libre telle que **LibreOffice** ou **OnlyOffice**. Lyon a opté pour OnlyOffice pour ses agents, tandis que le ministère du Numérique danois a commencé à déployer LibreOffice en 2025 sur la moitié de ses postes, avec l'objectif de l'imposer partout d'ici fin 2025. Ces suites libres permettent de créer des documents texte, tableurs et présentations tout en assurant une **compatibilité avec les formats Microsoft** (DOCX, XLSX, etc.). OnlyOffice, par exemple, offre une

interface proche d'Office et une bonne prise en charge des fichiers Office pour faciliter la transition.

- **Messagerie et agenda** : Remplacer Outlook/Exchange. Des solutions open source existent, comme **Thunderbird** (client mail) couplé à un serveur tel que **BlueMind**, **Zimbra** ou **Open-Xchange** pour la gestion du courrier, des calendriers et contacts en mode collaboratif. Le Schleswig-Holstein a retenu l'ensemble Open-Xchange + Thunderbird pour remplacer Outlook. Ces outils permettent d'assurer la continuité du service de messagerie interne et la synchronisation des agendas, souvent via des protocoles ouverts (IMAP, CalDAV…).
- **Stockage de fichiers et collaboration** : Remplacer OneDrive/SharePoint ou Google Drive par des solutions comme **Nextcloud** ou **Seafile**. Nextcloud, en particulier, est très populaire en Europe pour créer un cloud privé ou hybride : il offre partage de fichiers, synchronisation multi-appareils, co-édition de documents en ligne, messagerie instantanée, etc., avec de nombreux **modules additionnels**. Le Land de Schleswig-Holstein utilise Nextcloud comme substitut à SharePoint, et la ville de Lyon déploie également une plateforme collaborative basée sur Nextcloud et d'autres composants libres dans le cadre de son projet Territoire Numérique Ouvert.
- **Visioconférence et messagerie d'équipe** : Remplacer Teams, Zoom ou Google Meet par des outils libres tels que **Jitsi** (visioconférence), **BigBlueButton** (conférences en ligne, e-learning) ou **Mattermost** / **Element (Matrix)** pour la messagerie instantanée d'équipe. La suite **Territoire Numérique Ouvert (TNO)** développée pour les collectivités lyonnaises repose justement sur un bouquet d'outils open source couvrant la visioconférence et la co-édition bureautique. Cette suite collaborative libre, hébergée dans des datacenters de la région Auvergne–Rhône-Alpes, propose des **fonctions comparables** à Microsoft 365 (visioconf, partage de documents, édit docs en ligne) tout en étant **interopérable** avec les formats standard.
- **Applications métiers** : C'est un volet parfois invisible pour le public, mais les collectivités utilisent de nombreux logiciels métiers (gestion financière, ressources humaines, élections, cartographie SIG, etc.). Là aussi, il existe souvent des solutions libres ou *open source* soutenues par des communautés ou associations (par exemple, l'ADULLACT propose des logiciels libres pour les besoins spécifiques des mairies : gestion d'état-civil, cimetière, listes électorales, etc.). Au besoin, les collectivités peuvent même **développer en interne** ou en groupement une application sur-mesure, dont le code sera partagé et mutualisé. Cette approche collaborative est facilitée par le modèle open source, comme le montre le cas de Lyon et du **SITIV** (syndicat informatique regroupant plusieurs villes) qui ont co-développé Territoire Numérique Ouvert pour en faire bénéficier d'autres communes.

L'important est donc de **cartographier les besoins** et d'identifier pour chaque brique propriétaire l'équivalent libre approprié. Dans la plupart des cas, on trouve son bonheur dans l'écosystème libre, parfois en acceptant quelques ajustements (un logiciel unique GAFAM pouvant être remplacé par **plusieurs** outils spécialisés côté libre). Ce travail de sélection peut s'appuyer sur des ressources comme le *Socle Interministériel de Logiciels Libres (SILL)* publié par l'État, qui liste des logiciels libres recommandés pour chaque usage au sein des administrations. On bénéficie ainsi du recul d'autres utilisateurs publics avant de faire son choix.

(…)

Bénéfices et risques d'un passage à l'open source

Pour récapituler, faisons le point sur les principaux **gains attendus** d'une telle transition, ainsi que sur les **risques ou écueils** à surveiller.

Les bénéfices majeurs :

- **Souveraineté et conformité :** Reprise de contrôle sur les données et les outils, élimination du risque de voir des données sensibles aspirées par une puissance étrangère. Hébergement local ou national garantissant le respect du RGPD et des normes de sécurité nationales. On n'est plus prisonnier des lois extraterritoriales comme le Cloud Act.
- **Indépendance technologique :** Fin du **verrouillage fournisseur**. La collectivité n'est plus à la merci des changements de politique ou des hausses de prix d'un éditeur unique. Elle peut faire évoluer ses outils comme elle l'entend (code source ouvert) et changer de prestataire de support si besoin – ce qui introduit de la **concurrence saine** là où le monopole régnait.
- **Économies financières :** Réduction notable des coûts de licences. Par exemple, la région Occitanie a **divisé par quatre sa facture annuelle** en remplaçant Microsoft 365 par une solution open source. De son côté, le Land de Schleswig-Holstein estime qu'il économisera **des dizaines de millions d'euros** à moyen terme en abandonnant Microsoft. Même s'il faut investir au départ (formations, migration), l'investissement est rentabilisé sur la durée par l'absence de redevances logicielles récurrentes.
- **Allongement de la durée de vie du matériel :** Les systèmes libres (Linux, suites libres) sont souvent moins gourmands en ressources ou permettent d'optimiser l'existant, d'où une **durée de vie prolongée pour les PC**. Lyon a explicitement mis en avant cet objectif de prolonger ses équipements pour réduire son empreinte environnementale. En effet, ne plus être forcé de suivre le cycle imposé (ex : remplacement de PC car Windows 10 n'est plus supporté) permet d'éviter du gaspillage et de réduire les **déchets électroniques**.
- **Transparence et confiance :** Code source auditable par tous, ce qui renforce la confiance du public dans les services numériques. La population peut savoir quels algorithmes traitent leurs données, et même des développeurs locaux peuvent contribuer à améliorer les outils publics. Cela crée une **dynamique citoyenne positive** autour du numérique.
- **Innovation et développement local :** En faisant travailler des acteurs locaux sur des projets open source, les collectivités stimulent l'**économie locale** du numérique. Lyon a attribué la moitié de son projet collaboratif à des entreprises de sa région. On assiste ainsi à la création d'un cercle vertueux : l'argent public investi reste en grande partie dans le tissu économique local, et le produit développé peut être réutilisé ailleurs (logique de communs numériques). De plus, les équipes internes gagnent en compétence en participant à ces projets.
- **Interopérabilité et standards ouverts :** Fini les formats fermés qui créent des incompatibilités (combien de collectivités ont souffert de documents Word impossibles à ouvrir dans une ancienne version…). Avec l'open source, l'adoption de **standards ouverts** (tels que le format OpenDocument/ODF pour les textes, tableurs, etc.) assure une meilleure interopérabilité entre les systèmes et sur la durée. On peut dialoguer plus facilement avec d'autres partenaires, et même les citoyens peuvent utiliser des formats ouverts pour leurs démarches.

- **Sécurité renforcée :** Contrairement au cliché du « logiciel libre non sécurisé », de nombreux projets libres sont extrêmement sûrs grâce à la réactivité de leur communauté. Les failles peuvent être identifiées par **des milliers d'yeux** et corrigées rapidement, sans attendre le bon vouloir d'un éditeur. Par ailleurs, on élimine le risque de **porte dérobée cachée** dans un code propriétaire. Bien sûr, il faut mettre en place une politique de mises à jour régulières, mais c'est aussi le cas avec des logiciels propriétaires.

Les risques et défis :

- **Résistance au changement et conduite du projet :** C'est sans doute le principal défi. Changer les habitudes de travail de milliers d'agents publics ou d'employés est un **chantier humain** délicat. Si le projet est imposé sans pédagogie ni accompagnement, il peut échouer face aux réticences (« Pourquoi changer ce qui marche ? ») ou par découragement des utilisateurs. Il est donc crucial de prévoir un **volet d'accompagnement solide** (comme évoqué plus haut). Cela demande du temps, de la communication et du soutien de la hiérarchie. Le risque sinon est une fronde interne ou une démotivation, ce qui peut paralyser le bon fonctionnement des services.
- **Compatibilité des fichiers et fonctionnalités spécifiques :** Même si les suites libres lisent les formats Microsoft, il peut subsister des **problèmes de mise en forme** sur des documents Office complexes (par exemple des macros Excel très élaborées, des documents Word avec VBA, etc.). Ces cas particuliers doivent être anticipés. Parfois, il faudra adapter les macros dans LibreOffice ou trouver des solutions alternatives. Les **outils métiers** périphériques (ex : un logiciel qui s'interface avec Excel via des macros) peuvent aussi ne plus fonctionner tel quel. Il faut donc prévoir soit de conserver quelques postes avec Office pour ces usages précis, soit de financer le développement de nouvelles macros/scripts compatibles. Autrement dit, **la transition technique doit être étudiée en détail** pour éviter les pertes de données ou de fonctionnalités critiques.
- **Montée en compétence et support technique** : Passer à l'open source implique d'**internaliser plus de compétences** ou de s'appuyer sur de nouveaux prestataires. On ne peut plus appeler la hotline Microsoft en cas de souci ; à la place, il faut soit avoir une équipe technique interne capable de comprendre et résoudre les problèmes, soit un contrat de support avec une société open source. Cela nécessite potentiellement des formations techniques pour les équipes IT, et une réorganisation du support. Ce n'est pas forcément un inconvénient (on gagne en maîtrise), mais c'est un changement à bien gérer. Le risque sinon est de se retrouver bloqué sur un bug faute de savoir qui peut le corriger rapidement.
- **Choix et pérennité des solutions** : L'écosystème libre est foisonnant, ce qui est positif, mais cela implique de **choisir les bons outils** (ceux qui seront pérennes, bien supportés, évolutifs). Une collectivité pourrait être tentée par un petit logiciel libre très innovant, mais si la communauté derrière est minuscule ou le projet peu actif, il y a un **risque de pérennité**. Il faut donc évaluer la **viabilité à long terme** des solutions (communauté active, versions à jour, intégrateurs disponibles…). En pratique, les collectivités pionnières se tournent vers des projets déjà éprouvés (LibreOffice, Linux, Nextcloud, etc.) justement pour minimiser ce risque.
- **Coûts de transition à court terme** : Paradoxalement, si les économies sont au rendez-vous ensuite, il ne faut pas négliger que **migrer a un coût initial**. Déployer de nouveaux serveurs, migrer des dizaines de milliers de comptes utilisateurs, convertir éventuellement des fichiers, former les agents – tout cela représente un investissement.

Il peut être significatif (plusieurs millions d'euros pour une grande ville par exemple). Il faut donc un **soutien financier** et politique fort au départ. De plus, pendant la transition, certains coûts sont doublés (on paye encore les anciennes licences le temps du chevauchement, tout en finançant le nouveau). C'est un passage obligé, mais qu'il faut planifier budgétairement. Le risque sinon est d'avoir une pression financière qui vienne interrompre le projet en cours de route.

- **Risques organisationnels et politiques** : Un projet de cette ampleur doit absolument avoir le **soutien de la direction** et des élus. Si un changement de majorité politique ou de direction survient et que le soutien disparaît, le projet peut être remis en cause. On se souvient du cas de la ville de Munich qui, après des années en Linux, était partiellement revenue en arrière suite à un changement politique. Ce genre de revers peut arriver si la décision n'est pas solidement ancrée ou si les utilisateurs se plaignent trop. D'où l'importance d'aligner tout le monde sur les objectifs (souveraineté, économies) et de marquer des succès rapides pour **valider la démarche**.

En somme, les risques liés à l'abandon des GAFAM sont **gérables** à condition d'anticiper et d'accompagner la transition. Les bénéfices, eux, sont de taille et s'inscrivent dans une vision à long terme. Pour beaucoup de collectivités et d'organisations, le jeu en vaut largement la chandelle. Comme le souligne Dirk Schrödter, ministre du Numérique du Schleswig-Holstein, les développements géopolitiques et les enjeux de souveraineté ont rendu cette stratégie non seulement souhaitable, mais nécessaire : *« Les développements récents ont renforcé l'intérêt pour notre approche, surtout en Europe »*.

(...)

Les enjeux au long cours de la souveraineté en matière d'IA

11 juillet 2025 - Localtis

La Commission supérieure du numérique et des postes a organisé le 10 juillet 2025 un débat sur la souveraineté en matière d'IA. Il en ressort que l'autonomie stratégique à laquelle aspirent les élus ne pourra être atteinte qu'en agissant sur l'ensemble de la chaine de valeur de l'IA. Et une fois de plus, le rôle de la commande publique pour consolider l'écosystème européen a été souligné.

En matière de souveraineté numérique, l'intelligence artificielle tient une place singulière. La domination sino-américaine y est en effet particulièrement marquée mais à la différence de ce qui s'est passé pour l'informatique, l'Europe et la France ont (encore) quelques cartes en mains pour atteindre a minima "une autonomie stratégique", sous réserve d'actionner les bons leviers. S'y ajoute une réelle prise de conscience des décideurs, à l'image de la création toute récente d'un "**indice de résilience numérique**" pour mesurer les dépendances numériques des entreprises. C'est ce qu'il ressort d'un colloque organisé le 10 juillet 2025 par la **commission supérieure du numérique et des postes (CSNP)** sur la **souveraineté de l'IA**.

Agir sur toute la chaine de valeur

Guillaume Avrin, coordonnateur national pour l'intelligence artificielle qui vient de rejoindre le privé, a introduit les débats en insistant sur la nature "holistique" de la souveraineté appliquée à l'IA. C'est en effet sur l'ensemble de la chaine de valeur qu'il faut agir, de la production d'électricité décarbonée aux datacenters en passant par les puces de l'IA, les bases d'entrainement, les algorithmes et les compétences nécessaires pour créer des modèles de fondation souverains.

L'ancien haut fonctionnaire a souligné les acquis de la stratégie gouvernementale mise en œuvre depuis 2018. La France compte désormais des "**hubs territoriaux**" associant chercheurs et industriels et quelque 600 startups de l'IA dont **Mistral** (génération de texte) et **Photoroom** (génération d'images). Avec l'appui de l'Europe, l'Etat s'est engagé à créer des "communs" à la disposition de l'écosystème, à l'image d'**Atlt-Edic** pour entrainer des IA sur un corpus linguistique européen. Guillaume Avrin estime cependant qu'il manque encore un "airbus de l'IA", chaque pays européen ayant tendance à promouvoir ses leaders nationaux alors qu'"une interdépendance européenne est préférable à une indépendance totale". Dans les acquis, il y a aussi les 109 milliards d'investissement sur les datacenters annoncés lors du sommet de l'IA, dont "17 milliards ont été depuis confirmés". L'objectif de l'Etat est de réduire la dépendance de l'Europe aux capacités de calcul américaines en faisant grimper le parc de machines européennes équipées en GPU (puce indispensable à l'IA) de 3% à 20%.

Défis spécifiques à l'IA générative

La souveraineté en matière d'IA implique également que les **systèmes soient auditables** et leurs résultats explicables, garantie de leur sécurité. Or, ce défi est loin d'être simple pour les IA génératives car elles sont fondées sur une **approche statistique et probabiliste**. "Comme

on n'arrive pas à décomposer mathématiquement ces systèmes, nous ne savons pas comment ils prennent leurs décisions", explique Alix Durand, cheffe d'état-major adjointe de l'Anssi. Ces IA génèrent par ailleurs de nouvelles menaces avec les risques "d'empoisonnement" ou "d'extraction de données confidentielles" des bases d'entrainement. Des défis qui ont conduit l'Etat à créer en février 2025 l'**Institut national pour l'évaluation et la sécurité de l'intelligence artificielle**. Plus récemment, l'Anssi et la Cnil ont annoncé l'initiative Paname pour développer un outil évaluant la conformité des IA au RGPD. Si certains risques sont spécifiques aux IA, la représentante de l'Anssi insiste sur le fait que "les règles usuelles de sécurité informatique s'appliquent aux systèmes d'IA".

La commande publique comme levier

La **commande publique** émerge ensuite comme un instrument privilégié pour développer l'écosystème français d'IA et notamment une IA open source respectueuse des valeurs éthiques et environnementales européennes.

Dans ce domaine, l'Etat n'a pas toujours montré l'exemple, avec notamment l'affaire du **Health data hub** hébergé dans le cloud de Microsoft en 2019 du fait de l'absence supposée d'alternative. L'épisode est cependant en voie de se clore. "L'appel d'offres a été publié la semaine dernière pour trouver une solution souveraine intercalaire", a annoncé **David Sainati** en charge de la Délégation au numérique en santé. Avec au passage un énorme gâchis d'argent public puisque les serveurs du HDH n'ont finalement jamais hébergé les données de l'assurance maladie du fait des risques induits par le cloud act américain…

Les administrations, et particulièrement les collectivités, ont par ailleurs du mal à acheter européen, la législation ne permettant pas d'intégrer un critère local. Guillaume Avrin incite les administrations à insérer des critères environnementaux sur leurs achats de cloud et d'IA, les serveurs tournant aux USA étant "11 fois plus émetteurs de GES que les européens" du fait du recours massif à de l'électricité tournant aux énergies fossiles. La piste des centrales d'achat est également évoquée pour faciliter l'acquisition de solutions innovantes par les petites collectivités, sous réserve que les centrales comme l'**Ugap** offrent des conditions adaptées aux startups. Un sujet qui fait l'objet de propositions de la mission sénatoriale sur l'achat public.

Un cadre réglementaire à clarifier

La loi peut enfin contribuer à bâtir une IA souveraine mais force est de constater que ce cadre juridique est encore perfectible. "Tous les décrets de la loi SREN ne sont pas encore parus, notamment sur le cloud", a constaté la députée **Anne Le Henanff**.

Quant à l'**IA Act européen**, entré en vigueur il y a un an, les dispositions sur les IA génératives viennent tout juste d'être connues et celles sur les IA à haut niveau de risque ne le seront pas avant août 2026. "Aujourd'hui, on est dans le flou sur l'application de l'IA Act", reconnait Alexandra Iteanu. L'avocate spécialisée déplore également les nombreux renvois du texte à des "normes techniques" qui ne seront pas discutées par les instances politiques. Plus problématique encore, l'absence de régime de responsabilité. "Qui va être responsable quand on utilise un outil d'IA ? L'utilisateur ? Le fournisseur ? Le déployeur ?", s'interroge l'avocate. En attendant, cette carence réglementaire favorise de facto les acteurs dominant le marché, qui imposent leurs conditions contractuelles. "Dans les contrats sur les outils d'IA américains, la responsabilité est limitée, voire quasi exclue", dénonce Alexandra Iteanu. Enfin, l'articulation

de l'IA Act avec d'autres réglementations comme NIS 2 ou le Cyber Resilience Act reste à définir.

Un indice de résilience numérique pour mesurer les dépendances

Lors des Rencontres économiques d'Aix-en-Provence le 4 juillet 2025, un collectif d'acteurs économiques et d'experts a annoncé la création de l'indice de résilience numérique (IRN), pour mesurer et aider à réduire les dépendances technologiques du continent. Celle-ci coûte en effet **265 milliards d'euros aux entreprises** selon le Cigref, avec une majeure partie des **dépenses dirigée vers les États-Unis**.

L'IRN évalue la résilience numérique selon 8 critères répartis en deux catégories. Les critères quantitatifs mesurent la répartition géographique des dépenses informatiques, la localisation du stockage des données, le degré d'ouverture des technologies utilisées et la diversification des fournisseurs. Les critères qualitatifs analysent l'appropriation managériale des risques, la préparation aux chocs numériques, le suivi réglementaire et l'autonomie des compétences internes.

Un appel est lancé aux organisations pour valider la méthodologie avant le déploiement généralisé prévu pour 2026. L'IRN s'accompagnera d'un **Baromètre de souveraineté numérique** qui mesurera secteur par secteur les manques et axes d'amélioration.

Performance
MARKETING EXPERT

DOCUMENT 9

SecNumCloud : certification française pour le cloud souverain

25 décembre 2025

La **certification SecNumCloud** représente une réponse française aux enjeux de souveraineté numérique dans un contexte géopolitique tendu. Lancée officiellement en 2022 par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), cette certification vise à garantir que les services cloud respectent des critères stricts de sécurité et de souveraineté française. Face aux préoccupations croissantes concernant la protection des données sensibles et l'indépendance technologique européenne, SecNumCloud s'impose comme un référentiel exigeant pour les prestataires cloud souhaitant héberger des **données sensibles de l'État français**, incluant les informations classifiées jusqu'au niveau « confidentiel défense ».

Fondements et objectifs de la certification SecNumCloud

SecNumCloud constitue une certification française de sécurité pour les services cloud, délivrée par l'ANSSI, qui garantit que les prestataires respectent des critères stricts de souveraineté, sécurité et conformité légale française. Cette initiative s'inscrit dans une démarche plus large de **protection de la souveraineté numérique** française face aux géants technologiques américains et chinois.

Le référentiel SecNumCloud impose des exigences techniques et organisationnelles particulièrement strictes. Les prestataires candidats doivent démontrer leur capacité à protéger les données contre tout accès non autorisé, y compris de la part d'États tiers. Cette protection s'étend aux métadonnées, aux journaux d'audit et aux clés de chiffrement, qui doivent rester sous contrôle français en permanence.

L'ANSSI exige un **audit annuel obligatoire** pour maintenir la certification, garantissant une surveillance continue de la conformité. Cette approche diffère des certifications internationales classiques en intégrant explicitement des considérations géopolitiques dans les critères d'évaluation. Les prestataires doivent notamment prouver qu'ils ne sont pas soumis à des législations extraterritoriales susceptibles de compromettre la confidentialité des données françaises.

La certification couvre l'ensemble de la chaîne de valeur du cloud, depuis l'infrastructure physique jusqu'aux applications métier. Cette approche holistique permet d'identifier et de maîtriser tous les points de vulnérabilité potentiels, créant un **écosystème cloud de confiance** pour les administrations et entreprises stratégiques françaises.

(…)

Investissement et souveraineté numérique : le défi de 2026

Publié le 24/05/2026

L'essentiel à retenir : la France doit mobiliser 105 milliards d'euros pour son IA afin de pallier un retard de financement abyssal face aux États-Unis. Ce déficit de capitaux domestiques menace le contrôle des data centers et des données stratégiques. Transformer l'épargne longue en investissements productifs est vital pour garantir une autonomie technologique et sécuritaire durable en 2026.

L'Europe ne capte que 5 % du capital-risque mondial contre 52 % pour les États-Unis, laissant la France face à un **manque de 105 milliards d'euros pour financer ses infrastructures technologiques**. Ce déficit de capitaux d'investissement à long terme fragilise le déploiement de l'intelligence artificielle et la construction de centres de données sur notre sol.

Votre autonomie numérique est menacée par cette dépendance aux fonds étrangers pour sécuriser vos données stratégiques. Nous allons analyser les solutions de financement et les leviers d'épargne longue pour **garantir votre souveraineté numérique**.

Souveraineté numérique et déficit de capitaux : l'état des lieux en 2026

La France accuse un manque de fonds de pension pour financer les 105 milliards d'euros nécessaires à son IA. Sans capitaux domestiques massifs, la **maîtrise des données et des infrastructures stratégiques reste vulnérable**, imposant de sécuriser les trois piliers technologiques.

Mais au-delà de l'argent, la **question physique des serveurs devient un enjeu de sécurité nationale**.

Les trois piliers de l'autonomie technologique

L'indépendance de l'État repose sur trois piliers indissociables : les données, les infrastructures physiques et les logiciels. Sans cette triade complète, **la souveraineté nationale s'effrite** face aux puissances technologiques mondiales dominantes.

La cybersécurité constitue le socle indispensable pour **protéger les actifs nationaux et les systèmes critiques**. Elle permet de promouvoir et protéger la souveraineté numérique de l'UE face aux menaces extérieures croissantes.

La **localisation physique des serveurs est désormais une priorité absolue**. La géopolitique actuelle dicte ces choix techniques stratégiques.

Analyse du retard de financement face aux modèles étrangers

Le modèle français souffre d'un **manque d'épargne longue** par rapport au système anglo-saxon. Arthur Mensch, fondateur de Mistral, regrette cette faible profondeur financière. Pour comprendre ce défi, il faut analyser le nouveau paradigme économique actuel.

La dépendance est réelle car **75% des entreprises technologiques européennes se refinancent hors de l'Union européenne**. Cette situation est documentée par le Fonds européen pour la souveraineté numérique.

Le financement local est le nerf de la guerre. Sans capitaux propres, **le contrôle nous échappe**.

Mais au-delà de l'argent, la question physique des serveurs devient un enjeu de sécurité nationale immédiat.

Infrastructures critiques et data centers : les besoins capacitaires de 2026

Le **contrôle du matériel** constitue la seconde ligne de front pour garantir l'autonomie des données françaises.

Localisation des serveurs et puissance de calcul

L'hébergement local neutralise l'application des lois extraterritoriales. Le Cloud Act américain demeure une menace constante pour la confidentialité. La **France doit impérativement posséder ses propres murs physiques**.

L'entraînement des modèles d'intelligence artificielle exige une infrastructure robuste. Cette puissance de calcul nécessite des **processeurs haute performance installés directement sur notre sol**.

Selon l'Agefi, les investisseurs privilégient désormais la **localisation géographique des données**. Le contrôle physique des serveurs est devenu un élément indispensable de sécurité.

Atout nucléaire et gestion de l'énergie

Le parc nucléaire français offre un **avantage compétitif stratégique**. Cette électricité décarbonée permet d'alimenter des centres massivement énergivores. Les géants technologiques sont attirés par cette ressource stable.

Le **refroidissement liquide devient la norme** pour les installations haute densité. Ces systèmes exigent une ingénierie thermique complexe pour évacuer la chaleur des processeurs.

Les délais de raccordement électrique représentent toutefois un **défi majeur**. Le temps industriel nécessaire aux infrastructures ne suit pas toujours l'immédiateté du numérique.

Cycle de vie des actifs et innovations prospectives

Le bâti immobilier pérenne s'oppose à l'obsolescence rapide des puces électroniques. Le hardware se renouvelle tous les deux ans. L'infrastructure globale doit donc rester **modulaire**.

Les recherches sur les data centers orbitaux progressent actuellement. Cette piste futuriste pourrait assurer une **résilience accrue face aux risques terrestres**.

La souveraineté se gagne par une avance technologique constante et durable. L'investissement dans ces actifs constitue **l'atout patrimoine stratégique** de la décennie à venir.

Pour bâtir ces cathédrales numériques, la France doit maintenant **mobiliser des leviers financiers inédits**.

Leviers financiers et épargne longue : les solutions de financement en 2026

L'enjeu est de transformer l'épargne dormante des Français en un **moteur de croissance technologique**.

Rôle des fonds de pension et de la capitalisation

Le débat sur la retraite par capitalisation s'intensifie. Ces fonds stabiliseraient le capital de nos entreprises. **Les modèles nordiques prouvent leur efficacité** face aux marchés financiers mondiaux.

L'épargne longue finance l'innovation technologique de pointe. C'est un levier contre la prédation étrangère. La France doit **créer ses propres véhicules d'investissement massifs**. Il faut éviter la décote de retraite pour illustrer les enjeux de capitalisation.

La volonté politique est ici déterminante. **Le financement stratégique en dépend directement**.

Partenariats publics et montages financiers hybrides

Bpifrance joue un rôle central dans l'accompagnement des start-ups. La Caisse des Dépôts accompagne les projets régionaux d'envergure. Ces acteurs publics sont des **catalyseurs de confiance pour les investisseurs**.

Les financements hybrides se multiplient désormais. Mêler dette privée et fonds propres attire les institutionnels. Les **data centers deviennent une classe d'actifs prisée**.

Selon l' Institut Montaigne, la diversification des sources reste vitale. La **souveraineté numérique française nécessite une vigilance constante**.

Cependant, l'argent ne suffit pas sans un **cadre normatif protégeant nos intérêts et nos valeurs**.

Cadre réglementaire et cybersécurité : les normes de résilience de 2026

La régulation devient une **arme de défense face à la concurrence déloyale** des plateformes étrangères.

Certification SecNumCloud et confiance numérique

Le label SecNumCloud de l'ANSSI qualifie les prestataires de services cloud. Cette certification **garantit une sécurité maximale** pour les secteurs sensibles. Elle assure une protection rigoureuse contre les ingérences étrangères.

La conformité réglementaire oriente désormais les flux de capitaux. **Les investisseurs privilégient les infrastructures certifiées** pour sécuriser leurs actifs. Cette norme constitue un trésor face à la dette technologique actuelle.

La confiance numérique repose sur des référentiels stricts. **La norme construit la crédibilité du marché**.

Impact des directives RGPD et NIS2 sur les investissements

La directive NIS2 impose une résilience opérationnelle aux infrastructures critiques. Les gestionnaires de data centers doivent investir massivement pour se conformer. Ces obligations de gouvernance sécurisent la chaîne d'approvisionnement.

Les normes européennes favorisent l'émergence d'une intelligence artificielle souveraine. Ce cadre encourage une innovation responsable et frugale. La France développe ainsi un **modèle alternatif aux géants américains**.

La continuité des services critiques dépend de notre autonomie technologique. Cette stratégie garantit la survie de nos institutions. C'est **le basculement stratégique** nécessaire pour protéger nos données nationales.

La France doit impérativement mobiliser son épargne longue pour financer l'IA et ses infrastructures critiques. Sécuriser ces actifs industriels garantit votre indépendance technologique face aux puissances mondiales. Agissez maintenant pour **bâtir une souveraineté numérique durable** : le contrôle de nos données est le socle de notre puissance future.