MANIFESTE DE SOUVERAINETÉ NUMÉRIQUE

De GendBuntu à l'État numérique souverain

Table des matières

Mode de lecture recommandé : commencer par la fiche de décision politique, puis selon le profil, aller directement aux sections concernées. Le document peut être lu section par section de façon autonome.

Note de mise à jour — 8 avril 2026

C'est une bonne nouvelle. Et vous ne regardez que la partie visible de l'iceberg.

Ce qui s'est passé — Les faits

Le 8 avril 2026, à l'initiative du Premier ministre Sébastien Lecornu (en poste depuis le 9 septembre 2025, source : Élysée.fr, décret du 10 octobre 2025), du ministre de l'Action et des Comptes publics David Amiel et de la ministre déléguée chargée de l'Intelligence artificielle et du Numérique Anne Le Hénanff (composition du gouvernement Lecornu II publiée au Journal officiel du 26 février 2026), la direction interministérielle du numérique a organisé le premier séminaire interministériel consacré à la réduction des dépendances numériques extra-européennes. L'événement a réuni pour la première fois des ministères, des opérateurs publics et des acteurs industriels privés autour d'une ambition explicitement formulée par le ministre Amiel : « L'État ne peut plus se contenter de constater sa dépendance, il doit en sortir. »

Trois annonces concrètes ont été faites. La direction interministérielle du numérique a annoncé sa propre migration des postes de travail de Windows vers Linux. La Caisse nationale d'Assurance maladie a annoncé la migration de ses 80 000 agents vers les outils du socle numérique interministériel — Tchap pour la messagerie, Visio pour la visioconférence, FranceTransfert pour l'échange de documents. La plateforme nationale des données de santé migrera vers une solution européenne de confiance d'ici fin 2026. Chaque ministère, opérateurs inclus, devra par ailleurs formaliser avant l'automne 2026 son propre plan de réduction des dépendances couvrant sept axes : poste de travail, outils collaboratifs, antivirus, intelligence artificielle, bases de données, virtualisation et équipements réseau. Les premières « rencontres industrielles du numérique » sont prévues en juin 2026 pour fédérer acteurs publics et privés autour d'une alliance formelle.

Ce séminaire s'inscrit dans une séquence de signaux politiques convergents. En janvier 2026, la ministre Anne Le Hénanff avait déclaré en réponse à une question écrite que « la DINUM a lancé en 2025 une réflexion sur le développement d'un poste de travail sous système Linux » (Journal officiel de l'Assemblée nationale, réponse à question écrite, janvier 2026). Le catalyseur institutionnel décisif est l'audition sénatoriale du 10 juin 2025. Devant la commission d'enquête du Sénat sur les coûts et les modalités effectifs de la commande publique (présidée par le sénateur Simon Uzenat), Anton Carniaux, directeur des affaires publiques et juridiques de Microsoft France, a fait deux déclarations sous serment. Premièrement : « Si nous sommes contraints par une décision de justice américaine, nous devons remettre les données. » (Source primaire : Sénat, compte rendu de la commission d'enquête sur la commande publique, séance du 10 juin 2025, senat.fr/compte-rendu-commissions/20250609/ce_commande_publique.html — confirmé par Techniques de l'Ingénieur, 6 août 2025, et Usine Digitale, 22 juillet 2025.) Deuxièmement, interrogé directement par le président Uzenat sur la question de savoir s'il pouvait garantir que les données des citoyens français « ne seront jamais transmises, à la suite d'une injonction du gouvernement américain, sans l'accord explicite des autorités françaises », Carniaux a répondu : « Non, je ne peux pas le garantir, mais cela ne s'est encore jamais produit. » (Source : Usine Digitale, 22 juillet 2025, d'après le compte rendu sénatorial.) L'Autorité européenne de protection des données (EDPS) a par ailleurs rendu le 8 mars 2024 (communiqué de presse du 11 mars 2024) une décision constatant que l'utilisation de Microsoft 365 par la Commission européenne violait le règlement (UE) 2018/1725 en transférant des données hors de l'Union européenne sans garanties adéquates (source primaire : edps.europa.eu/data-protection/our-work/publications/investigations/2024-03-08-edps-investigation-european-commissions-use-microsoft-365_en). La Commission a contesté cette décision devant le Tribunal UE (affaires T-262/24 et T-265/24, en cours). L'EDPS a clos sa procédure d'exécution en juillet 2025 après que la Commission eut mis en conformité son utilisation de Microsoft 365 — la décision du 8 mars 2024 reste néanmoins valide comme constat de violation pendant la période 2021-2024.

Sources primaires et secondaires : DINUM, communiqué officiel du 8 avril 2026 (numerique.gouv.fr) · Gouvernement Lecornu II, composition (Journal officiel, 26 février 2026) · Élysée, décret de nomination du Premier ministre (10 octobre 2025) · April, communiqué de presse (10 avril 2026) · Developpez.com, article (9 avril 2026) · IT-Connect, article (9 avril 2026) · Clubic, article (9 avril 2026) · Mac4ever, article (9 avril 2026) · GoodTech, article (9 avril 2026) · Anne Le Hénanff, réponse à question écrite (janvier 2026, Journal officiel AN).

Lecture n°1 — C'est une bonne nouvelle, et voici pourquoi

Cette annonce valide chacun des constats de ce manifeste. Elle confirme que le diagnostic sur la dépendance est désormais partagé au plus haut niveau de l'État. Elle amorce concrètement ce que ce document décrit comme les premières actions possibles : signal sur les postes de travail, migration des outils collaboratifs vers les solutions souveraines, et obligation pour chaque ministère de cartographier ses dépendances. Le fait que sept axes soient explicitement couverts — dont l'intelligence artificielle, les bases de données et les équipements réseau — correspond précisément à l'approche intégrée décrite dans ce manifeste. Ce n'est plus un document de plaidoyer : c'est devenu un document d'accompagnement de politique publique en cours de déploiement.

Lecture n°2 — Vous ne regardez que la partie visible de l'iceberg

La presse a salué la migration de la direction du numérique vers Linux comme un tournant historique. Lisons attentivement. Le communiqué officiel du 8 avril n'indique ni le nombre de postes ciblés, ni de calendrier d'exécution au-delà des plans ministériels attendus à l'automne. Selon les données publiques sur les effectifs de la direction interministérielle du numérique (environ 250 agents selon IT-Connect, 9 avril 2026, cohérent avec les données budgétaires publiées sur numerique.gouv.fr), la migration Linux annoncée porte sur une estimation d'environ 200 à 250 postes — soit, rapportés aux 3,5 millions de postes du secteur public français, un ratio de

0,007 %. C'est un signal fort — et l'extrême bout de la partie émergée de l'iceberg.

Note sur un chiffre circulant dans la presse : certains médias (notamment itsense.fr, 9 avril 2026) annoncent « 2,5 millions de postes de fonctionnaires sous Linux d'ici 2027 ». Ce chiffre ne figure ni dans le communiqué officiel de la direction interministérielle du numérique, ni dans aucune source gouvernementale vérifiée. Il n'est pas repris dans ce manifeste. Sa diffusion illustre précisément le phénomène décrit dans la Lecture n°3 : l'enthousiasme des commentateurs produit des chiffres que les faiseurs n'ont pas encore produits.

La migration de la Caisse nationale d'Assurance maladie de ses 80 000 agents vers Tchap et Visio est réelle et significative. Elle porte sur des outils collaboratifs — non sur le poste de travail ni sur les applications métier. Elle n'aborde pas les 10 000 applications métier de l'État, dont une proportion estimée entre 35 et 50 % est incompatible avec Linux sans refactorisation préalable — estimation de raisonnement par analogie internationale, non auditée en France (voir Section 6.3). L'association April, qui représente les utilisateurs et développeurs de logiciels libres en France depuis 1996, a relevé le 10 avril 2026 que le mot « logiciel libre » n'apparaît pas une seule fois dans le communiqué de presse officiel. Cette observation, formulée avec mesure, mérite d'être suivie de près dans les plans ministériels à venir.

> **La question que le communiqué ne pose pas :** quel est le budget alloué au portage applicatif ? Sans réponse à cette question, les plans ministériels de l'automne resteront des déclarations d'intention, aussi bien intentionnées soient-elles. Ce document estime ce programme entre 5 et 10 milliards d'euros sur dix ans — estimation non auditée, mais aucun chiffre de cette nature n'apparaît dans le communiqué du 8 avril.

Lecture n°3 — Beaucoup de commentateurs, peu de faiseurs

Le séminaire du 8 avril a produit des annonces. Il n'a pas produit un budget sanctuarisé, une loi de programmation, ni un mécanisme contraignant garantissant que les plans ministériels de l'automne seront suivis d'exécution. Mac4ever a noté un fait vérifiable — non une extrapolation — le 9 avril : « Le problème, c'est que pour la migration Linux, aucune date précise n'a été communiquée. Les plans ministériels sont attendus pour l'automne 2026, mais il s'agit de plans, pas de migrations effectives. » Cette observation porte sur l'absence documentée d'un élément dans un document officiel public — ce n'est pas de l'extrapolation, c'est de la lecture attentive d'un communiqué. Elle est à distinguer des chiffres extrapolés par certains médias (voir ci-dessus). La distinction entre un plan et une transformation reste précisément celle que ce manifeste pose en son cœur depuis sa première page.

La presse a également relevé, à raison, que cette annonce intervient à un an de l'élection présidentielle (GoodTech, 9 avril 2026). Le précédent munichois y est cité. La question de la continuité politique n'est pas une question de mauvaise foi — c'est la question centrale pour tout décideur qui veut que cette dynamique survive au prochain changement de gouvernement. L'application des recommandations de la Cour des comptes sur la direction du numérique de l'État, la sanctuarisation d'un budget pluriannuel, et l'inscription en loi de programmation ne sont pas des options supplémentaires après le séminaire du 8 avril. Elles sont devenues les conditions sine qua non pour que les annonces du 8 avril ne connaissent pas le sort de Munich en 2017 ou des circulaires logiciels libres de 2012.

Ce manifeste ne change pas un mot à son analyse. Il l'actualise : le signal politique est donné. La machinerie institutionnelle est en mouvement. L'iceberg est sous la surface. Les faiseurs ont maintenant un cadre politique — il leur manque trois choses précises : un budget sanctuarisé par la loi, une autorité de pilotage dont le mandat survit au calendrier électoral, et un Programme national de modernisation applicative (PNMA) financé avant de migrer le moindre ordinateur. Tant que ces trois conditions ne sont pas réunies, les annonces du 8 avril suivront le chemin documenté dans ce manifeste : signal fort, plans à l'automne, exécution incertaine. La distinction entre un plan et une transformation, c'est précisément ce que vingt ans d'échecs européens documentés — et vingt ans de succès de la Gendarmerie — ont établi.

Ce manifeste a été finalisé les 9 et 10 avril 2026, dans les quarante-huit heures suivant le séminaire de la DINUM. Son analyse précède l'annonce — et en constitue désormais la grille de lecture critique.

Fiche de décision politique — Pour le ministre ou le secrétaire d'État

Contexte immédiat : le gouvernement a organisé le 8 avril 2026 un séminaire interministériel sur la souveraineté numérique et annoncé une première accélération. La note de mise à jour en évalue le périmètre réel. Cette fiche présente ce que les annonces du 8 avril ne contiennent pas encore : le budget, le mécanisme contraignant, et les trois décisions qui conditionnent leur succès.

Cette fiche est conçue pour être lue en cinq minutes. Elle évite les sigles techniques. Le reste du document constitue l'étayage analytique complet pour vos équipes.

Le problème en trois faits

Fait 1 — Le 4 décembre 2025, Microsoft a annoncé des hausses de prix de 5 % à 33 % sur ses suites Microsoft 365 et Office 365 pour les entreprises et les clients gouvernementaux, applicables au 1er juillet 2026 (annonce officielle Microsoft, 4 décembre 2025 ; ChannelNews, 5 déc. 2025 ; Banque des Territoires, 12 déc. 2025). Pour les plans les plus répandus dans le secteur public, la hausse se situe entre 5 % et 13 % selon les offres — le taux de 33 % s'applique aux plans agents de terrain (F3). Pour l'État français, qui dépend de ces logiciels pour la quasi-totalité de ses ordinateurs, même une hausse de 10 % représente plusieurs centaines de millions d'euros supplémentaires par an — sans aucune possibilité de négociation, faute d'alternative crédible en place.

Fait 2 — Le droit américain autorise Washington à exiger l'accès aux données hébergées chez des entreprises américaines, même si ces données se trouvent sur des serveurs en France. Ce risque n'est pas neutralisé par les accords européens de transfert de données, qui régissent la légalité des transferts mais ne protègent pas contre une injonction gouvernementale américaine adressée directement à une entreprise soumise au droit américain. Un responsable de Microsoft France l'a confirmé sous serment devant une commission du Sénat en juin 2025. Les données fiscales, médicales et judiciaires des Français sont dans cette situation.

Fait 3 — La Gendarmerie nationale a accompli en vingt ans, sans rupture de service, la migration de 103 000 ordinateurs vers des logiciels dont elle contrôle entièrement le code. Elle ne paie plus de licences à Microsoft pour ses postes bureautiques. C'est possible. C'est fait. La question n'est plus de savoir si c'est possible — mais comment l'État applique cette méthode à sa propre échelle.

Ce qui se passe si l'on ne fait rien

Une facture numérique de 10 à 12 milliards d'euros sur dix ans — contre 4 à 7 milliards si la transformation est conduite correctement. Une dépendance juridique croissante vis-à-vis du droit américain. Et une incapacité à peser dans les négociations tarifaires futures, car sans alternative, il n'y a pas de levier. L'inaction n'est pas une option neutre : c'est un choix coûteux, renouvelé tacitement chaque année.

La mise en garde essentielle : ne pas reproduire l'erreur de Munich

En 2017, la ville de Munich a tenté de migrer ses ordinateurs vers des logiciels libres sans avoir préparé les applications métier à ce changement. Résultat : retour à Microsoft, ~50 millions d'euros de gaspillage, et dix ans de perdus. Quatre autres pays ont commis la même erreur. Ce document explique pourquoi, et quelle est la seule approche qui évite ce piège : traiter les applications en premier, les ordinateurs ensuite, les agents formés avant le déploiement — jamais après.

Les trois décisions que ce document vous demande

Décision 1 — Donner à la direction du numérique de l'État un budget pluriannuel protégé et l'autorité pour imposer ses choix techniques aux ministères — conformément aux recommandations que la Cour des comptes a déjà formulées en juillet 2024 et qui n'ont pas encore été appliquées.

Décision 2 — Inscrire en loi de finances 2027 un programme national sur cinq ans pour moderniser les 500 applications informatiques critiques de l'État afin qu'elles fonctionnent sur n'importe quel système — y compris des logiciels libres. Sans cela, aucune migration d'ordinateurs n'est possible sans provoquer une crise opérationnelle.

Décision 3 — Imposer par circulaire que tous les achats publics d'ordinateurs se fassent sans système d'exploitation pré-installé. Cette décision coûte zéro euro, peut être prise cette semaine, et envoie un signal immédiat aux éditeurs que la France reprend le contrôle de ses achats.

La question à poser à votre directeur des systèmes d'information dès aujourd'hui :

« Quel est notre plan si Microsoft augmente à nouveau ses tarifs de 30 % en 2029 ? Avons-nous une alternative crédible, ou sommes-nous dans la même situation qu'aujourd'hui ? »

▶ Pour l'étayage analytique complet, les sources vérifiées et les plans opérationnels, lire le résumé exécutif et les sections suivantes, destinés aux équipes techniques.

Résumé exécutif — Pour les équipes techniques et les responsables opérationnels

Si vous venez de lire la fiche de décision politique, ce résumé constitue le premier niveau d'étayage analytique. Il s'adresse aux directeurs de systèmes d'information, secrétaires généraux et responsables de transformation numérique chargés d'instruire et de préparer la décision. L'analyse complète, les sources et les arguments développés figurent dans les neuf sections qui suivent.

Ce qui est déjà en marche — État des fondations au 8 avril 2026

→ Les réalisations récentes — CNAM, données de santé, messagerie Tchap, cloud souverain — sont détaillées dans la **Note de mise à jour du 8 avril 2026**, première section de ce document. Le présent résumé exécutif en retient la synthèse analytique : des fondations existent et progressent, elles restent insuffisantes au regard de l'enjeu structurel, et les annonces du gouvernement doivent désormais être accompagnées des trois conditions décrites ci-dessous pour produire leurs effets.

La philosophie : intégrée, séquencée, sanctuarisée

La transformation proposée dans ce document repose sur un triptyque — trois mots qui peuvent paraître techniques mais dont chacun répond à un échec documenté. Il est utile d'en saisir le sens précis.

Intégrée ne signifie pas simultanée. Cela signifie que toutes les dimensions — poste de travail, applications, cloud, intelligence artificielle, formation, cadre juridique — doivent être **planifiées ensemble** dès le premier jour, même si elles ne sont pas toutes **déployées** simultanément. Aucun domaine ne peut être décidé en ignorant les autres — ni les ordinateurs sans les applications, ni le cloud sans l'intelligence artificielle. Planification intégrée, exécution séquencée.

Séquencée signifie que l'ordre d'exécution n'est pas arbitraire : les applications doivent toujours être préparées avant les ordinateurs, et les agents doivent toujours être formés avant le déploiement. Cette règle est non négociable : chaque fois qu'elle a été inversée, dans n'importe quel pays, le programme a échoué.

Sanctuarisée signifie que la transformation doit être adossée à un budget pluriannuel légalement protégé et à une autorité de pilotage dont le mandat survit aux changements de gouvernement. Sans cette condition, les programmes numériques de l'État n'ont jamais dépassé la durée d'une mandature.

Les cinq décisions opérationnelles — Correspondance avec la fiche politique

Les décisions 1, 2 et 3 ci-dessous correspondent directement aux trois décisions de la fiche politique. Les décisions 4 et 5 sont les conditions opérationnelles sans lesquelles les trois premières resteront sans effet.

➜ Fiche politique Décision 3

1. Imposer par instruction gouvernementale que tout achat public d'ordinateurs se fasse sans système d'exploitation fourni par l'éditeur. Cette décision relève d'une circulaire — elle ne nécessite aucune loi.

➜ Fiche politique Décision 1

2. Appliquer les recommandations R1, R3 et R8 de la Cour des comptes (rapport juillet 2024) sur la direction interministérielle du numérique sans attendre une réforme législative.

➜ Fiche politique Décision 2

3. Sanctuariser 500 millions d'euros sur cinq ans pour le Programme national de modernisation applicative (PNMA), couvrant les 500 applications métier critiques de l'État — portage vers le web, portage Linux natif et remplacement fonctionnel.

➜ Conditions opérationnelles — Sans lesquelles les trois décisions ci-dessus échouent

4. Intégrer contractuellement un poste de formation des utilisateurs avant tout déploiement d'outil informatique.
5. Fixer la doctrine sur les formats de documents : format ouvert (ODF) obligatoire pour les échanges internes à l'État, avec un convertisseur professionnel maintenu pour les échanges avec les partenaires extérieurs restant sous Microsoft.

1. Historique analytique de la migration GendBuntu

1.1 La décision intellectuelle fondamentale

Avant 2004, la Gendarmerie nationale achète 13 000 licences bureautiques par an, tourne intégralement sous Windows et Office, et n'a aucun levier de négociation face à un éditeur privé étranger dont elle dépend structurellement. Trois signaux convergents déclenchent la réflexion : la pression financière croissante sur les licences, l'exigence de sécurité incompatible avec la dépendance à un éditeur dont on ne maîtrise ni le code ni les mises à jour, et le contexte institutionnel favorable aux logiciels libres — contexte qui prendra sa forme officielle avec le Référentiel Général d'Interopérabilité (RGI, première version publiée par la Direction générale de la modernisation de l'État en 2009) et la circulaire du Premier ministre Jean-Marc Ayrault du 19 septembre 2012 (n°35837, Légifrance) formulant des orientations explicites pour l'usage des logiciels libres dans l'administration. Note : la Loi pour la Confiance dans l'Économie Numérique du 21 juin 2004 (LCEN), parfois citée dans ce contexte, porte sur le commerce électronique, les signatures électroniques et la responsabilité des hébergeurs — elle n'institue pas les standards ouverts dans les marchés publics.

La décision intellectuelle fondamentale, formulée dès 2004 par le colonel Nicolas Géraud — un officier qui a changé la trajectoire informatique d'une institution entière — est que le système d'exploitation est une commodité : « Ce qui est important, ce sont les applications métier ; le PC est neutre, banalisé. » Cette conviction a rendu la migration politiquement et techniquement indolore — en déplaçant l'enjeu du système d'exploitation vers les applications, domaine où la Gendarmerie maîtrisait le sujet.

1.2 La stratégie progressive : remplacer les applications avant les ordinateurs

Entre 2004 et 2007, la Gendarmerie remplace successivement chaque composant Microsoft : LibreOffice (ex-OpenOffice.org) remplace Office sur 90 000 postes en 2004-2005, Firefox remplace Internet Explorer en 2006, Thunderbird remplace Outlook la même année. Résultat : sur les exercices 2005 à 2007, 27 licences bureautiques achetées contre 13 000 par an précédemment. Quand le système d'exploitation Windows disparaîtra ensuite, les utilisateurs ne remarqueront presque rien — leur environnement de travail n'a pas changé.

En 2007, Vista — trop lourd, trop coûteux, incompatible avec le parc existant — crée le contexte favorable à la décision. Le commandant Jean-Pascal Chateau est direct : « Nous ne rencontrions pas de problèmes techniques, mais financiers. Pour la même quantité de travail, Windows nous coûterait deux millions d'euros de plus par an qu'Ubuntu. » En janvier 2008, l'annonce officielle au salon Solutions Linux est qualifiée de « non-événement » — formule qui résume quatre ans de préparation silencieuse.

1.3 Architecture et déploiement de GendBuntu

GendBuntu est une distribution Ubuntu entièrement adaptée : interface reproduisant l'ergonomie de Windows XP pour minimiser la rupture visuelle, applications métier pré-intégrées, politiques de sécurité définies par l'Agence nationale de la sécurité des systèmes d'information, outils de déploiement centralisé sur 4 300 sites géographiques incluant les territoires d'outre-mer. Depuis 2008, 90 % des achats de postes se font sans système d'exploitation pré-installé. La structure de support comprend une équipe centrale, une équipe opérationnelle, et environ 1 200 techniciens locaux. Cette internalisation des compétences est une condition de la durabilité : Canonical fournit le socle, la Gendarmerie maîtrise tout le reste.

L'objectif initial de 80 000 postes fin 2014 n'est pas atteint — 65 000 seulement en juin de cette année, soit un retard de cinq ans jamais officiellement reconnu. Le rattrapage s'opère discrètement : 90 % du parc fin 2019, 85 000 postes en janvier 2021, 103 000 postes et 97 % de couverture en 2025. Les 5 500 postes Windows résiduels (6 % du parc) hébergent les applications les plus critiques — forensique numérique, logiciels judiciaires spécialisés, systèmes d'interopérabilité avec des partenaires opérant sous Windows. Ce résiduel n'est pas un échec : il est la démonstration que les adhérences applicatives constituent le verrou structurel de toute transformation numérique, et que les résidus doivent être documentés et assumés, non camouflés.

1.4 Les limites objectives du modèle

Trois limites structurelles méritent d'être nommées. D'abord, la substitution d'une dépendance par une autre : Canonical est une société privée britannique opérant hors du cadre juridique de l'Union européenne depuis le Brexit — le Royaume-Uni dispose d'un équivalent au règlement général sur la protection des données, mais les décisions architecturales de Canonical (calendriers des versions à support prolongé, adoption de nouvelles technologies, fins de support) sont prises unilatéralement. La migration anticipée de GendBuntu 20.04 vers 22.04, réalisée avant la fin du support standard fixée à avril 2025, illustre cette contrainte : le calendrier de l'éditeur, même en logiciel libre, s'impose à l'institution.

Ensuite, la vulnérabilité par homogénéité : l'incident XZ Utils (CVE-2024-3094, mars 2024) — dans lequel un contributeur malveillant avait introduit une porte dérobée dans une bibliothèque critique du noyau Linux — a montré qu'un parc homogène massif constitue une surface d'attaque prévisible. La diversité technologique est aussi un mécanisme de résilience défensive.

Enfin, la pertinence décroissante du débat sur le poste de travail : en 2026, les dépendances souveraines les plus critiques se situent dans le cloud, dans les modèles d'intelligence artificielle et dans les équipements réseau — non sur le bureau de l'agent. Migrer des millions de postes vers Linux tout en maintenant les données dans les serveurs d'un acteur américain et les flux de travail dans son outil d'intelligence artificielle, c'est sauver l'apparence de la souveraineté tout en perdant sa substance.

2. Frise chronologique de la migration GendBuntu

Année	Phase	Événement clé
2001	Phase 0	Migration des serveurs internes vers Debian GNU/Linux. Première preuve de concept, formation des techniciens.
2004	Phase 1	OpenOffice.org remplace MS Office sur 20 000 postes pilotes. Format ouvert ODF adopté comme standard national.
2005	Phase 1	Migration bureautique achevée sur 90 000 postes. 27 licences achetées en 3 ans contre 13 000 par an précédemment.
2006	Phase 1	Firefox remplace Internet Explorer. Thunderbird remplace Outlook.
2007	Phase 2	Vista évalué : trop lourd, trop coûteux. Décision de principe pour Linux.
Jan. 2008	Phase 2	Annonce officielle salon Solutions Linux. Col. Géraud : « un non-événement » — fruit de quatre ans de préparation.
2008	Phase 3	Lancement GendBuntu (partenariat Canonical). 90 % des achats PC sans système d'exploitation dès cette date.
Juin 2014	Phase 3	65 000 postes déployés. Objectif 2014 manqué de 15 000 postes. Retard effectif : cinq ans.
2017	JALON	Munich (LiMux) abandonne Linux. Retour à Windows budgété à ~50 M€. La Gendarmerie maintient sa doctrine.
2019	Phase 4	90 % du parc (77 000 postes). Rattrapage silencieux du retard de 2014.
Jan. 2021	Phase 4	85 000 postes Linux + 5 500 Windows résiduels (6 %). Stabilisation.
2022–2024	Phase 5	Migration anticipée 20.04 → 22.04. Fin du support standard Canonical : avril 2025.
Avr. 2024	SIGNAL	Schleswig-Holstein annonce la migration de 30 000 postes vers Linux/LibreOffice. Motivation : droit américain extraterritorial.
Oct. 2025	JALON	Fin du support de Windows 10 par Microsoft. Renouvellements de matériel non budgétés imposés.
Déc. 2025	JALON	Microsoft annonce des hausses de 5 % à 33 % sur les licences Microsoft 365 et Office 365 au 1er juillet 2026 (annonce officielle du 4 décembre 2025 ; hausse de 5 % à 13 % pour les plans secteur public selon offre). Catalyseur politique majeur.
2025	Phase 5	103 000 postes GendBuntu, 97 % du parc.

3. Retour d'expérience

3.1 Ce que les faits établissent

Voici ce qui est établi sans ambiguïté. Le déploiement à 97 % du parc est confirmé par des sources multiples et concordantes. Les économies de deux millions d'euros annuels sur les licences du système d'exploitation sont corroborées par des données Canonical et Gendarmerie. La réduction des achats de licences bureautiques — de 13 000 à 27 sur trois ans — est documentée directement par le colonel Géraud en 2008. En revanche, le chiffre de neuf millions d'euros d'économies annuelles, souvent repris sans précaution, correspond à une estimation auto-déclarée de 2009 sans méthode comptable publiée ni audit indépendant. Les sept millions d'écart représentent des économies dites indirectes qui n'ont jamais été objectivées par une tierce partie.

3.2 Les conditions de succès

Condition	Rôle	Transposable ?
Poste de travail traité comme commodité	La décision de séparer l'enjeu des applications de celui du système d'exploitation a rendu la migration politiquement et techniquement indolore.	Oui — principe universel
Applications remplacées avant le système d'exploitation	En substituant Office, Firefox et Thunderbird avant de toucher à Windows, 90 % des résistances ont été supprimées en amont.	Oui — méthode universellement applicable
Continuité du leadership sur vingt ans	Trois responsables successifs, une doctrine cohérente sans déviation.	Difficile — exige une sanctuarisation institutionnelle
Incentive comportemental positif	Nouveau matériel associé à la migration. Transformer une contrainte en opportunité.	Oui — adaptable à tout contexte
Hiérarchie militaire permettant l'imposition directe	Facteur le plus efficace et le moins reproductible — aucune administration civile ne dispose de ce levier.	Non — condition absente dans le civil

4. Panorama international comparé — Vingt ans d'expériences mondiales

Vingt ans de migrations de logiciels libres dans le secteur public à travers le monde ont produit un corpus d'expériences riche — et souvent mal utilisé. Certains en citent les succès pour prouver que c'est simple. D'autres en citent les échecs pour prouver que c'est impossible. Les deux ont tort, parce qu'ils mélangent des contextes non comparables. Cette section distingue trois niveaux de comparabilité, pour permettre au lecteur de raisonner avec rigueur sur ce que chaque cas enseigne réellement.

4.1 Niveau 1 — Cas directement comparables

France — Gendarmerie nationale : la référence de méthode

Migration de 103 000 postes sur vingt ans dans un organisme public français. C'est le seul cas de migration Linux réussie à cette échelle dans le secteur public français. Il prouve la faisabilité dans un contexte militaire à commandement hiérarchique centralisé. Il ne prouve pas directement la faisabilité dans une administration civile. Sources : Wikipedia GendBuntu (fév. 2026), Connect LP-125 (2021), CIO-Online (janv. 2008).

Allemagne — Munich / LiMux : la référence de l'échec

Déployé à partir de 2004, LiMux atteignait environ 18 500 postes en 2017 (parallèlement à 10 700 postes restés sous Windows). En 2017, le conseil municipal a voté à une majorité le retour à Windows 10, dans le cadre d'une restructuration informatique budgétée à environ 50 millions d'euros pour la seule migration Windows, et environ 89 millions pour l'ensemble du projet. Le chiffre de 100 millions d'euros parfois cité dans la presse anglophone (Softpedia, 2018) n'a été confirmé par aucune source institutionnelle allemande ou française. Trois causes sont documentées : Munich n'a jamais migré ses serveurs de messagerie ni son annuaire d'authentification, créant une hétérogénéité permanente entre postes et serveurs ; entre 20 et 40 % des postes n'ont jamais quitté Windows pour des raisons d'applications métier incompatibles ; la migration du poste de travail a précédé la préparation des applications. Sources : Developpez.com (nov. 2017), LeMagIT (déc. 2017), Silicon.fr (2018), Le Monde Informatique (2017).

Allemagne — Schleswig-Holstein : le cas en cours, le plus rigoureux

Décision d'avril 2024, 30 000 postes civils, migration vers Linux, LibreOffice, Nextcloud, Thunderbird et Open-Xchange. Le format ouvert ODF est obligatoire pour tous les échanges officiels depuis août 2024. Fin 2025, 80 % des postes migrés, 15 millions d'euros économisés. Le projet a survécu aux élections grâce à un consensus entre partis politiques — premier facteur de pérennité identifié par les responsables. Limite reconnue : moins de 80 % des agents sont capables d'utiliser correctement les nouveaux outils — neuf millions d'euros de formation de rattrapage ont été budgétés pour 2026. Ce retournement illustre précisément la règle la plus souvent violée : former avant de déployer, jamais après. Sources : EuroStack Directory (mars 2025), LibreOffice Conference 2024, The Register (avr. 2024), Developpez.com (déc. 2025).

Corée du Sud : l'annonce sans préparation

En 2022, le gouvernement a annoncé la migration de 3,3 millions de postes vers une distribution nationale d'ici 2026. Selon les observations disponibles en avril 2024 (source la plus récente), moins de 20 % de cet objectif avait été réalisé. Ces chiffres n'ont pas été mis à jour depuis par une source institutionnelle. Les causes identifiées recoupent exactement celles de Munich : proportion élevée d'applications métier incompatibles, résistance administrative, et changement de gouvernement en 2022 réduisant l'ambition politique. Source : IT Brew (avr. 2024) — données non confirmées pour 2025.

4.2 Niveau 2 — Cas partiellement comparables

Allemagne — openDesk et les forces armées fédérales

En 2025, ZenDiS (Centre pour la souveraineté numérique de l'administration allemande) et BWI GmbH (la société de systèmes informatiques de la Bundeswehr) ont signé un accord-cadre de sept ans pour déployer openDesk — une suite collaborative ouverte — comme solution souveraine de poste de travail dans les forces armées allemandes. Ce cas est partiellement comparable : il confirme que la convergence civil-militaire autour de logiciels libres est possible à l'échelle nationale, mais porte sur la suite collaborative, non sur le système d'exploitation des postes. Il est aussi directement pertinent pour la France dans le contexte de la Suite numérique de la direction du numérique de l'État. Source : opendesk.eu (2025).

Allemagne — Basse-Saxe : le retour arrière discret

En 2018, le Land de Basse-Saxe a mis fin à une expérimentation de migration Linux sur ses postes de terrain et est revenu à Windows. L'argument officiel : la cohérence du parc, une partie significative des agents de terrain continuant d'utiliser Windows pour des applications métier incompatibles. Ce retour arrière, moins médiatisé que celui de Munich, valide la même règle : une administration ne peut pas migrer à moitié. La coexistence durable de deux systèmes d'exploitation sur un même réseau — sans migration des serveurs et sans homogénéisation des applications — produit une complexité opérationnelle qui finit par l'emporter sur les bénéfices. Source : CIO-Online (2018).

Barcelone : initiative lancée en 2017, résultats post-2019 non documentés

En 2017, la mairie de Barcelone a lancé une migration vers Ubuntu, Open-Xchange, LibreOffice et Firefox, avec 1 000 postes pilotes et l'objectif d'achever la transition avant le printemps 2019. Après les élections municipales de mai 2019, la commissaire à la technologie et à l'innovation numérique Francesca Bria a quitté ses fonctions. Aucune source publiée ne documente l'état d'avancement de la migration sous la municipalité suivante. Ce cas illustre le risque majeur du portage politique par un individu sans continuité institutionnelle garantie — et non un succès à citer. Sources : LeMagIT (janv. 2018), Silicon.fr (janv. 2018).

4.3 Niveau 3 — Cas illustratifs (contextes non comparables)

Kerala (Inde) — Programme IT@School

Depuis 2001, l'État indien du Kerala forme des millions d'élèves dans les écoles publiques sur des logiciels libres. Ce cas illustre la faisabilité de la formation scolaire sur logiciels libres à grande échelle et sur le long terme — leçon utile pour la politique éducative française. Le contexte économique et administratif du Kerala n'est pas comparable à celui de l'État français. Source : Wikipedia FOSS public sector (avr. 2026).

Pérou et Équateur : la logique démocratique explicite

En 2005, le Pérou a adopté une loi rendant les logiciels à code source ouvert obligatoires dans tous ses organismes publics, avec une argumentation directement fondée sur les garanties démocratiques : des logiciels dont le code source ne peut pas être inspecté ne sont pas compatibles avec les exigences de transparence d'un État de droit. En 2008, l'Équateur a suivi par un décret similaire. Ces cas illustrent la dimension juridique et démocratique de l'argument souverainiste — mais sans résultats de déploiement documentés à grande échelle. Source : Wikipedia FOSS public sector.

Station spatiale internationale — Référence historique

L'Alliance Spatiale Unie, qui gérait les systèmes informatiques de la Station Spatiale Internationale jusqu'en 2017, avait choisi Linux pour les fonctions critiques avec cet argument : « Nous avions besoin d'un système stable et fiable — un système qui nous donnerait le contrôle en interne. Si nous devions corriger, ajuster ou adapter, nous pouvions le faire. » Cette logique — maîtrise interne, capacité d'adaptation immédiate — est exactement celle que la Gendarmerie a appliquée. La citation reste valide comme argument de fiabilité opérationnelle. Note : l'Alliance Spatiale Unie a cessé ses opérations en 2017. Source : Wikipedia FOSS public sector (avr. 2026).

4.4 Tableau comparatif consolidé — Trois niveaux

Cas	Niveau	Périmètre	Résultat	Leçon opérationnelle
Gendarmerie FR	Comparable	103 000 postes militaires, 20 ans	97 % — succès pérenne documenté	Séquencer les applications avant le poste. Contexte militaire non reproductible tel quel.
Munich DE	Comparable	~18 500 postes LiMux + 10 700 Windows, 2004-2017	Retour à Windows (~50 M€ migration, ~89 M€ IT total)	Migration du poste sans migration des serveurs = échec assuré.
Schleswig-Holstein DE	Comparable	30 000 postes civils, 2024–	80 % migrés fin 2025, 15 M€ économisés — gap de formation	Consensus politique trans-partis vital. Former avant de déployer.
Corée du Sud	Comparable	3,3 M postes, 2022–	< 20 % (données avr. 2024, non confirmées depuis)	Annonce sans applications préparées = retard systématique.
openDesk + Bundeswehr DE	Part. comparable	Suite collaborative, 7 ans, 2025–	Accord-cadre signé, déploiement en cours	Convergence civil-militaire sur logiciels libres possible.
Basse-Saxe DE	Part. comparable	Postes de terrain, retour arrière 2018	Retour à Windows	Coexistence poste/serveur sans homogénéité = complexité croissante intenable. (CIO-Online 2018)
Barcelone ES	Part. comparable	~1 000 postes pilotes, plan 2017-2019	Résultats post-2019 non documentés	Portage sur un individu sans sanctuarisation = fragilité structurelle. (LeMagIT 2018)
Kerala Inde	Illustratif	Écoles publiques, 2001–	Succès scolaire durable	Formation scolaire sur logiciels libres : possible et durable.
Pérou / Équateur	Illustratif	Secteur public, 2005/2008	Cadre légal adopté — résultats non documentés	L'argument démocratique (code transparent) est juridiquement fondé.
ISS (historique)	Illustratif	Systèmes critiques jusqu'en 2017	Linux sur fonctions critiques — entité dissoute en 2017	Stabilité + maîtrise interne : argument opérationnel universel.

4.5 Les quatre règles empiriques

> **Règle 1 :** L'administration ne migre jamais le poste de travail d'un périmètre avant d'avoir rendu ses applications métier compatibles. Aucune exception documentée dans les cas de succès.
>
> **Règle 2 :** La formation des utilisateurs doit précéder le déploiement. Former après est aussi inefficace que ne pas former du tout.
>
> **Règle 3 :** La continuité politique et la sanctuarisation institutionnelle sont des conditions préalables. Munich 2017, Basse-Saxe 2018 et Barcelone 2019 en sont les preuves les plus claires.
>
> **Règle 4 :** L'homogénéité poste/serveur est indispensable. Migrer les postes sans migrer les serveurs de messagerie et d'annuaire produit une hétérogénéité plus coûteuse à gérer que l'homogénéité propriétaire.

5. Le cadre européen obligatoire — Ce que la France n'a pas le choix d'ignorer

La souveraineté numérique de l'État français ne se construit pas dans un vide institutionnel. En 2026, quatre règlements et directives européens directement applicables redéfinissent les obligations de sécurité, de traçabilité et d'interopérabilité des systèmes d'information publics. Ces textes constituent, pour une partie des décisions décrites dans ce manifeste, non plus des choix politiques optionnels mais des obligations juridiques contraignantes.

Mais avant d'examiner ces textes européens, un prérequis conceptuel s'impose. Les règlements européens décrits ci-dessous encadrent les transferts et le traitement des données au sein de l'Union. Ils ne protègent pas, seuls, contre les mécanismes d'accès extraterritoriaux américains qui opèrent en parallèle selon une logique entièrement distincte. Comprendre cette distinction est la condition pour ne pas tirer de fausses conclusions de la conformité réglementaire.

5.0 — Prérequis de lecture : trois instruments américains opérant indépendamment du droit européen

> **Point de droit fondamental — à lire avant les sections 5.1 à 5.4 :** Trois instruments juridiques américains donnent au gouvernement des États-Unis des droits d'accès aux données hébergées par des entreprises soumises à la juridiction américaine, indépendamment de tout accord européen sur les données. (1) Le CLOUD Act (18 U.S.C. § 2713) : outil judiciaire, mandat requis, ciblé. (2) FISA Section 702 (50 U.S.C. § 1881a) : surveillance de masse par les agences de renseignement, sans mandat individuel. (3) Executive Order 12333 : surveillance la plus étendue, hors cadre judiciaire. La conformité aux règlements européens (DPF, RGPD, NIS2) répond à des questions juridiques entièrement distinctes — elle ne neutralise aucun de ces trois instruments. L'analyse juridique détaillée est présentée ci-dessous pour les lecteurs juristes et décideurs techniques.

Le premier instrument est le CLOUD Act (Clarifying Lawful Overseas Use of Data Act, Pub.L. 115-141, art. 103(a), codifié au 18 U.S.C. § 2713, promulgué le 23 mars 2018). Il s'agit d'un outil des forces de l'ordre judiciaires. Le texte exact de 18 U.S.C. § 2713 dispose — cité ici en anglais, aucune traduction officielle en français n'existant : « shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States » [traduction : doit se conformer aux obligations du présent chapitre de conserver, sauvegarder ou divulguer le contenu de toute communication et tout enregistrement relatif à un client, indépendamment du fait que cette information se trouve à l'intérieur ou à l'extérieur du territoire des États-Unis]. Chaque demande est fondée sur un mandat délivré par un tribunal américain — contrôle judiciaire ex ante, outil ciblé, cadre pénal. C'est précisément ce mécanisme — la contrainte par décision judiciaire américaine — qu'Anton Carniaux, directeur des affaires publiques et juridiques de Microsoft France, a décrit sous serment le 10 juin 2025 devant la commission d'enquête sénatoriale (source primaire : senat.fr/compte-rendu-commissions/20250609/ce_commande_publique.html) : « Si nous sommes contraints par une décision de justice américaine, nous devons remettre les données. » Son verbatim confirme l'exposition au CLOUD Act ; il ne décrit pas le mécanisme de FISA 702, instrument distinct opérant sans mandat individuel.

Le deuxième instrument est la Section 702 du Foreign Intelligence Surveillance Act (FISA Section 702, 50 U.S.C. § 1881a, adoptée en 2008, réautorisée en 2024 par le RISAA Act). Note sur le statut au moment de la finalisation du document : la loi RISAA prévoyait un sunset au 20 avril 2026. Au 11 avril 2026, aucun vote du Congrès américain n'avait encore renouvelé cette autorisation. Le Foreign Intelligence Surveillance Court a recertifié les procédures opérationnelles le 17 mars 2026 — certification qui permet la continuité d'exécution mais ne constitue pas un renouvellement de l'autorité législative, dont l'échéance légale est fixée au 20 avril 2026 (Nextgov/FCW, 11 avril 2026 ; Brennan Center, ressource 2026 active ; American Prospect, mars 2026). FISA Section 702 est d'une nature radicalement différente du CLOUD Act : il autorise la NSA et le FBI à collecter les communications de personnes non américaines situées à l'étranger, dans le cadre de programmes approuvés annuellement par la FISC — sans mandat individuel par cible. L'entreprise visée ne

peut pas informer ses clients. C'est précisément FISA 702 et l'Executive Order 12333 qui ont été au cœur des arrêts Schrems I et Schrems II de la CJUE, établissant leur incompatibilité avec les droits fondamentaux européens. L'exposition à FISA 702 est établie par ces arrêts et par la décision EDPS du 8 mars 2024 — non par le verbatim Carniaux, qui décrit un mécanisme judiciaire distinct.

Le troisième instrument est l'Executive Order 12333 (EO 12333, signé par le président Reagan en 1981, modifié en 2008). Il autorise le renseignement américain à collecter des données à l'étranger dans des conditions encore plus larges que FISA 702, en dehors de tout cadre FISC. Il constitue le fondement juridique de la grande majorité des activités de surveillance de masse de la NSA documentées par Edward Snowden en 2013.

Ces trois instruments opèrent indépendamment du droit européen des données personnelles et indépendamment l'un de l'autre. Le Data Privacy Framework (DPF, décision d'adéquation 2023/1795 de la Commission européenne, adoptée le 10 juillet 2023) répond à une question entièrement distincte : peut-on transférer légalement des données personnelles de l'Union européenne vers des entités américaines certifiées au titre du Chapitre V du RGPD ? Sa validité a été confirmée par le Tribunal de l'Union européenne le 3 septembre 2025 (affaire T-553/23, recours Latombe) sur les points contestés. Mais le DPF ne modifie ni la portée du CLOUD Act (§ 2713), ni celle de FISA 702, ni celle de l'EO 12333. Un transfert légalement encadré par le DPF peut faire l'objet d'une demande CLOUD Act le lendemain (confirmé par le verbatim Carniaux sous serment, 10 juin 2025, cité ci-dessus) — et les données peuvent par ailleurs avoir été collectées indépendamment via FISA 702 (établi par Schrems II, C-311/18, 2020) ou EO 12333. L'Autorité européenne de protection des données a constaté l'exposition structurelle dans sa décision du 8 mars 2024 sur l'utilisation de Microsoft 365 par la Commission européenne (décision complète : edps.europa.eu/data-protection/our-work/publications/investigations/2024-03-08-edps-investigation-european-commissions-use-microsoft-365_en ; communiqué du 11 mars 2024 ; affaires T-262/24 et T-265/24 devant le Tribunal UE en cours ; procédure d'exécution close juillet 2025 après correction). Les règlements européens qui suivent dans cette section répondent à des obligations réelles et contraignantes — ils ne constituent pas une réponse suffisante à ces trois instruments américains.

5.1 Le règlement sur la cyber-résilience (CRA) — Règlement EU 2024/2847

Le règlement européen sur la cyber-résilience (Cyber Resilience Act) est entré en vigueur le 10 décembre 2024. Ses obligations de signalement de vulnérabilités s'appliquent dès le 11 septembre 2026 ; l'ensemble des obligations sera exigible à compter du 11 décembre 2027. Ce texte impose à tout produit numérique mis sur le marché européen des exigences de sécurité tout au long de son cycle de vie — de la conception à la mise hors service.

Sa portée pour les administrations publiques est plus subtile qu'elle n'y paraît : le règlement impose ses obligations aux fabricants et aux opérateurs économiques qui mettent des produits sur le marché européen — non directement aux organisations qui les déploient. Une administration qui installe Microsoft Office n'est pas tenue de produire elle-même la documentation de sécurité de ce logiciel. C'est Microsoft qui l'est. Ce renversement est en réalité plus puissant argumentairement : le règlement sur la cyber-résilience est un outil de pression sur les éditeurs propriétaires, qui devront documenter et assurer la traçabilité de tout ce qui compose leurs produits — y compris les bibliothèques tierces. Pour les administrations acheteuses, cela se traduit en un droit nouveau : exiger contractuellement, dans les marchés publics, que leurs fournisseurs fournissent une nomenclature des composants logiciels, une politique de gestion des vulnérabilités, et une documentation de sécurité du cycle de vie. Les logiciels propriétaires à code source fermé satisferont ces exigences avec une difficulté structurelle que les logiciels libres, dont le code est public et auditable, ne rencontrent pas.

5.2 La directive sur la sécurité des réseaux et des systèmes d'information (NIS2) — Directive EU 2022/2555

La directive NIS2 est en cours de transposition en droit français via le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité (dit « loi Résilience »). Ce texte a été adopté par le Sénat le 12 mars 2025 et par la commission spéciale de l'Assemblée nationale le 10 septembre 2025.

En avril 2026, il n'a toujours pas été inscrit à l'ordre du jour de la séance plénière de l'Assemblée nationale, en raison d'un désaccord politique sur l'article 16 bis — ajouté par le Sénat — qui interdit aux fournisseurs de messageries chiffrées la création de portes dérobées. La Commission supérieure du numérique et des postes (CSNP) a formellement demandé une inscription d'urgence dans un communiqué du 18 mars 2026 (Banque des Territoires, 18 mars 2026 ; Acteurs Publics, 4 février 2026). La France est en infraction de transposition depuis le 17 octobre 2024, délai européen dépassé : elle est l'un des six États membres n'ayant pas encore transposé au 1er janvier 2026. L'adoption en séance plénière est anticipée pour juillet 2026, sous réserve d'une session extraordinaire. En conséquence, la directive NIS2 n'est pas encore pleinement applicable en France en avril 2026 — l'ANSSI encourage néanmoins les entités concernées à commencer leur mise en conformité, s'appuyant sur le référentiel ReCyF publié le 17 mars 2026. Ce texte élargira le périmètre des entités régulées de 500 à environ 15 000 entités, dont les administrations publiques classées en « entités essentielles ». Sources : Vie-publique.fr (octobre 2025), Assemblee-nationale.fr dossier législatif n°50731, Sénat rapport n°393 (mars 2025), Acteurs Publics (4 février 2026), CSNP communiqué (18 mars 2026), Orange Cyberdefense (17 mars 2026).

Les obligations concrètes pour les administrations couvrent la gestion des risques, les mesures de sécurité de la chaîne d'approvisionnement (y compris les logiciels tiers), la notification obligatoire des incidents significatifs à l'Agence nationale de la sécurité des systèmes d'information, et la responsabilité personnelle des dirigeants. Les sanctions prévues peuvent atteindre 2 % du budget pour les entités essentielles. Un outil d'IA ou un logiciel cloud hébergé par un acteur hors du cadre européen — et donc hors de la portée d'un audit de sécurité national — sera difficile à justifier devant ces obligations.

5.3 Le règlement sur l'intelligence artificielle — Règlement EU 2024/1689

Le règlement européen sur l'intelligence artificielle est publié depuis juin 2024 et appliqué progressivement. Les interdictions sont applicables depuis août 2024 ; les obligations pour les systèmes à haut risque s'appliquent depuis août 2026. Ce texte classe comme « à haut risque » tout système d'intelligence artificielle utilisé par une administration publique pour des décisions individuelles affectant des droits — évaluation de demandes de prestations, décisions d'affectation, analyse de risques judiciaires. Ces systèmes doivent faire l'objet d'une évaluation de conformité, d'une documentation technique, d'une supervision humaine active, et d'un enregistrement dans une base de données européenne.

Un assistant d'intelligence artificielle générative utilisé par des agents publics pour instruire des dossiers administratifs peut relever de cette catégorie. L'utilisation de modèles propriétaires américains pour ces usages pose une question de conformité directe : comment documenter et auditer un modèle dont on ne contrôle ni les données d'entraînement ni les mécanismes de décision ? Un modèle souverain à code ouvert répond structurellement mieux à cette exigence — ce qui constitue un argument réglementaire en faveur de l'assistant d'intelligence artificielle actuellement expérimenté par la direction du numérique de l'État.

5.4 Le cadre européen d'interopérabilité et le schéma de certification cloud

Le cadre européen d'interopérabilité (European Interoperability Framework, EIF 2.0) recommande que les échanges entre administrations publiques européennes s'appuient sur des standards ouverts. La directive ODF y est inscrite comme référence pour les documents texte. Toute administration qui maintient des formats propriétaires dans ses échanges officiels prend le risque d'une non-conformité à ce cadre dès lors que des échanges transfrontaliers sont concernés.

Par ailleurs, la Commission européenne développe depuis 2019 un schéma européen de certification des services cloud (EU Cloud Services Scheme, EUCS). Le projet initial prévoyait un niveau « High+ » exigeant l'immunité aux législations extraterritoriales — une exigence directement inspirée du référentiel SecNumCloud français. Ce niveau High+ a été retiré dans la version publiée en mars 2024, sous la pression d'une majorité d'États membres (notamment Pays-Bas, Allemagne, Autriche) qui refusaient d'exclure de fait les hyperscalers américains. En 2026, les négociations sont dans l'impasse : la France — soutenue par l'Italie et l'Espagne — bloque toute adoption de l'EUCS sans rétablissement d'exigences d'immunité extraterritoriale (CSNP, avis du 4 septembre 2024 ; Banque des Territoires, octobre 2024 ; INCYBER, juin 2025). La Commission supérieure du numérique et des postes et la CNIL ont toutes deux alerté que l'EUCS

actuel, s'il est adopté tel quel, pourrait remettre en cause la légalité du référentiel SecNumCloud national, perçu par certains États comme une restriction anticoncurrentielle au sens du droit européen. SecNumCloud 3.2 est donc, en 2026, plus exigeant que ce que l'Europe a accepté de négocier — et non le contraire. Sources : INCYBER (juin 2025), CIO-Online (septembre 2024), IT for Business (avril 2024), Banque des Territoires (octobre 2024), CSNP avis (4 septembre 2024), CNIL (juillet 2024).

Synthèse du cadre réglementaire européen

Texte	En vigueur	Obligations clés pour l'État	Lien avec la souveraineté numérique
CRA (EU 2024/2847)	Déc. 2024 — obligations complètes déc. 2027	Oblige les fournisseurs à documenter leurs produits (nomenclature des composants, gestion des vulnérabilités, cycle de vie). Donne aux administrations acheteuses le droit d'exiger ces documents dans leurs marchés publics.	Droit nouveau pour l'acheteur public : exiger contractuellement la traçabilité complète des logiciels achetés. Les fournisseurs de logiciels à code fermé auront du mal à satisfaire cette exigence de façon vérifiable.
NIS2 (EU 2022/2555)	En transposition FR — applicable 2026-2027	Gestion des risques, sécurité de la chaîne d'approvisionnement, notification incidents, responsabilité des dirigeants	Les dépendances à des acteurs hors cadre européen constituent une exposition difficile à justifier devant l'obligation de sécurisation de la chaîne d'approvisionnement.
AI Act (EU 2024/1689)	Systèmes haut risque : août 2026	Évaluation de conformité, documentation, supervision humaine, enregistrement EU pour les systèmes d'IA à haut risque dans l'administration	Les modèles souverains à code ouvert permettent l'audit de conformité ; les modèles propriétaires américains le rendent structurellement difficile.
EIF 2.0	Applicable	Standards ouverts pour échanges inter-administrations européens	ODF comme format de référence — obligation de compatibilité pour les échanges transfrontaliers.

6. Plan de transformation intégrée — Les dix domaines

La transformation numérique souveraine de l'État s'articule autour de dix domaines interdépendants. Ce plan répond à la fois à un impératif stratégique — reprendre un levier de décision sur l'infrastructure numérique de l'État — et à des obligations réglementaires européennes déjà en vigueur ou en cours de transposition, détaillées en Section 5 : règlement sur la cyber-résilience, directive NIS2, règlement sur l'intelligence artificielle. Ces textes ne sont pas de simples incitations — plusieurs de leurs dispositions s'imposeront aux administrations françaises avant la fin de ce plan. Aucun de ces domaines ne peut être décidé indépendamment des autres — c'est ce que signifie « intégrée ». Leur exécution doit suivre une séquence précise — c'est ce que signifie « séquencée ».

> **Note — Relation avec les sept axes du plan gouvernemental du 8 avril 2026 :** Le communiqué de la direction interministérielle du numérique identifie sept axes de dépendance dans les plans ministériels (poste de travail, outils collaboratifs, antivirus, intelligence artificielle, bases de données, virtualisation, équipements réseau). Ces sept axes correspondent aux domaines D2 à D5 et D9 du présent plan — ils y sont intégralement couverts. Les trois domaines supplémentaires de ce plan — la gouvernance (D1), la formation des agents (D6) et l'interopérabilité des formats (D8) — n'apparaissent pas dans le communiqué du 8 avril. Ils ne sont pas optionnels : Munich a échoué sans D6, la Basse-Saxe sans D2 et D8, la Corée du Sud sans D1 suffisamment ancré. Ce plan couvre les sept axes gouvernementaux et ajoute les trois conditions structurelles de leur succès. L'absence de ces trois conditions dans les plans ministériels à remettre à l'automne 2026 constituera le premier signal d'alerte.

6.1 Matrice d'interdépendances

Domaine	Déclenché par	Déclenche à son tour
D1 — Gouvernance	Décision politique + loi de finances	Tous les autres domaines
D4 — Cloud souverain	D1 (doctrine + budget)	D5 (IA hébergée) + D2 (applications portées vers le web hébergées)
D9 — Matériel (auditabilité)	D1 (révision des marchés publics)	Réduction des risques en chaîne d'approvisionnement matérielle
D2 — Applications métier	D1 (programme financé) + D6 (formation des équipes)	D3 — bloqué tant que les applications ne sont pas portées vers le web sur le périmètre
D6 — Formation agents	D1 (renforcement du Campus DINUM)	D3 — des postes migrés sans agents formés ne servent à rien
D5 — IA souveraine	D4 (cloud)	Réduction des usages d'intelligence artificielle hors cadre
D10 — Cybersécurité	D1 (ANSSI renforcée)	Protection des phases de transition
D3 — Poste de travail (Linux)	D2 (applications portées vers le web) + D6 (formation faite)	Ne jamais être déclenché sans D2 et D6 sur le périmètre concerné
D8 — Interopérabilité ODF	D1 (circulaire) + D2 (convertisseurs)	Réduction de la dépendance aux formats propriétaires dans les échanges
D7 — Formation scolaire	Décision ministère de l'Éducation nationale	Formation d'une génération numériquement agnostique à l'outil

6.2 La gouvernance : donner à la direction du numérique de l'État une autorité réelle

La direction interministérielle du numérique de l'État souffre d'une « instabilité administrative et stratégique » qui nuit à sa capacité de pilotage, selon la Cour des comptes dans son rapport de juillet 2024. Ce même rapport formule neuf recommandations dont trois sont applicables sans réforme législative : renforcer l'assise interministérielle de la direction (R1), créer une instance de gestion des ressources humaines de la filière numérique de l'État (R3), lui conférer un pouvoir de veto budgétaire sur les projets ayant reçu un avis défavorable de sa part (R8). Ces recommandations existent depuis dix mois. Elles n'ont pas encore été appliquées. Porter les effectifs de 180 à 350 agents techniques d'ici 2027 et sanctuariser 250 millions d'euros par an sur cinq ans constituent le programme minimal de mise à niveau.

6.3 Les applications métier : le verrou à lever en premier

Aucune étude publique française n'a, à ce jour, établi de façon consolidée et auditée la proportion d'applications de l'État incompatibles avec Linux. L'estimation de 35 à 50 % — retenue dans ce manifeste — est une estimation de raisonnement construite par analogie avec quatre cas internationaux documentés. À Munich, entre 20 et 40 % des postes n'ont jamais quitté Windows en raison d'applications métier incompatibles (Developpez.com, novembre 2017 ; LeMagIT, décembre 2017). En Basse-Saxe, une proportion non chiffrée mais « significative » d'applications métier incompatibles a motivé le retour à Windows en 2018 (CIO-Online, 2018). En Corée du Sud, les applications patrimoniales incompatibles sont citées comme première cause de retard sur l'objectif de migration (IT Brew, avril 2024). Au Schleswig-Holstein, la proportion d'applications nécessitant une adaptation est estimée supérieure à 30 % par les équipes techniques (EuroStack Directory, 2025). En France, la Cour des comptes, dans son rapport sur la DINUM de juillet 2024, identifie une « dette technique massive » dans les applications des administrations mais ne fournit pas de chiffrage des applications incompatibles avec des systèmes alternatifs. Cette estimation de 35 à 50 % doit être considérée comme un ordre de grandeur de raisonnement en l'absence d'audit national — et non comme un fait établi. Elle appelle un inventaire technique exhaustif, dont l'absence constitue elle-même un signal d'alerte : aucune migration nationale ne peut être conduite sérieusement sans connaître le périmètre réel de compatibilité applicative. Programme national de modernisation applicative (PNMA) en trois niveaux : portage vers le web (niveau 1, ciblant 60 % des applications), portage Linux natif (niveau 2, 25 %) et remplacement fonctionnel (niveau 3, 15 %). Le coût de ce programme n'a fait l'objet d'aucune étude publique consolidée à ce jour. Par analogie avec des programmes comparables en Europe (programme openDesk allemand — ZenDiS, 2025 ; Linux Foundation Europe, rapport 2023), il peut être estimé entre 5 et 10 milliards d'euros sur dix ans. Cette estimation doit faire l'objet d'un audit de coût total de possession indépendant et contradictoire avant tout engagement budgétaire.

6.4 Le cloud souverain : la priorité réglementaire et stratégique

La qualification SecNumCloud 3.2 de l'Agence nationale de la sécurité des systèmes d'information constitue le référentiel français de protection des données contre les législations extraterritoriales. Fin 2025, OVHcloud, Cloud Temple, Outscale (groupe Dassault Systèmes), Oodrive et S3NS disposent de certifications SecNumCloud 3.2.

> **Note spécifique sur S3NS :** S3NS est une coentreprise détenue à 95 % par Thales et à 5 % par Google. L'ensemble de la technologie sous-jacente provient de Google Cloud Platform. La qualification SecNumCloud garantit un cadre juridique français — elle ne garantit pas une indépendance technique vis-à-vis de Google. Héberger des données sur S3NS dans le cadre d'une doctrine de souveraineté structurelle est un choix de pragmatisme opérationnel assumé, non un choix de souveraineté complète. Pour les données relevant de la catégorie la plus sensible (secret de la défense, données judiciaires), S3NS ne constitue pas une réponse suffisante. Pour les usages collaboratifs courants, c'est une option de transition légitime, à condition d'être présentée comme telle et non comme l'équivalent d'un hébergeur 100 % européen.

6.5 L'intelligence artificielle souveraine

Depuis octobre 2025, 10 000 agents publics dans huit ministères testent l'Assistant IA, un assistant conversationnel basé sur le modèle Mistral Medium 3, hébergé par Outscale sur infrastructure

SecNumCloud. La première version du projet (Albert France Services) a été mise en pause en janvier 2026 suite à des dysfonctionnements. La version actuelle est plus robuste. Un bilan complet est attendu pour l'été 2026. Le budget de la direction du numérique de l'État consacré à l'intelligence artificielle s'établit à 1,2 million d'euros par an — largement insuffisant pour une généralisation. L'enjeu réglementaire est direct : les systèmes d'intelligence artificielle utilisés par des administrations pour des décisions affectant des droits relèvent du règlement européen sur l'intelligence artificielle, qui impose un audit de conformité que les modèles à code fermé satisferont difficilement.

6.6 Calendrier intégré — Horizon 2026-2036

Horizon	Domaines actifs	Jalons et décisions
2026 (immédiat)	D1, D4, D9	Appliquer R1/R3/R8 Cour des comptes. 100 % achats PC sans système d'exploitation. Audit de l'auditabilité du micrologiciel des équipements réseau. Audit TCO indépendant sur 3 ministères pilotes. Indicateur public mensuel de dépendance propriétaire.
2027–2028	D1, D2, D4, D5, D6	Portage applicatif des 200 premières applications standard. Cloud souverain pour 80 % des applications de l'État central. Assistant IA souverain sur 100 000 agents. Campus DINUM 500 formations par an.
2028–2030	D2, D3, D6, D7	Migration du système d'exploitation sur 500 000 postes bureautiques standard (périmètre porté vers le web). Formation scolaire révisée dans 50 % des académies. 10 % des équipements réseau d'origine européenne.
2030–2033	D3, D5, D8	Migration OS à 60 % du parc total (périmètre préparé). Intelligence artificielle souveraine pour 100 % des usages sur données sensibles. Format ouvert ODF quasi-exclusif en interne.
2033–2036	D3, D7	Migration OS à 80 % du parc. Résiduel Windows 15-20 % documenté et assumé. Formation scolaire révisée dans 90 % des académies.

7. Trois scénarios prospectifs — Le coût réel de chaque option

Toute décision publique se prend en comparant des scénarios, jamais en comparant l'action à l'inaction. Cette section présente les trois trajectoires réalistes pour la décennie 2026-2036 — leurs coûts, leurs risques et ce qu'elles produisent réellement en matière de souveraineté. Les chiffres sont des projections de raisonnement, pas des certitudes : ils appellent un audit indépendant avant tout engagement budgétaire. Leur seul objectif est de montrer que les trois options ne coûtent pas la même chose.

7.1 Scénario A — Le statu quo : décider de ne pas décider

Ce scénario ne consiste pas à rester immobile — il consiste à continuer sur la trajectoire actuelle, en renouvelant les contrats Microsoft, en migrant vers Windows 11, et en adoptant les outils d'intelligence artificielle intégrés à l'écosystème propriétaire. C'est le choix qui demande le moins d'effort à court terme et le plus de ressources à long terme.

- Coût des licences logicielles sur dix ans : la base de départ retenue est une dépense annuelle estimée entre 500 et 700 millions d'euros pour l'ensemble du secteur public en licences Microsoft (État central, collectivités, hôpitaux) — fourchette de raisonnement non auditée de façon consolidée. Après application d'une hausse moyenne retenue de 10 % en juillet 2026 — fourchette conservatrice correspondant aux plans secteur public (5 % à 13 % selon les offres ; annonce Microsoft du 4 décembre 2025, confirmée par ChannelNews et Banque des Territoires) — puis d'une progression de 5 % par an, la facture cumulée sur dix ans s'établit entre 8 et 10 milliards d'euros. Toute nouvelle hausse non prévue — que rien ne permet d'exclure au vu du comportement tarifaire documenté de l'éditeur — déplace ce plafond vers le haut.
- Coût du renouvellement matériel imposé par Windows 11 : les exigences techniques de Windows 11 (processeur TPM 2.0 requis) excluent entre 20 et 30 % des postes existants. Sur un parc de 3,5 millions de postes, cela représente entre 700 000 et 1 million de machines à remplacer sans nécessité fonctionnelle — coût estimé entre 560 millions et 800 millions d'euros.
- Aucun levier de négociation tarifaire : en l'absence d'alternative crédible documentée, tout refus de payer se traduit par une rupture de service. Microsoft le sait. C'est la définition d'une dépendance captive.
- Exposition juridique croissante : le CLOUD Act américain et le FISA s'appliquent à toutes les données hébergées chez des acteurs soumis au droit américain, y compris sur sol européen. La probabilité d'une réquisition liée à un différend diplomatique ou commercial entre les États-Unis et la France n'est pas nulle — et elle ne diminue pas avec le temps.

7.2 Scénario B — La migration partielle : l'illusion de la souveraineté

Ce scénario consiste à migrer les postes de travail vers Linux sans avoir préalablement préparé les applications et les agents. C'est le scénario le plus dangereux politiquement : il génère un signal de transformation sans produire de résultat réel, et sa probabilité d'échec documentée est supérieure à 80 %.

- Munich, Basse-Saxe, Corée du Sud ont toutes emprunté cette voie. Le coût direct de Munich — 50 millions d'euros pour le retour à Windows, dans un projet total de 89 millions — ne compte pas le coût indirect : dix ans de perte de confiance dans la transformation numérique publique.
- À l'échelle de l'État français (parc quarante fois plus grand que Munich), un retour arrière coûterait entre 2 et 4 milliards d'euros et retarderait de dix ans toute nouvelle tentative.
- Ce scénario produit une apparence de souveraineté sur le poste de travail tout en maintenant la dépendance structurelle sur le cloud, sur l'intelligence artificielle et sur les applications métier — qui sont, en 2026, les vecteurs de dépendance les plus critiques.

7.3 Scénario C — La transformation intégrée (ce manifeste)

Ce scénario suit le plan décrit dans ce document : planification intégrée des dix domaines, exécution séquencée applications avant-postes, sanctuarisation de la gouvernance et du financement. C'est le scénario le plus exigeant à court terme et le moins coûteux à long terme.

- Portage applicatif : entre 5 et 10 milliards d'euros sur dix ans (estimation de raisonnement non auditée).
- Économies sur les licences logicielles à partir de l'année 6 ou 7 : environ 500 millions d'euros par an, soit 2 à 3 milliards d'euros sur les quatre dernières années de la décennie.
- Coût net sur dix ans : entre 4 et 7 milliards d'euros, en comparaison d'un scénario A à 10-12 milliards.
- Retour sur investissement : positif à partir de l'année 8 ou 9, selon le rythme réel de portage applicatif.
- Dividende de souveraineté : reprise d'un levier de négociation réel face aux éditeurs, conformité structurelle aux obligations NIS2 et CRA, indépendance juridique vis-à-vis du CLOUD Act.

7.4 Tableau de comparaison des trois scénarios

Critère	A — Statu quo (aucune décision)	B — Migration partielle (OS sans applications)	C — Transformation intégrée (ce manifeste)
Coût estimé sur 10 ans	10 à 12 Md€ (licences + renouvellement matériel imposé par Windows 11 ~800 M€ + hausses tarifaires prévisibles)	10 à 14 Md€ : coût du statu quo + migration OS ~500 M€ + retour arrière probable ~2 à 4 Md€	4 à 7 Md€ nets (PNMA ~5-10 Md€, économies licences dès l'an 7 ~500 M€/an)
Niveau de dépendance en 2035	Dépendance maximale. Aucun levier de négociation. Exposition juridique au droit américain structurelle.	Apparence de souveraineté sur l'OS. Dépendance totale sur le cloud, l'IA et les applications.	Dépendance structurellement réduite. Souveraineté réelle sur les données, le cloud et les usages courants.
Résultat probable	Dépendance structurellement renforcée. Aucun levier de négociation. Exposition juridique croissante.	Taux d'échec observé dans les cas documentés (Munich, Basse-Saxe, Corée du Sud) : supérieur à 80 %. La répétition de Munich à l'échelle nationale est le scénario le plus probable.	Résultat positif estimé par analogie avec les cas de succès — sous réserve de réunir les conditions de gouvernance (loi de programmation, autorité de pilotage réelle, financement sanctuarisé).
Risque réglementaire	NIS2 et CRA imposent des obligations de sécurité que les outils propriétaires non auditables satisferont avec difficulté	Idem — l'OS seul n'adresse pas les obligations NIS2/CRA sur la chaîne d'approvisionnement logicielle	Conforme par construction — logiciels libres auditables, inventaire des composants logiciels obligatoire
Signal politique	Aucun. Dépendance assumée, acceptée, finançable indéfiniment.	Signal fort, résultat nul ou contre-productif. Le plus dangereux politiquement.	Signal fort avec résultats mesurables à 3 ans (Tchap, cloud souverain, IA souveraine) et 10 ans (OS).

Mise en garde méthodologique : Toutes les estimations financières de cette section sont des projections de raisonnement construites à partir de données partielles. Elles ne constituent pas un audit. Avant tout engagement budgétaire, un audit de coût total de possession (TCO) indépendant et contradictoire est indispensable. Ces chiffres ont pour seul objectif de montrer que les trois scénarios ne sont pas équivalents économiquement — ils montrent que le statu quo est le plus coûteux des trois.

8. Évaluation des risques

8.1 Risques politiques et institutionnels

Risque	Description et enjeux	Niveau
Instabilité de gouvernance	Onze ans de circulaires sans résultat probant (2012-2026). Sans ancrage législatif, chaque alternance remet à zéro des années de travail. C'est le risque le plus structurant.	**CRITIQUE**
Pression des éditeurs propriétaires	Munich a cédé en 2017 après une offre de rabais. L'Éducation nationale a signé un contrat significatif avec Microsoft en 2025 malgré la doctrine souveraine. La probabilité d'une tentative est certaine — la réponse doit être une alternative crédible en place, non une résolution de principe.	**CRITIQUE**
Substitution symbolique	Migrer les postes vers Linux tout en hébergeant les données sur un cloud américain et en adoptant des outils d'intelligence artificielle propriétaires. Souveraineté de façade, dépendance de fond.	**ÉLEVÉ**
Fragmentation interministérielle	Sans coordination contraignante, chaque ministère adopte sa propre approche. L'hétérogénéité produite est plus coûteuse à gérer que l'homogénéité propriétaire — c'est la leçon de Munich.	**ÉLEVÉ**

8.2 Risques techniques

Risque	Description et enjeux	Niveau
Violation du séquençage	Migrer le poste de travail avant les applications du périmètre. Cause directe de Munich, Basse-Saxe et Corée du Sud. Aucune exception documentée dans les cas de succès.	**CRITIQUE**
Retard de formation post-déploiement	Schleswig-Holstein 2025 : 80 % de postes migrés, moins de 80 % d'agents compétents. Neuf millions d'euros de rattrapage. Ce risque est systématiquement sous-estimé dans les plans initiaux.	**ÉLEVÉ**
Compromission de la chaîne d'approvisionnement logicielle	Porte dérobée XZ Utils (CVE-2024-3094, mars 2024). Un parc homogène massif constitue une cible prévisible. La nomenclature des composants logiciels obligatoire est la réponse structurelle.	**ÉLEVÉ**
Interopérabilité ODF dégradée	Pertes de fidélité réelles sur macros et mises en forme complexes sans convertisseur professionnel certifié.	**MODÉRÉ**

8.3 Risques financiers

Risque	Description et enjeux	Niveau
Sous-estimation systématique des coûts	Munich : 23 millions investis dans LiMux, ~50 millions pour en sortir. Les postes de formation, de perte temporaire de productivité et de portage applicatif sont systématiquement absents des estimations initiales. Marge prudentielle recommandée : 30 à 50 %.	**CRITIQUE**
Programme de PNMA non financé	Estimé entre 5 et 10 milliards d'euros sur dix ans (estimation de raisonnement non auditée). Absent de tous les dossiers de justification budgétaire actuels. Sans ce financement, aucune migration du poste de travail n'est possible.	**CRITIQUE**
Surcoût cloud souverain non absorbé	Les services qualifiés SecNumCloud sont 30 à 50 % plus chers que leurs équivalents AWS ou Azure. Pour les collectivités aux budgets contraints, ce surcoût peut conduire à des contournements informels.	**ÉLEVÉ**

9. Portraits de résistance — Et comment les dépasser

Tout document de transformation génère trois types de résistance. Aucune n'est irrationnelle. Chacune exprime une peur légitime, mal adressée. Cette section identifie le profil réel derrière chaque posture, formule la vraie question sous-jacente, et y répond avec les arguments les plus forts disponibles — pas les plus faciles.

9.1 — Le souverainiste dogmatique

Ce manifeste vous donnera raison en vous donnant tort.

Qui est-il vraiment ? Il a lu Snowden. Il connaît le CLOUD Act sur le bout des doigts. Sa colère est réelle et son diagnostic juste. Mais la certitude de son analyse l'a, imperceptiblement, glissé vers une position où la perfection de la solution est devenue le seul critère d'acceptabilité. Et comme la perfection n'existe pas aujourd'hui — avec les acteurs disponibles — aucune proposition concrète ne lui convient jamais entièrement. Il risque ainsi de devenir, malgré lui, le meilleur allié de ceux qu'il combat.

Sa vraie question : « Vingt ans de transition, c'est plus long que la durée de vie de la menace. Dans vingt ans, les dépendances auront migré vers l'intelligence artificielle et les algorithmes — et nous aurons migré des postes de travail devenus secondaires. »

C'est l'objection la plus forte et la moins souvent entendue dans ce débat. Elle mérite une réponse directe. Première réponse : ce manifeste ne propose pas de migrer uniquement les postes de travail sur vingt ans. Il propose de traiter simultanément — dans sa phase de planification — les dix domaines : cloud, intelligence artificielle, matériel, formation, interopérabilité. Le calendrier de déploiement couvre l'ensemble. Deuxième réponse : la fenêtre critique pour l'intelligence artificielle est maintenant, pas dans vingt ans. L'Assistant IA basé sur Mistral Medium 3 est déjà en expérimentation. L'infrastructure cloud souveraine existe. Les obligations réglementaires du règlement européen sur l'intelligence artificielle s'appliquent dès 2026. La question de la souveraineté sur l'IA est traitée dans ce manifeste — elle ne se substitue pas à la question du poste de travail, elle s'y ajoute. Troisième réponse : refuser une trajectoire de vingt ans au motif que les menaces évolueront, c'est refuser de construire une autoroute en 1960 parce que les voitures allaient plus

vite en 2000. La méthode reste juste même si le contexte change — et elle est la seule qui garantisse de ne pas reproduire Munich.

Ce que ce manifeste lui demande : diriger sa radicalité vers la gouvernance et le financement — les deux seuls leviers qui font la différence entre une doctrine et une déclaration d'intention. Sur ces deux points, aucun compromis n'est demandé.

9.2 — Le technicien sceptique

Ce manifeste a besoin de vous. Pas de votre conversion — de votre vigilance.

Qui est-il vraiment ? Ce n'est pas un défenseur de Microsoft. C'est un professionnel qui a vu, de près, la distance abyssale entre ce que les décideurs annoncent et ce que les équipes techniques reçoivent à exécuter. Il connaît LOUVOIS — 400 millions d'euros de pertes pour des payes de militaires mal calculées. Il connaît Parcoursup version 1. Il a lu le rapport de la Cour des comptes sur la direction du numérique de l'État. Sa méfiance n'est pas du cynisme : c'est de la mémoire professionnelle.

Sa vraie question : « Ce programme survivrait-il à trois changements de majorité ? Avez-vous un seul exemple de programme numérique de l'État ayant tenu ses engagements sur dix ans ? »

Voici la réponse honnête : non, il n'y en a pas beaucoup. Et ce manifeste ne prétend pas que la transformation décrite ici sera sans turbulences. Ce qu'il affirme, c'est que les conditions de l'échec sont parfaitement documentées — et que l'absence d'ancrage législatif est systématiquement présente dans chaque cas d'échec. C'est précisément pourquoi ce document recommande une loi de programmation numérique, l'application des recommandations de la Cour des comptes qui ont déjà une légitimité institutionnelle indépendante de tout gouvernement, et un indicateur public mensuel qui met la pression sur toute administration qui dévie de la trajectoire. La vraie réponse à votre question n'est pas 'le programme survivra' — c'est 'voici les mécanismes qui augmentent cette probabilité, et voici les signes qui indiqueront à temps que ça dérape'. Ce manifeste décrit les deux. Il sera utile dans dix ans à quiconque voudra vérifier si la transformation a été conduite correctement. Y compris vous.

Ce que ce manifeste lui demande : non pas croire — surveiller. Exiger les indicateurs publics, pointer les incohérences entre le calendrier annoncé et le portage applicatif réel, demander les audits contradictoires.

9.3 — Le décideur non acculturé au numérique

Ce manifeste a quelque chose d'important à vous dire : vous n'êtes pas le problème.

Qui est-il vraiment ? Il n'est pas ignorant — il est passé à côté d'un débat dont personne ne lui a jamais expliqué pourquoi il le concernait directement. Il gère une commune, dirige un hôpital de proximité, préside un conseil départemental. Il a des préoccupations concrètes et une impression légitime que les discussions sur les systèmes d'exploitation appartiennent à un monde très loin du sien. Ce n'est pas de la résistance — c'est de l'indifférence raisonnée face à un débat mal présenté.

Sa vraie question : « En quoi le fait que mes agents utilisent Windows ou Linux change quelque chose à la qualité du service public que je dois rendre ? »

La réponse ne passe pas par Linux. Elle passe par une image concrète : imaginez que tous les dossiers de votre collectivité — actes d'état civil, dossiers d'aide sociale, instructions de marchés publics, données de santé de vos administrés — soient stockés dans les armoires d'un prestataire étranger privé qui peut légalement en ouvrir l'accès à son gouvernement d'origine, sans vous en informer, et qui vient d'annoncer qu'il augmente ses tarifs de 5 % à 33 % selon les offres à partir du 1er juillet 2026. Vous n'avez pas d'autre prestataire. Et ce prestataire, ce n'est pas une hypothèse de fiction administrative : c'est Microsoft, AWS ou Google, auxquels la quasi-totalité des systèmes d'information publics français sont aujourd'hui liés par des contrats pluriannuels sans alternative documentée. Ce risque juridique est établi par deux arrêts de la Cour de justice de l'Union européenne — Schrems I (C-362/14, 2015) et Schrems II (C-311/18, 2020) — qui ont constaté que la surveillance américaine sur les données hébergées en Europe chez des filiales d'entreprises américaines est incompatible avec les droits fondamentaux européens. Avez-vous été alerté que Microsoft applique des hausses tarifaires de 5 % à 33 % selon les offres à compter du 1er juillet 2026, avec une hausse de 10 % sur les plans les plus courants du secteur public (annonce officielle Microsoft, 4 décembre 2025) ? Que la réglementation européenne NIS2, en cours de transposition en droit français, va vous imposer des obligations de sécurité informatique que votre contrat actuel rend difficiles à satisfaire ? Ce n'est pas une question de logiciels. C'est une question d'infrastructure publique souveraine.

Ce que ce manifeste lui demande : poser à sa direction informatique deux questions précises : quel est notre plan si les tarifs Microsoft augmentent à nouveau de 30 % en 2029 ? Et où sont hébergées nos données les plus sensibles, sous quel droit, et avec quelles garanties d'accès exclusif ?

Conclusion

Ce que l'analyse de ce document établit, section après section, peut se résumer en quatre constats.

Premier constat : la transformation est techniquement prouvée. La Gendarmerie nationale a migré 103 000 postes sur vingt ans, sans rupture de service, avec des économies mesurables et documentées. Le Schleswig-Holstein progresse. La convergence civil-militaire autour de logiciels libres se concrétise en Allemagne. L'argument technique contre la faisabilité n'existe plus — seul subsiste l'argument sur les conditions.

Deuxième constat : le statu quo est le scénario le plus coûteux des trois. Les hausses tarifaires de Microsoft en 2026 (de 5 % à 33 % selon les offres, annonce du 4 décembre 2025), le renouvellement de matériel imposé par Windows 11, la trajectoire tarifaire documentée des éditeurs et l'exposition juridique au droit américain font du « ne rien faire » une option dont le coût cumulé sur dix ans dépasse celui d'une transformation bien menée. Ce n'est plus un argument de souveraineté abstraite — c'est un argument financier concret que tout directeur financier d'administration peut vérifier.

Troisième constat : les conditions de l'échec sont aussi bien documentées que les conditions du succès. Munich, Basse-Saxe, Barcelone, Corée du Sud ont fourni un corpus de cas négatifs précis. Chaque fois, la même cause : une migration du poste de travail sans préparation des applications, sans formation préalable des agents, sans continuité institutionnelle. Ce document ne prétend pas que la transformation réussira si ces conditions sont réunies — il affirme qu'elle échouera si elles ne le sont pas.

Quatrième constat — la contribution analytique originale de ce document : la conformité aux règlements européens de protection des données ne constitue pas une protection contre les mécanismes d'accès extraterritoriaux américains. Le Data Privacy Framework, validé par le Tribunal de l'Union européenne le 3 septembre 2025 (affaire T-553/23), régit la légalité des transferts de données entre entités privées au titre du Chapitre V du RGPD. Le CLOUD Act (18 U.S.C. § 2713, art. 103(a), Pub.L. 115-141), le FISA Section 702 (50 U.S.C. § 1881a) et l'Executive Order 12333 opèrent sur un registre entièrement distinct : ils donnent aux forces de l'ordre et aux agences de renseignement américaines le droit d'accéder aux données hébergées par des entreprises soumises à la juridiction américaine, indépendamment de tout accord transatlantique. Le directeur des affaires publiques et juridiques de Microsoft France l'a confirmé sous serment devant la commission d'enquête sénatoriale le 10 juin 2025 (Sénat, senat.fr/compte-rendu-commissions/20250609/ce_commande_publique.html ; Techniques de l'Ingénieur, 6 août 2025 ; Usine Digitale, 22 juillet 2025) : « Non, je ne peux pas garantir que les données des citoyens français ne seront jamais transmises au gouvernement américain. » Cette déclaration, faite sous serment devant une commission d'enquête officielle de la République française, constitue la base factuelle institutionnelle la plus précise disponible sur l'exposition structurelle au CLOUD Act. Un décideur public qui l'a lue dispose désormais de l'information nécessaire pour instruire cette décision en connaissance de cause.

La conséquence décisionnelle est simple. L'État dispose déjà d'un début de réponse : des outils souverains en production, une infrastructure cloud qualifiée, un assistant d'intelligence artificielle en cours d'expérimentation, et des recommandations de la Cour des comptes qui n'attendent qu'une décision politique pour être appliquées. Il ne manque pas un plan — il manque une autorité pour le tenir, un budget pour le financer, et une instruction pour que les achats d'ordinateurs cessent d'inclure par défaut le système d'exploitation de l'éditeur. Trois décisions. Aucune révolution.

« Oui, c'est possible. Mais seulement si vous l'abordez de manière intégrée, séquencée et sanctuarisée. »

Analyse indépendante produite en avril 2026, à partir des corpus documentaires cités en couverture. Les faits sont sourcés, les opinions argumentées, les limites nommées. Les estimations financières sont des projections de raisonnement qui nécessitent un audit indépendant avant tout engagement budgétaire.

Annexe — Bibliographie complète

Toutes les sources utilisées dans ce document sont listées ci-dessous par catégorie. Les sources primaires (textes officiels, comptes rendus institutionnels, décisions de juridiction) sont distinguées des sources secondaires (presse spécialisée, publications sectorielles). Les sources primaires ont été vérifiées directement sur les sites institutionnels à la date de finalisation du document (avril 2026).

I. Sources juridiques et réglementaires primaires

Textes législatifs européens

- Règlement (UE) 2024/2847 du Parlement européen et du Conseil relatif aux exigences horizontales de cybersécurité applicables aux produits comportant des éléments numériques (Cyber Resilience Act — CRA). Journal officiel de l'Union européenne, 20 novembre 2024. EUR-Lex : eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32024R2847
- Directive (UE) 2022/2555 du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (NIS2). Journal officiel de l'Union européenne, 27 décembre 2022. EUR-Lex : eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32022L2555
- Règlement (UE) 2024/1689 du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (AI Act). Journal officiel de l'Union européenne, 12 juillet 2024. EUR-Lex : eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32024R1689
- Règlement (UE) 2018/1725 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union. Journal officiel de l'Union européenne, 23 octobre 2018.
- Décision d'adéquation de la Commission européenne 2023/1795 relative au Data Privacy Framework (cadre de protection des données UE–États-Unis). Journal officiel de l'Union européenne, 10 juillet 2023.

Textes législatifs français

- Circulaire du Premier ministre Jean-Marc Ayrault, n°35837, du 19 septembre 2012 : Orientations pour l'usage des logiciels libres dans l'administration. Légifrance : legifrance.gouv.fr/circulaire/id/35837
- Loi n°2016-1321 du 7 octobre 2016 pour une République numérique, article 16 (Socle Interministériel de Logiciels Libres). Journal officiel de la République française, 8 octobre 2016. Légifrance : legifrance.gouv.fr/loi/id/JORFTEXT000033202746
- Référentiel Général d'Interopérabilité (RGI), première version. Direction générale de la modernisation de l'État (DGME), 2009. Disponible sur : numerique.gouv.fr

Textes législatifs américains

- Clarifying Lawful Overseas Use of Data Act (CLOUD Act), art. 103(a), Pub.L. 115-141, div. V. Promulgué le 23 mars 2018. Codifié au 18 U.S.C. § 2713. Texte intégral : congress.gov/bill/115th-congress/house-bill/4943/text ; law.cornell.edu/uscode/text/18/2713
- Foreign Intelligence Surveillance Act (FISA), Section 702 (50 U.S.C. § 1881a). Adoptée en 2008 dans le cadre du FISA Amendments Act. Réautorisée en 2024 par le Reforming Intelligence and Securing America Act (RISAA, H.R.7888). Sunset prévu au 20 avril 2026.
- Executive Order 12333, signé par le président Reagan le 4 décembre 1981, modifié par les Executive Orders 13355 (2004) et 13470 (2008). Texte : archives.gov

II. Arrêts et décisions juridictionnelles

- Cour de justice de l'Union européenne, arrêt Schrems I, 6 octobre 2015, affaire C-362/14, Maximillian Schrems c/ Data Protection Commissioner. Invalidation de la décision Safe Harbor.
- Cour de justice de l'Union européenne, arrêt Schrems II, 16 juillet 2020, affaire C-311/18, Data Protection Commissioner c/ Facebook Ireland Limited et Maximillian Schrems. Invalidation du Privacy Shield.
- Tribunal de l'Union européenne, ordonnance en référé du 12 octobre 2023, affaire T-553/23, Philippe Latombe c/ Commission européenne. Rejet de la demande de mesures provisoires.
- Tribunal de l'Union européenne, arrêt du 3 septembre 2025, affaire T-553/23, Philippe Latombe c/ Commission européenne. Rejet du recours en annulation du Data Privacy Framework. (Source : Silicon.fr, 4 septembre 2025 ; La Revue — Squire Patton Boggs, décembre 2025)
- Tribunal de l'Union européenne, affaires T-262/24 et T-265/24 (recours contre la décision EDPS du 8 mars 2024 relative à Microsoft 365). Procédures en cours en avril 2026.
- Autorité européenne de protection des données (EDPS), décision du 8 mars 2024 (communiqué de presse du 11 mars 2024). Constat de violation du règlement (UE) 2018/1725 par la Commission européenne dans l'utilisation de Microsoft 365. Source primaire : edps.europa.eu/data-protection/our-work/publications/investigations/2024-03-08-edps-investigation-european-commissions-use-microsoft-365_en

III. Sources institutionnelles françaises

- Direction interministérielle du numérique (DINUM). Communiqué officiel du séminaire interministériel du 8 avril 2026 sur la réduction des dépendances numériques extra-européennes. numerique.gouv.fr
- Élysée.fr. Décret de nomination de Sébastien Lecornu comme Premier ministre, 10 octobre 2025. elysee.fr
- Service d'information du Gouvernement. Composition du gouvernement Lecornu II publiée au Journal officiel du 26 février 2026. info.gouv.fr
- Sénat, commission d'enquête sur les coûts et les modalités effectifs de la commande publique. Compte rendu de l'audition de Microsoft France (Anton Carniaux et Pierre Lagarde), séance du mardi 10 juin 2025. Source primaire : senat.fr/compte-rendu-commissions/20250609/ce_commande_publique.html
- Assemblée nationale. Dossier législatif n°50731, projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité. assemblee-nationale.fr/dyn/17/dossiers/DLR5L17N50731
- Sénat. Rapport n°393 sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, mars 2025. senat.fr
- Commission supérieure du numérique et des postes (CSNP). Avis sur le schéma européen de certification des services cloud (EUCS), 4 septembre 2024.
- Commission supérieure du numérique et des postes (CSNP). Communiqué demandant l'inscription urgente du projet de loi Résilience, 18 mars 2026. banquedesterritoires.fr
- Cour des comptes. Rapport sur la direction interministérielle du numérique, juillet 2024. ccomptes.fr
- Anne Le Hénanff, ministre déléguée chargée de l'Intelligence artificielle et du Numérique. Réponse à question écrite, Journal officiel de l'Assemblée nationale, janvier 2026.
- Vie-publique.fr. Fiche du projet de loi relatif à la résilience des infrastructures critiques, octobre 2025. vie-publique.fr

IV. Sources institutionnelles européennes et internationales

- Commission européenne. Décision d'adéquation DPF 2023/1795, 10 juillet 2023. ec.europa.eu
- Agence de l'Union européenne pour la cybersécurité (ENISA). Travaux sur l'European Union Cybersecurity Certification Scheme for Cloud Services (EUCS), versions 2022–2024. enisa.europa.eu
- ZenDiS (Centre pour la souveraineté numérique de l'administration allemande) et BWI GmbH. Accord-cadre de sept ans pour le déploiement d'openDesk dans les forces armées allemandes, 2025. opendesk.eu
- Nextgov/FCW. « Judge renews procedures for 702 surveillance program that could soon lapse. » 11 avril 2026. nextgov.com
- Brennan Center for Justice. Section 702 of the Foreign Intelligence Surveillance Act (FISA) : 2026 Resource Page. brennancenter.org
- American Prospect. « Warrantless Spying Reform Just Got a Whole Lot More Interesting. » Mars 2026. prospect.org

V. Sources de presse spécialisée françaises

- Acteurs Publics. « Comment l'Intérieur tente de faire freiner la transposition de la loi Résilience et Cybersécurité. » 4 février 2026. acteurspublics.fr
- April (Association de promotion et de défense du logiciel libre). Communiqué de presse sur le séminaire DINUM du 8 avril 2026. april.org, 10 avril 2026.
- Banque des Territoires. « Face à l'augmentation des licences de Microsoft, la bureautique libre pousse son avantage. » 12 décembre 2025. banquedesterritoires.fr
- Banque des Territoires. « Cloud souverain : la révision à la baisse des objectifs européens agace. » Octobre 2024. banquedesterritoires.fr
- Banque des Territoires. « Cybersécurité : la CSNP presse le Parlement d'examiner sans délai le projet de loi de résilience transposant NIS 2. » 18 mars 2026. banquedesterritoires.fr
- ChannelNews. « Microsoft annonce des hausses jusqu'à 33 % des prix d'abonnement pour Microsoft 365. » 5 décembre 2025. channelnews.fr
- CIO-Online. « Gendarmerie nationale, la migration libre à grande échelle. » Janvier 2008. cio-online.com
- CIO-Online. « Le nouvel accord transatlantique pour les données à caractère personnel déjà sous le feu des critiques. » Septembre 2024. cio-online.com
- CIO-Online. « EUCS, la certification cloud européenne qui menace de désarmer SecNumCloud. » Septembre 2024. cio-online.com
- Clubic. « Microsoft face au Sénat : l'aveu qui fait vaciller la souveraineté numérique française. » Juillet 2025. clubic.com
- Clubic. Article sur le séminaire DINUM du 8 avril 2026. 9 avril 2026. clubic.com
- Developpez.com. « Munich et sa migration LiMux vers Linux : voici les vraies raisons du retour à Windows. » Novembre 2017. developpez.com
- Developpez.com. « Schleswig-Holstein : bilan de la migration Linux. » Décembre 2025. developpez.com
- Developpez.com. « Séminaire DINUM du 8 avril 2026. » 9 avril 2026. developpez.com
- Framablog. Article sur le séminaire DINUM du 8 avril 2026. Mars 2026. framablog.org
- GoodTech. Article sur le séminaire DINUM du 8 avril 2026. 9 avril 2026.
- INCYBER NEWS. « EUCS, le rêve d'un cloud souverain européen au pied du mur. » Juin 2025. incyber.org
- IT for Business. « EUCS : La directive cloud au centre de l'État en péril. » Avril 2024. itforbusiness.fr
- IT for Business. « EUCS, le va-tout (très) risqué de la France sur le niveau High+. » Mai 2025. itforbusiness.fr

- IT-Connect. « Microsoft 365 en 2026 : plus de fonctionnalités, des tarifs en hausse. » 4 décembre 2025. it-connect.fr
- IT-Connect. Article sur le séminaire DINUM du 8 avril 2026. 9 avril 2026. it-connect.fr
- Le Monde Informatique. « Hausse des prix de Microsoft 365 pour les entreprises en 2026. » 5 décembre 2025. lemondeinformatique.fr
- LeMagIT. « Munich : le retour à Windows 10. » Décembre 2017. lemagit.fr
- LeMagIT. « Barcelone : lancement de la migration Ubuntu. » Janvier 2018. lemagit.fr
- Mac4ever. Article sur le séminaire DINUM du 8 avril 2026. 9 avril 2026. mac4ever.com
- Next.ink. « Microsoft 365 : hausses de prix à venir pour les entreprises et le secteur public. » Décembre 2025. next.ink
- Orange Cyberdefense. « Tout sur NIS2 en 2025 — mise à jour mars 2026. » 17 mars 2026. orangecyberdefense.com
- Silicon.fr. « Pourquoi la CJUE n'a pas invalidé le Data Privacy Framework. » 4 septembre 2025. silicon.fr
- Techniques de l'Ingénieur. « Microsoft avoue ne pas garantir la confidentialité des données. » 6 août 2025. techniques-ingenieur.fr
- Usine Digitale. « Oui, Microsoft peut transmettre les données des Français aux États-Unis… et ce n'est pas nouveau. » 22 juillet 2025. usine-digitale.fr
- Usine Digitale. « Alors que l'Europe s'inquiète de sa dépendance numérique... Microsoft relève les tarifs d'Office 365. » 5 décembre 2025. usine-digitale.fr
- Usine Digitale. « Stratégie nationale de cybersécurité : Malgré ses injonctions aux entreprises, l'État traîne les pieds sur NIS 2. » Janvier 2026. usine-digitale.fr
- Wikipedia. Article « GendBuntu ». Consulté en février 2026. fr.wikipedia.org
- WEKA/AFP. Article sur la transformation numérique de l'État français. Janvier 2026.

VI. Sources de presse spécialisée internationales

- EuroStack Directory. Répertoire des initiatives européennes de logiciels libres. Mars 2025. eurostack.eu
- IT Brew. « South Korea Linux migration : four years later. » Avril 2024. itbrew.com
- LibreOffice Conference 2024. Présentations sur la migration Schleswig-Holstein vers LibreOffice.
- Linux Foundation Europe. Rapport 2023 sur les migrations de logiciels libres dans le secteur public européen. linuxfoundation.eu
- opendesk.eu. Informations sur le programme openDesk (ZenDiS, Bundeswehr). Consulté en 2025. opendesk.eu
- The Register. « Schleswig-Holstein moves to Linux for 30,000 civil servants. » Avril 2024. theregister.com
- Wikipedia. Article « Logiciels libres et open source dans l'administration » (Free and open-source software in government). Consulté en avril 2026. en.wikipedia.org

VII. Sources documentaires internes et académiques

- Connect LP-125. Lieutenant-colonel Dumond, Gendarmerie nationale. Retour d'expérience sur la migration GendBuntu. 2021. (Revue interne Gendarmerie nationale.)
- LibreCon Bilbao 2014. Présentation sur la migration GendBuntu et les leçons de méthode.
- Sénat, Questions de l'Assemblée nationale n°482 (session 2024). Renouvellement du FISA section 702. questions.assemblee-nationale.fr

Note méthodologique : Les sources primaires sont définies comme les textes législatifs officiels, les comptes rendus institutionnels, les décisions judiciaires et les communiqués officiels accessibles directement sur les sites des institutions. Les sources secondaires sont les publications journalistiques, sectorielles ou associatives qui rapportent, analysent ou commentent ces sources primaires. Lorsqu'une même information est disponible à la fois dans une source primaire et une source secondaire, la source primaire a été vérifiée et est citée en priorité. Plusieurs sources secondaires sont citées pour les faits qui ont été rapportés de façon concordante par plusieurs publications indépendantes.