Cour des comptes

PREMIÈRE CHAMBRE

S2025-1479

QUATRIÈME SECTION

OBSERVATIONS DÉFINITIVES

(Article R. 143-11 du code des juridictions financières)

LES ENJEUX DE SOUVERAINETÉ DES SYSTÈMES D'INFORMATION CIVILS DE L'ÉTAT

Le présent document, qui a fait l'objet d'une contradiction avec les destinataires concernés, a été délibéré par la Cour des comptes, le 11 septembre 2025.

TABLE DES MATIÈRES

PROCEDURES ET METHODES

Les rapports de la Cour des comptes sont réalisés par l'une des six chambres thématiques[1] que comprend la Cour ou par une formation associant plusieurs chambres et/ou plusieurs chambres régionales ou territoriales des comptes.

Trois principes fondamentaux gouvernent l'organisation et l'activité de la Cour ainsi que des chambres régionales et territoriales des comptes, donc aussi bien l'exécution de leurs contrôles et enquêtes que l'élaboration des rapports publics : l'indépendance, la contradiction et la collégialité.

L'**indépendance** institutionnelle des juridictions financières et l'indépendance statutaire de leurs membres garantissent que les contrôles effectués et les conclusions tirées le sont en toute liberté d'appréciation.

La **contradiction** implique que toutes les constatations et appréciations faites lors d'un contrôle ou d'une enquête, de même que toutes les observations et recommandations formulées ensuite, sont systématiquement soumises aux responsables des administrations ou organismes concernés ; elles ne peuvent être rendues définitives qu'après prise en compte des réponses reçues et, s'il y a lieu, après audition des responsables concernés.

La **collégialité** intervient pour conclure les principales étapes des procédures de contrôle et de publication. Tout contrôle ou enquête est confié à un ou plusieurs rapporteurs. Le rapport d'instruction, comme les projets ultérieurs d'observations et de recommandations, provisoires et définitives, sont examinés et délibérés de façon collégiale, par une formation comprenant au moins trois magistrats. L'un des magistrats assure le rôle de contre-rapporteur et veille à la qualité des contrôles.

Sauf pour les rapports réalisés à la demande du Parlement ou du Gouvernement, la publication d'un rapport est nécessairement précédée par la communication du projet de texte que la Cour se propose de publier, pour exercice de leur droit de réponse, aux ministres, directeurs d'administration centrale ou chefs de service intéressés (selon les cas) et aux responsables des organismes concernés, ainsi qu'aux autres personnes morales ou physiques directement intéressées. Leurs réponses sont présentées en annexe du rapport publié par la Cour.

⁂

Le présent rapport d'observations définitives est issu d'une enquête conduite sur le fondement de l'article L. 111-3 du code des juridictions financières. Il est rendu public en vertu des dispositions de l'article L. 143-6 du même code.

La première chambre a inscrit à son programme de travail pour 2024 une enquête relative aux enjeux de souveraineté des systèmes d'information de l'État. Notifiée le 7 novembre 2024, l'enquête s'est déroulée de décembre 2024 à avril 2025. L'instruction a

[1] La Cour comprend aussi une chambre contentieuse, dont les arrêts sont rendus publics.

principalement été conduite sur le fondement d'une recherche documentaire approfondie et d'entretiens, suivis de l'envoi de questionnaires, qui ont concerné :

- au sein des services du Premier ministre : l'Agence nationale de la sécurité des systèmes d'information, le secrétariat général des affaires européennes ;

- au ministère de l'action publique, de la fonction publique et de la simplification : la direction interministérielle du numérique ;

- au ministère de l'économie, des finances et de la souveraineté industrielle et numériques : l'Agence pour l'informatique financière de l'État, la direction des achats de l'État, la direction générale des entreprises, la direction générale des finances publiques ;

- au ministère de l'éducation nationale : le secrétariat général, la direction du numérique pour l'éducation, la direction générale de l'enseignement scolaire, le service de modernisation des systèmes d'information des ressources humaines ;

- au ministère du travail, de la santé, des solidarités et des familles : la délégation au numérique en santé ; la direction de la recherche, des études, de l'évaluation et des statistiques.

L'équipe de contrôle s'est, par ailleurs, entretenue avec le vice-président de la Caisse nationale d'assurance maladie, le délégué général du Club informatique des grandes entreprises françaises, le directeur des technologies et de l'innovation de la Commission nationale de l'informatique et des libertés, le président-directeur général de Docaposte, la responsable senior des affaires publiques de Doctolib, la directrice de la plateforme des données de santé, le président-directeur général de l'Ugap.

Enfin, elle a rencontré le député de la 3e circonscription du Cher, le député de la 1re circonscription de la Vendée et la sénatrice de la Seine-Maritime.

⁂

Le projet de rapport d'observations définitives a été préparé, puis délibéré le 11 septembre 2025, par la première chambre, présidée par M. Boudy, président de section, et composée de MM. Tersen, Linquier, Von Lennep, Vareille, Gobelet, conseillers maîtres, ainsi que, en tant que rapporteurs, M. Marcovitch, conseiller maître, M. Huiban, conseiller référendaire, M. Zérah, conseiller référendaire en service extraordinaire, et, en tant que contre-rapporteur, M. Barbé, conseiller maître.

Les rapports publics de la Cour des comptes sont accessibles en ligne sur le site internet de la Cour et des chambres régionales et territoriales des comptes : www.ccomptes.fr.

SYNTHÈSE

La souveraineté numérique est une préoccupation qui a émergé depuis les années 2010. Elle implique une maîtrise par un État des technologies numériques et du droit qui leur est applicable, pour conserver une capacité autonome d'appréciation, de décision et d'action dans le cyberespace. Elle suppose ainsi de ne pas se faire dicter des choix technologiques structurants par un tiers et que soient protégées les données d'une sensibilité particulière des systèmes d'information de l'État. Il s'agit des données qui relèvent de secrets protégés par la loi[2] ou qui sont nécessaires à l'accomplissement des missions essentielles de État et dont la violation est susceptible d'engendrer une atteinte à l'ordre public, à la sécurité publique, à la santé et à la vie des personnes, ou à la protection de la propriété intellectuelle.

L'ambition affichée par la France en matière de souveraineté numérique peine à être satisfaite du fait notamment de la position prééminente des entreprises américaines et de la législation qui leur est applicable, mais aussi d'un environnement européen qui encadre la latitude dont la France dispose en la matière.

Dans ce contexte, l'autonomie technologique est un objectif difficile à assurer dans le champ des matériels et composants. En revanche l'identité numérique et les applications sont des domaines où la maîtrise de la souveraineté est atteignable. Par ailleurs, un enjeu majeur pour les systèmes d'information de l'État est celui de la maîtrise des données les plus sensibles de l'administration, des citoyens et des entreprises, notamment avec le développement de l'informatique en nuage (*cloud*). Même si le coût de la souveraineté numérique est resté jusqu'ici modéré pour l'État, une tension se fait jour entre les enjeux de souveraineté et de performance des administrations.

La souveraineté des systèmes d'information civils de l'État sous la pression des cyberattaques et des lois extraterritoriales américaines

Garantir la sécurité de ses systèmes d'information est l'élément de base de l'exercice de la souveraineté numérique. L'actualité a montré que certains systèmes d'information civils (hors domaines de la défense et du renseignement) sont particulièrement exposés. Les attaques informatiques sont de plus en plus nombreuses et peuvent paralyser des administrations publiques, sans compter la perte ou le vol de données confidentielles. Ces intrusions émanent le plus souvent d'entités criminelles, mais peuvent également provenir d'États.

Au-delà, certains pays ont légalement la possibilité d'accéder à des informations confidentielles détenues par un autre pays. C'est le cas notamment des États-Unis qui ont adopté plusieurs décrets ou lois à portée extraterritoriale, dont le décret présidentiel (*Executive Order 12333*) de 1981 ; l'article 702 du *Foreign Intelligence Surveillance Act*, adopté en 2008 ; le *Cloud Act* de 2018 qui autorisent la collecte de données sur des personnes ou des entités, même si ces données sont stockées en dehors des États-Unis.

Les opérateurs américains du numérique, présents sur tous les continents, sont soumis à ces lois. Si certains rendent compte approximativement du nombre de demandes qu'ils ont reçues à ce titre de la part des autorités américaines, ces procédures restent marquées par une

[2] Au sens du code des relations entre le public et l'administration.

grande opacité. La dépendance des administrations publiques à ces entreprises peut être une entrave à l'objectif de souveraineté numérique qu'il convient de dépasser par une maîtrise des conditions d'exploitation et de stockage des données les plus sensibles.

La vigilance de l'État pour protéger ses données les plus sensibles dans toutes les composantes de la chaîne de production numérique

Pour atteindre la souveraineté numérique, il est nécessaire de contrôler la chaîne de production des systèmes d'information. Cet enjeu comporte trois volets : la maîtrise des matériels, celle des logiciels, et désormais le sujet majeur de la maîtrise des données sensibles.

Concernant les matériels, très peu d'industries sont présentes en Europe. La production des semi-conducteurs se fait principalement aux États-Unis et en Asie. De même, les équipements réseau, les ordinateurs et les smartphones, fabriqués à l'aide de ces composants électroniques, proviennent des États-Unis et d'Asie. L'État veille néanmoins à ce que les matériels qu'il acquiert soient pleinement fiables et sans risques sécuritaires. L'Agence nationale de sécurité des systèmes d'information (Anssi), créée en 2009, s'y emploie et la mutualisation des achats via des marchés interministériels facilite ce contrôle.

La résilience des communications gouvernementales est assurée depuis 2015 par le réseau interministériel de l'État (RIE) qui garantit un bon niveau de fonctionnement, même en cas de défaillances majeures d'Internet. Conformément aux recommandations passées de la Cour, la Direction interministérielle du numérique (Dinum) consolide encore ce réseau en préparant un plan de continuité et de reprise d'activité.

En ce qui concerne les logiciels, la plupart des applications métier des administrations sont hébergées dans des centres informatiques ministériels ou interministériels. L'État en maîtrise ainsi l'exploitation et garantit la sécurité des données hébergées.

En revanche, se pose la question de la dépendance de l'État vis-à-vis des éditeurs de logiciels. Certaines administrations se prémunissent de ce risque en développant ou en faisant développer des applications propres. Si elles gardent ainsi la main sur le logiciel, cette démarche n'est pas sans défaut, notamment pour respecter les budgets alloués et les délais de réalisation. Beaucoup d'exemples de dérapages financiers et opérationnels ont été constatés par la Cour au fil de ses précédents contrôles.

D'autres administrations préfèrent recourir à des logiciels du marché, pour offrir à leurs agents des fonctionnalités déjà éprouvées et assurer une plus grande rapidité de déploiement. Si cette démarche peut apporter une plus grande performance à court terme, elle crée une dépendance de fait vis-à-vis de l'éditeur qui risque de confronter l'administration à des revirements de politiques techniques et commerciales, notamment avec des éditeurs qui basculent vers de nouveaux modèles, fondés sur le *cloud*, et augmentent leurs tarifs. Même lorsque les marchés incluent formellement des clauses de réversibilité, les changements de logiciels sont généralement des projets longs et coûteux. Tel a été le cas avec l'usage, très répandu, des logiciels de bureautique et de messagerie qui composent la suite Microsoft Office. L'entreprise a annoncé basculer son offre sur le *cloud*, et la Dinum a demandé aux ministères de ne pas y souscrire, pour des raisons de souveraineté des communications électroniques.

Pour autant, deux approches coexistent au sein de l'État : le ministère de l'éducation nationale (MEN) a entrepris de remplacer la suite Office par un ensemble d'applications sous licence logicielle libre ; la Dinum, de son côté, développe par elle-même une nouvelle suite

bureautique et de messagerie, en coordination avec ses homologues allemand et néerlandais. S'il est regrettable qu'il n'y ait pas convergence d'approche entre le ministère aux effectifs les plus nombreux et la Dinum, ces deux exemples illustrent l'existence d'alternatives, même face à un éditeur en position de force.

Enfin, la Dinum a porté le projet d'identité numérique FranceConnect pour des motifs de souveraineté face à des offres d'authentification émanant de grandes entreprises américaines, comme Facebook et Google. Ce produit est aujourd'hui massivement utilisé, montrant qu'il répond à des besoins de simplicité et de confiance des citoyens. Dans la conduite de ce projet, la Dinum apparaît toutefois dépendante de ses prestataires et n'a pris que tardivement des mesures de sécurisation, aussi bien face aux risques liés aux sous-traitants qu'à ceux, plus globaux, d'usurpation d'identité. Le renforcement de la sécurisation de FranceConnect, via l'outil FranceConnect+, a permis de lutter contre des fraudes parfois massives.

La question de la gestion des données est devenue encore plus prégnante avec le développement du *cloud*, dont le marché est largement dominé par quelques grandes entreprises américaines, dites *hyperscalers*[3], qui ont investi des sommes très élevées dans des infrastructures robustes, sécurisées et performantes. Tout en incitant les administrations à recourir au *cloud*, l'État a édicté des règles visant à protéger les données les plus sensibles vis-à-vis des lois extraterritoriales auxquelles sont soumises ces entreprises.

La priorité donnée au cloud dans un équilibre complexe entre enjeux de souveraineté et respect réglementaire du cadre européen

Le Premier ministre a édicté une doctrine, dite « *Cloud au centre* », pour que les administrations privilégient les infrastructures *cloud* pour leurs nouveaux projets numériques. La première version de la circulaire, diffusée en juillet 2021, indiquait que toute application maniant des données d'une sensibilité particulière, et notamment des données personnelles de citoyens français, devait être hébergée sur une infrastructure souveraine. Une seconde version de mai 2023 a restreint l'obligation de recours à une offre souveraine en ne l'exigeant que lorsque deux critères cumulatifs sont observés : les données doivent relever de secrets protégés par la loi et leur violation doit être susceptible « *d'engendrer une atteinte à l'ordre public, à la sécurité publique, à la santé et à la vie des personnes, ou à la protection de la propriété intellectuelle* ». Ces critères cumulatifs ont été élevés au niveau législatif avec la loi du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (loi SREN) en son article 31.

Le choix de restreindre ainsi les obligations de recours à une infrastructure souveraine s'explique notamment par la nécessité de respecter les règles du marché intérieur européen et le principe du pays d'origine. La France ne peut pas imposer des règles de souveraineté qui excluraient de manière trop large des marchés publics une entreprise installée dans un autre État membre. La Commission européenne n'a, à cet égard, pas émis d'objection à l'issue de la période dite de *statu quo* sur le projet de décret d'application de l'article 31 de la loi SREN présenté par la France.

L'Union européenne (UE) peut imposer des règles uniformes en son sein, comme elle l'a fait sur la protection des données personnelles avec le RGPD. Elle est alors en mesure d'infliger de lourdes sanctions aux entreprises qui ne respectent pas ces règles. Mais elle ne

[3] Entreprises spécialisées dans la fourniture de services d'infrastructure cloud à grande échelle et évolutifs

s'est pas approprié les enjeux de souveraineté de façon aussi exigeante que la France. Ainsi, ses deux premières décisions dites d'adéquation, ayant pour objet d'instaurer un cadre de confiance pour l'échange des données personnelles entre l'UE et les États-Unis (*Safe Harbour* en 2000 et *Privacy Shield* en 2016), ont été annulées par la Cour de justice de l'Union européenne (CJUE) qui a considéré que les États-Unis n'apportaient pas suffisamment de garanties aux citoyens de l'Union. La troisième décision d'adéquation, le *Data Privacy Framework*, est en vigueur depuis juillet 2023.

Enfin, la Commission travaille sur un schéma de certification des fournisseurs de services de *cloud* (EUCS[4]), comportant plusieurs niveaux d'exigence de sécurité selon la sensibilité des données concernées. La France a plaidé pour y introduire un niveau de supérieur de sécurité inspiré de la qualification SecNumCloud de l'Anssi qui garantirait une immunité face aux lois extraterritoriales. Cela reconnaîtrait à l'échelle européenne l'exigence de souveraineté et sécuriserait juridiquement cette approche. La démarche de la France est restée jusqu'à présent isolée au sein de l'UE.

Le coût de la souveraineté : un investissement de l'État jusqu'ici modéré ; un marché de l'hébergement souverain non stabilisé

La Dinum a arrêté des orientations qui intègrent un axe relatif à la souveraineté numérique. Celles-ci ne constituent cependant pas une stratégie de l'État opposable aux ministères. Ces derniers disposent d'ailleurs de budgets informatiques propres et aucun pilotage transversal de leurs investissements numérique n'est organisé.

Pour accompagner le développement du *cloud* au sein de l'État, deux infrastructures développées, d'une part, par le ministère des finances (*cloud* Nubo) et, d'autre part, par le ministère de l'intérieur (*cloud* Pi), ont été ouvertes aux autres administrations. Ces deux *clouds*, qui ont mobilisé des niveaux de financement modérés (55 M€ en neuf ans pour Nubo au regard des dépenses numériques de l'État d'environ 3 Md€ par an), restent peu utilisés, non seulement par les services des ministères qui les ont créés, mais aussi par les autres administrations. La gamme des services offerts demeure limitée (en termes de disponibilité, d'expérience utilisateur ou de capacité à recourir à l'intelligence artificielle) et leur tarification apparaît inadaptée.

Il conviendrait d'engager la convergence de ces deux *clouds* pour qu'ils atteignent une taille critique et les rendre plus attractifs pour accroître significativement leur utilisation par l'ensemble des ministères. Le réseau interministériel de l'État (RIE) a été réalisé grâce à un effort budgétaire raisonnable (10 M€ par an) qui a permis de surcroît des économies d'exploitation. Cet exemple illustre le fait que, en sus de la mutualisation des enveloppes budgétaires ministérielles, de l'ordre de 15 à 20 M€ par an, consacrées aux *clouds* Nubo et Pi, leur convergence pourrait être réalisée à un coût modéré.

Concernant l'offre émanant de prestataires privés, l'Anssi a développé la qualification SecNumCloud qui assure le plus haut niveau de sécurité et une immunité aux lois extraterritoriales. À l'heure actuelle, seulement une dizaine de prestataires offrent des services ayant obtenu cette qualification. Le surcoût d'exploitation d'une infrastructure SecNumCloud par rapport à un hébergement *cloud* traditionnel se situe entre +25 et +40 %, sans compter le

[4] *European Union Cybersecurity Certification Scheme for Cloud Services*.

coût de migration pour des applications déjà existantes. Par ailleurs, à ce jour, les services qualifiés SecNumCloud n'ont pas la profondeur des *hyperscalers*.

Aussi, face à des données financières éparses, la définition d'une stratégie de souveraineté des systèmes d'information de l'État devrait impérativement être complétée par un chiffrage des investissements à réaliser.

Une tension entre les enjeux de souveraineté et de performance : un niveau de performance à mettre en regard des besoins réels et surtout de la préservation de la souveraineté

Les diligences menées par la Cour dressent un panorama de situations très diverses selon les ministères pour la gestion des données sensibles, sans que la Dinum soit en mesure de faire prévaloir une doctrine claire.

Le système d'information des ressources humaines (recrutements, évaluations, formations) du ministère de l'éducation nationale, Virtuo, est opéré en mode *cloud* par une entreprise appartenant à un groupe américain. Si cette application gère des données d'une sensibilité particulière, le ministère estime qu'il n'est pas contraint de recourir à une solution souveraine, car leur éventuelle divulgation n'entrerait pas dans une catégorie prévue dans la loi SREN. La Dinum ne se prononce pas sur cette appréciation. Dans le cadre juridique actuel, de telles données personnelles pourraient être considérées comme ne relevant pas des exigences de souveraineté, mais sans que cela résulte d'une analyse interministérielle partagée.

Les données confidentielles des entreprises relèvent quant à elles des deux critères inscrits dans la loi SREN (données sensibles et divulgation pouvant causer un trouble à l'ordre public ou à la protection de la propriété intellectuelle). Ainsi, le portail public chargé de la généralisation de la facturation électronique, porté par le ministère des finances, est hébergé dans un environnement souverain. En revanche, tel n'est pas encore le cas de la plateforme d'achat public. Le fait que le ministère recoure, pour une partie des prestations, à une entreprise d'un groupe canadien, a inquiété plusieurs parlementaires et montré que la migration vers un environnement souverain devrait être plus fermement programmée.

La plateforme des données de santé (dite *Health Data Hub*), regroupant des données médicales pseudonymisées à des fins de recherche, témoigne aussi des difficultés de faire prévaloir une position unanime. Le choix d'un hébergement par l'entreprise Microsoft a permis de disposer d'un service opérationnel en quelques mois ; en revanche il a suscité la méfiance des fournisseurs de données de santé, ce qui a entravé son bon fonctionnement et son développement. Une plateforme initialement moins performante, mais souveraine, aurait probablement permis un déploiement moins heurté et un usage plus répandu.

Aussi la Cour recommande-t-elle à l'État de réaliser et régulièrement actualiser une cartographie des données sensibles qui nécessiteraient un hébergement souverain.

Enfin, des entreprises privées proposent des offres liées à des missions de service public et manient des données d'une grande sensibilité. Dans le champ de la santé, c'est le cas de Doctolib, par exemple, qui recueille des informations médicales très précises. À cet égard, la certification « *hébergeur des données de santé* » à laquelle ces entreprises sont soumises mériterait d'intégrer des critères de souveraineté qui s'imposeraient à tous les acteurs, y compris privés. Dans le domaine de l'éducation, c'est le cas de Pronote qu'utilisent la plupart des

établissements publics du second degré pour retracer la vie scolaire de leurs élèves. Ces entreprises ne sont aujourd'hui pas couvertes par les exigences de souveraineté, même si Docaposte, éditeur de Pronote et filiale du groupe La Poste, a fait le choix d'un hébergement qualifié SecNumCloud.

Tant que l'Europe ne dispose pas d'opérateurs capables de rivaliser avec les *hyperscalers*, les administrations publiques devraient viser une performance des systèmes d'information plus strictement adaptée à leurs besoins. Le parfait exercice des missions de service public peut être garanti sans nécessairement aligner les spécifications des systèmes d'information sur le plus haut niveau technologique dès lors qu'un degré trop élevé de performance à court terme peut constituer un double écueil : par la mise en cause de la souveraineté sur les données et par une dépendance de l'administration vis-à-vis de la politique commerciale d'un éditeur dominant.

À l'issue de cette enquête, la Cour formule cinq recommandations visant à mieux prendre en compte les enjeux de souveraineté dans les systèmes d'information civils de l'État qui deviennent de plus en plus prégnants dans le contexte du développement rapide de l'intelligence artificielle et la perspective de l'informatique quantique.

RECOMMANDATIONS

Recommandation n° 1. (Direction interministérielle du numérique) : Mettre en place en 2026 avec les ministères un calendrier de déploiement d'outils de bureautique et de communication respectant la souveraineté des données.

Recommandation n° 2. (Direction interministérielle du numérique) : À l'occasion de la révision de la feuille de route de la Dinum, intégrer une stratégie de souveraineté numérique qui définisse, notamment, les modalités de développement et d'exploitation des applications informatiques de l'État, et procéder à son chiffrage.

Recommandation n° 3. (Direction interministérielle du numérique, Direction générale des finances publiques, Secrétariat général du ministère de l'intérieur) : Définir la trajectoire de convergence des *clouds* interministériels pour les rendre plus performants et augmenter significativement leur utilisation mutualisée par l'ensemble des ministères civils.

Recommandation n° 4. (Direction interministérielle du numérique, Agence nationale de la sécurité des systèmes d'information) : Veiller à ce que chaque ministère cartographie en 2026 l'ensemble de ses données sensibles à héberger de manière souveraine.

Recommandation n° 5. (Délégation au numérique en santé) : Assurer la souveraineté de l'hébergement des données de santé en alignant la certification « Hébergeur de données de santé » sur les exigences de la qualification SecNumCloud en matière de protection vis-à-vis du droit extra-européen.

INTRODUCTION

L'enquête de la Cour a porté sur les dimensions des systèmes d'information civils de l'État (c'est-à-dire hors domaines de la défense et du renseignement) qui concentrent les enjeux en matière de souveraineté, à savoir des réalisations ou projets en matière de logiciels et de déploiement informatique dans le nuage, ou cloud computing.

N'entraient pas dans le champ de l'enquête :

- *les politiques de cybersécurité des ministères car, si les enjeux de sécurité informatique sont évoqués, en tant qu'ils constituent un prérequis de la souveraineté numérique, l'enquête n'avait pas pour objet de contrôler les actions et moyens mis en œuvre par les administrations en la matière ;*
- *le soutien à la filière industrielle numérique, même si les interactions possibles avec les enjeux de souveraineté peuvent être évoquées.*

Depuis une quinzaine d'années, le concept de souveraineté numérique a progressivement émergé dans le débat public, jusqu'à prendre place dans l'élaboration de la stratégie numérique de l'État.

Elle s'est traduite en France pour la première fois en 2014 par l'organisation des « Assises de la souveraineté numérique ». L'expression a été ensuite consacrée par la loi du 7 octobre 2016 pour une République numérique – qui envisageait la création d'un « Commissariat à la souveraineté numérique » – puis dans l'intitulé du « ministère de l'économie, des finances et de la souveraineté industrielle et numérique » depuis mai 2022. C'est une des priorités assignées à la Direction interministérielle du numérique.

La capacité à assurer la confidentialité, l'intégrité et la disponibilité des données gérées par l'État face à des intrusions étrangères, attaques, malveillances ou négligences est essentielle pour disposer d'un minimum de souveraineté. Par conséquent, dans le domaine du numérique, la souveraineté de l'État est conditionnée par sa capacité à développer et mettre en œuvre ses propres systèmes d'information, dans les segments régaliens de son action et des domaines où les données traitées – de ses agents, des citoyens comme des entreprises – doivent être pleinement protégées.

À ce titre, deux éléments constitutifs des enjeux de souveraineté des systèmes d'information de l'État semblent prépondérants :

- la maîtrise des technologies et la garantie de ne pas être dépendant d'éditeurs, notamment étrangers, afin de prémunir l'État des risques techniques, opérationnels et financiers qu'il encourt lorsqu'un fournisseur utilise des technologies propriétaires ou spécifiques, rendant difficile toute réversibilité ;
- la maîtrise des données, leur intégrité, leur disponibilité et, pour les données sensibles, leur confidentialité, préoccupations rendues d'autant plus aiguës par le développement actuel de l'intelligence artificielle, fortement consommateur de données.

Cependant, les notions de souveraineté, de cybersécurité, mais aussi de productivité ne sont pas toujours pleinement conciliables. L'objectif de confidentialité des données peut se heurter au caractère extraterritorial de certaines législations étrangères permettant d'accéder

légalement à des données détenues par l'État, notamment pour ce qui concerne des infrastructures dominées par les grands groupes américains du numérique. Or, ces derniers sont souvent décrits comme étant en avance en termes de sécurité et comme proposant des services éprouvés, simples à mettre en place et déployer.

Si le gouvernement a entendu mettre la priorité sur les enjeux de souveraineté, ce choix est donc parfois contradictoire avec les objectifs fixés par ailleurs aux administrations publiques en termes de performance.

⁂

Les travaux antérieurs de la Cour et les enjeux associés à l'enquête ont amené à inclure dans le périmètre du contrôle :

- le ministère chargé de l'économie et des finances, et plus particulièrement la direction générale des finances publiques (DGFiP) notamment pour ce qui concerne le *cloud* interne Nubo ;
- le ministère de l'éducation nationale, aussi bien pour les outils bureautiques et de messagerie que pour ses projets métiers ;
- le ministère de la santé et de l'accès aux soins, pour la plateforme des données de santé.

Le présent rapport fait état du résultat des diligences réalisées par la Cour.

La première partie présente le constat d'une ambition de souveraineté numérique pour l'État qui demeure insatisfaite, en analysant la place de cet enjeu, les difficultés rencontrées au niveau européen et les limites de la gouvernance interne actuelle.

La deuxième partie examine les défis concrets rencontrés pour assurer une réelle autonomie technologique, en abordant la dépendance matérielle et les réseaux, les questions liées à l'identité numérique et les enjeux de souveraineté des applications critiques.

Enfin, la troisième partie aborde la priorité politique accordée à la maîtrise des données, notamment via le *cloud*, et met en lumière les obstacles à sa mise en œuvre effective, confrontée aux usages, aux réalités du marché et à la conciliation avec l'exigence de performance.

1 UNE AMBITION DE SOUVERAINETÉ NUMÉRIQUE ENCORE INSATISFAITE

L'ambition affichée par l'État d'assurer sa souveraineté numérique se heurte à de nombreux obstacles qui freinent sa pleine réalisation. La définition et la prise en compte effective de cet enjeu (1.1), l'inscription de l'action de la France dans un cadre européen complexe (1.2) et les limites de la gouvernance interne de ses systèmes d'information (1.3) expliquent que cet objectif ne soit encore qu'imparfaitement atteint.

1.1 La place prise progressivement par les enjeux de souveraineté dans le numérique de l'État

La définition de la notion de souveraineté numérique et ses implications concrètes pour l'action publique constituent un enjeu fondamental (1.1.1). Cette préoccupation s'est imposée progressivement au cœur des politiques de transformation numérique de l'État (1.1.2). L'importance de l'enjeu est par ailleurs renforcée par le développement de technologies critiques telles que l'informatique en nuage (*cloud*) et l'intelligence artificielle, qui accentuent les dépendances potentielles et la vulnérabilité des données (1.1.3).

1.1.1 La notion de « souveraineté numérique », qui a émergé dans les années 2010, est confrontée à la position des États-Unis et d'autres puissances

Depuis une quinzaine d'années, le concept de « souveraineté numérique » a émergé dans le débat public, et a pris une place croissante dans la politique numérique de l'État. L'expression est utilisée dès les années 2010 mais une vraie prise de conscience a eu lieu en 2013, quand Edward Snowden[5] a révélé au monde l'ampleur de la surveillance de masse opérée par les États-Unis à son profit en dehors de tous les canaux légaux internationaux, dans un espace numérique dominé par les entreprises américaines.

Suite à ces révélations, l'Union européenne (UE) a renforcé ses lois sur la protection des données, avec l'adoption du règlement général sur la protection des données (RGPD) en mai 2018, qui vise à garantir un meilleur contrôle des citoyens sur leurs données personnelles[6].

[5] Analyste de sécurité pour un sous-traitant de la *National Security Agency* (NSA) américaine, il a divulgué des dizaines de milliers de documents confidentiels de l'agence de renseignement, révélant des programmes de surveillance de masse des communications, tant de citoyens américains que de dirigeants étrangers.

[6] La protection des données personnelles était antérieurement encadrée par la directive 95/46/CE. Le RGPD, entré en application le 25 mai 2018, a permis 1/ d'uniformiser cette politique à l'échelle de l'UE 2/ d'élargir son champ d'application à toutes les entreprises qui traitent des données personnelles de citoyens de l'UE, y compris celles situées en dehors de l'Union 3/ de renforcer les exigences envers les hébergeurs en matière de sécurité des données 4/ de renforcer les droits des individus 5/ d'aggraver les sanctions, pouvant atteindre, selon la gravité de l'infraction, jusqu'à 4 % du chiffre d'affaires mondial ou 20 M€.

En France, cela s'est matérialisé par l'organisation en 2014 des « Assises de la souveraineté numérique » à l'initiative du gouvernement et s'est traduit par la loi du 7 octobre 2016 pour une République numérique, puis celle du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique. La souveraineté numérique est désormais une des priorités stratégiques de la direction interministérielle du numérique (Dinum).

Dans son acception traditionnelle, la souveraineté se définit comme l'exclusivité de la compétence de l'État sur le territoire national et son indépendance dans l'ordre international où il n'est limité que par ses propres engagements. Au niveau européen, le numérique fait partie, selon les termes de l'article 4 du traité sur le fonctionnement de l'UE, des compétences dites « partagées » : les États membres ne peuvent agir que si l'UE a décidé de ne pas le faire ou si elle n'a pas encore proposé de législation.

La notion de souveraineté numérique suppose la maîtrise des technologies par un État afin de conserver une capacité autonome d'appréciation, de décision et d'action dans le cyberespace. Cela nécessite de ne pas se faire dicter de choix structurants par un tiers, alors même que les entreprises dominantes dans le domaine du numérique sont américaines. Cette capacité est également menacée par le développement de lois extraterritoriales.

Aux termes du droit international public, un État est susceptible d'établir une compétence extraterritoriale en l'absence d'un texte international l'interdisant explicitement. Pour autant, cette compétence est encadrée par des critères de rattachement : territorial, personnel (nationalité) et matériel (intérêts fondamentaux de l'État comme la sécurité nationale et la protection des intérêts de la communauté internationale). Par ailleurs, la mise en œuvre d'une loi extraterritoriale suppose le respect des principes d'intégrité territoriale et d'indépendance des États, *via* le recours aux accords ou mécanismes officiels d'entraide.

Ces règles se heurtent en pratique à deux difficultés accentuées par le développement du numérique : la démonstration du lien de rattachement au territoire et, surtout, la capacité à rechercher des documents, des informations et autres éléments de preuve en dehors des canaux de la coopération judiciaire internationale ou bilatérale.

Si l'extraterritorialité du droit est ancienne, elle s'est particulièrement développée aux États-Unis depuis la fin des années 1990. De nombreux domaines sont concernés, par exemple les sanctions internationales (lois « Helms-Burton » et « Amato-Kennedy » de 1996), la lutte contre la corruption (le *Foreign Corrupt Pratices Act*, modifié en 1998), contre la fraude fiscale (le *Foreign Account Tax Compliance Act* de 2010), contre le blanchiment d'argent et le financement du terrorisme (le *Patriot Act* de 2001), la sécurité nationale (le *Foreign Intelligence Surveillance Act*, amendé en 2008).

Ces textes s'adossent désormais à la puissance technologique des États-Unis à travers les grandes entreprises que sont Google, Apple, Meta, Amazon et Microsoft. Si ces entreprises privées sont théoriquement soumises au droit interne du pays où s'exercent leurs activités commerciales, le *Clarifying Lawful Overseas Use of Data Act* (Cloud Act) de 2018 permet aux agences fédérales américaines d'exiger, via un mandat ou une citation à comparaître émanant d'un juge, qu'elles fournissent des données stockées sur des serveurs, qu'ils soient situés aux États-Unis ou à l'étranger (cf. *infra*).

Si les débats sur la volonté d'imposer des compétences extraterritoriales dans le monde du numérique portent aujourd'hui essentiellement sur les États-Unis, d'autres puissances ont des velléités similaires, notamment la Chine. Des géants chinois du numérique actifs en France sont régulièrement soupçonnés d'entretenir des liens étroits avec leur gouvernement. Les lois

chinoises de 2017 sur les données personnelles, la cybersécurité et le renseignement suscitent les mêmes inquiétudes que le Cloud Act et le Fisa. La loi chinoise sur le renseignement national pose ainsi dans son article 7 le devoir, pour les citoyens et les entreprises, de coopérer avec les agences de renseignement et de sécurité de l'État. L'article 10 attribue en outre une portée extraterritoriale à cette disposition.

1.1.2 La transformation numérique de l'État et l'intégration progressive des enjeux de souveraineté

Depuis les années 1990, le numérique transforme les administrations et simplifie les démarches des usagers. La question de la souveraineté n'était pas initialement posée, l'enjeu étant avant tout d'améliorer l'efficacité et l'efficience des services publics, tant dans leur fonctionnement interne que vis-à-vis des citoyens.

1.1.2.1 Le numérique perçu initialement comme un levier de simplification des services pour les usagers et d'amélioration de l'efficacité administrative

Le mouvement, initié en 1998 avec le programme d'action gouvernemental pour la société de l'information, s'est poursuivi avec le plan ADministration ÉLEctronique (ADELE) sur la période 2004-2007 visant à faire de l'administration électronique un levier de la modernisation de l'État. En 2008, le plan « France numérique 2012 » a notamment pour but d'accroître l'accessibilité des sites Internet publics, de développer le paiement en ligne, d'améliorer l'interopérabilité entre administrations et d'ouvrir les données publiques (*open data*). Selon un bilan en date de novembre 2011[7], ce plan a permis la dématérialisation de 76 % des procédures les plus attendues par les usagers contre 30 % en 2007[8].

De manière concomitante, la volonté s'est manifestée de renforcer l'autonomie de l'État dans le domaine numérique. Ainsi, en 2001, un rapport[9] sur la modernisation de l'administration électronique remis au Premier ministre soulignait déjà l'intérêt d'un *« recours accru aux logiciels libres par les administrations »*. En 2012, une circulaire[10] du Premier ministre émettait pour la première fois des recommandations sur l'usage des logiciels libres[11] par les services de l'État. Si la circulaire n'évoquait pas explicitement le terme de « souveraineté », cet enjeu apparaissait de manière implicite à travers la référence aux *« avantages d'indépendance vis-à-vis des acteurs externes »*.

[7] Premier ministre, *France numérique 2012-2020, bilan et perspectives*, novembre 2011.

[8] Ce mouvement s'est poursuivi. Encore sur la période 2017-2025, la délégation interministérielle à la transformation publique a porté la dématérialisation de 250 procédures.

[9] Thierry Carcenac, *Pour une administration électronique citoyenne*, rapport au Premier ministre, 2001.

[10] Circulaire n° 5608/SG du 19 septembre 2012 relative aux orientations pour l'usage des logiciels libres dans l'administration.

[11] Un logiciel est dit « libre » lorsqu'il est distribué avec l'intégralité de ses codes sources, ce qui permet à ses utilisateurs de l'exécuter librement, de le modifier et de l'enrichir pour répondre à leurs besoins et d'en redistribuer des copies. Ces logiciels ne sont pas nécessairement gratuits et les droits des auteurs sont préservés.

1.1.2.2 L'émergence des enjeux liés à la cybersécurité et à la résilience des réseaux

Parallèlement au développement du numérique et des réseaux, la question de la maîtrise de ce nouvel environnement a d'abord été appréhendée sous l'angle de la cybersécurité avec la création en 2009 de l'agence nationale de la sécurité des systèmes d'information (Anssi) afin de combler le retard du pays en la matière, souligné par plusieurs rapports parlementaires.

Ce focus sur la cybersécurité et la résilience des réseaux dans un contexte marqué par le développement de cyberattaques a amené les pouvoirs publics à mettre en place le réseau interministériel de l'État (RIE) à compter de 2011, permettant ainsi la continuité de l'action gouvernementale en cas de dysfonctionnement grave d'Internet (cf. 2.1.3).

Cette logique d'approche globale des problématiques numériques de l'État s'est poursuivie en 2011 avec la création de la direction interministérielle des systèmes d'information et de communication de l'État (Disic), remplacée en 2015 par la direction interministérielle du numérique et des systèmes d'information et de communication de l'État (Dinsic), puis, en 2019, par la direction interministérielle du numérique (Dinum).

1.1.2.3 La loi « pour une République numérique » de 2016 marque un tournant

La loi n° 2016-1321 du 7 octobre 2016 pour une République numérique marque un premier tournant dans la concrétisation de la notion de souveraineté numérique au sein de l'État, soit la question de la double maîtrise des technologies et des données qui y transitent.

Par cette loi, l'administration doit ouvrir ses données au public (*open data*) en mettant en ligne dans un standard ouvert ses principaux documents et ses données qui présentent un intérêt économique, social, sanitaire ou environnemental, sous réserve d'anonymisation ou d'occultation des mentions touchant notamment à la vie privée et à des secrets protégés. Elle introduit également la notion de données d'intérêt général. Ces données de nature privée doivent être ouvertes en raison de leur intérêt pour améliorer les politiques publiques : données des délégations de service public (transports, eau, gestion des déchets, etc.), celles relatives aux subventions publiques supérieures à 23 000 € ou de consommation d'énergie.

Cette logique de transparence de l'action publique suppose que l'État renforce sa maîtrise de ses systèmes d'information. En effet, la loi oblige l'État à publier ses codes sources, l'incite à choisir des logiciels libres ou encore à détenir des capacités en développement et en animation de communautés numériques pour encourager l'écosystème du logiciel libre.

Cette politique d'ouverture des données publiques a posé la question des données publiables *« dans le respect des secrets protégés par la loi »*, sans pour autant définir à ce stade la zone des données dites « sensibles » dont l'État doit garder impérativement la maîtrise.

La notion de souveraineté numérique est introduite à l'article 29 avec *« la possibilité de créer un Commissariat à la souveraineté numérique rattaché aux services du Premier ministre, dont les missions concourent à l'exercice, dans le cyberespace, de la souveraineté nationale et des droits et libertés individuels et collectifs que la République protège »*.

Avec ce texte, la transformation numérique de l'État n'est donc plus uniquement orientée vers la simplification des démarches pour les usagers, du fonctionnement des services

au profit des agents et vers les questions de sécurité informatique, mais est de plus en plus axée sur la question de la maîtrise des données, qui deviendra un enjeu majeur de souveraineté.

La politique de la donnée devient une priorité de l'État à travers la circulaire du Premier ministre du 27 avril 2021[12] qui fait suite au rapport du député Éric Bothorel[13]. La Dinum décline ces orientations dans sa feuille de route, dont une des priorités est de *« préserver la souveraineté numérique de l'État »*. Chaque ministère doit désormais disposer d'une feuille de route « numérique et données » et d'un administrateur des données, des algorithmes et codes sources.

1.1.3 Une préoccupation renforcée par le développement du *cloud* et de l'intelligence artificielle

Le *cloud computing*, ou informatique en nuage, désigne la pratique consistant à utiliser des serveurs distants, hébergés dans des centres de données connectés à Internet, pour stocker, gérer et traiter des données, plutôt que d'utiliser un serveur local ou un ordinateur personnel.

1.1.3.1 Le développement du *cloud* accéléré par celui de l'intelligence artificielle

Le développement de l'intelligence artificielle (IA) accentue l'externalisation des ressources informatiques. Son fonctionnement exige en effet une puissance de calcul très élevée pour entraîner des modèles complexes sur des ensembles de données. Le *cloud computing* facilite cette tâche en permettant d'ajuster les ressources selon les besoins (cf. Annexe n° 1).

Par ailleurs, le *cloud computing* permet de mieux garantir la disponibilité, l'intégrité et la confidentialité des données par des protocoles de cybersécurité généralement plus robustes et des mécanismes de continuité et de reprise d'activité qui se veulent plus avancés que dans le cas des solutions d'hébergement traditionnelles internes (« *on premise* »). Outre la mise à disposition dynamique de ressources, le *cloud* offre des outils et plateformes (bibliothèques d'algorithmes, services de *machine learning*[14], modèles, etc.) qui facilitent le développement d'applications dans le domaine de l'intelligence artificielle.

---

[12] *« La politique de la donnée doit constituer une priorité stratégique de l'État dans ses relations avec tous ses partenaires, notamment les collectivités territoriales et les acteurs privés »* et *« L'année 2021 doit poser les fondements d'une politique ambitieuse de la donnée, des algorithmes et des codes sources dans chacun de vos ministères »*.

[13] Éric Bothorel, *Pour une politique publique de la donnée*, rapport au Premier ministre, décembre 2020.

[14] Le *machine learning*, ou apprentissage automatique, est une sous-discipline de l'intelligence artificielle qui permet aux ordinateurs d'apprendre à partir de données sans avoir été explicitement programmés pour effectuer des tâches spécifiques. Ex. : modèles de prédiction des risques et détection de fraude, aide au diagnostic et analyse de données médicales, optimisation des itinéraires et gestion des flux de trafic.

1.1.3.2 Un marché dominé par trois géants américains

Le marché du *cloud* en pleine croissance[15] est dominé par des acteurs américains, dits *hyperscalers*[16]. Amazon Web Services (AWS), Microsoft Azure et Google Cloud représentent ainsi 70 % des parts de marché en Europe. La part des fournisseurs de *cloud* européens, y compris français, a connu une diminution au cours des dernières années : entre 2017 et 2021, elle est passée de 27 % à moins de 16 % alors même que leur chiffre d'affaires a augmenté de 167 % selon le cabinet d'études Sybergy Research Group. Le marché a connu une très forte hausse et était, en 2022, cinq fois plus important qu'en 2017 avec un chiffre d'affaires cumulé de 10,4 Md€. Les *clouds* d'IBM, Oracle ou Salesforce, qui n'ont pas la même envergure que les trois *hyperscalers* précités, ont plus de poids en Europe que des entreprises européennes telles que SAP, T-Systems, Orange, 3DS Outscale.

La difficulté pour les fournisseurs européens est que les entreprises américaines profitent d'un effet d'échelle avec des coûts fixes élevés et des coûts variables faibles qui leur permettent de croître rapidement. Cette barrière à l'entrée complique la concurrence, d'autant plus que, selon le Sybergy Research Group, les fournisseurs américains continueraient d'investir plus de 4 Md€ chaque trimestre dans des programmes d'investissement européens.

La question pour les États de la maîtrise de la confidentialité, de l'intégrité et de la disponibilité de leurs propres données est devenue plus aiguë avec le développement de services distants par les trois opérateurs susmentionnés soumis à l'extraterritorialité du droit américain.

1.1.3.3 Le développement du marché du *cloud* dominé par des acteurs soumis à l'extraterritorialité du droit américain pose la question de la maîtrise des données

La domination d'entreprises américaines sur le marché du *cloud* pose la question du droit qui leur applicable pour leurs opérations hors des États-Unis. L'extraterritorialité du droit américain applicable aux hébergeurs qui ont leur siège outre-Atlantique concerne trois textes majeurs : l'*Executive Order* (EO) 12333, le *Stored Communications Act* de 1986 modifié par le *Clarifying Lawful Overseas Use of Data Act* (Cloud Act) de 2018 et la section 702 du *Foreign Intelligence Surveillance Act* (Fisa).

L'*Executive Order* 12333, signé le 4 décembre 1981 par le président américain, définit les objectifs, rôles et responsabilités des agences de renseignement des États-Unis. Ce décret a été progressivement renforcé au fil des ans par plusieurs amendements, notamment par l'*Executive Order* 13470 en 2008 qui a accentué le rôle du directeur du renseignement national.

Bien qu'il soit principalement axé sur les activités de renseignement dans un objectif de sécurité nationale sans pouvoir officiellement contraindre une entreprise privée, il permet des activités de collecte d'informations de manière unilatérale, en dehors de tout contrôle judiciaire

[15] Selon le cabinet Markess by Exaegis, le marché des solutions et services *cloud* avoisine les 16 Md€ en 2021 (+15,5 % par rapport à 2020) et devrait atteindre 27 Md€ en 2025 (+14 % de croissance annuelle).

[16] L'*hyperscale* est la capacité d'une architecture technique à s'adapter rapidement à des demandes importantes de ressources dans des systèmes à grande échelle.

et sans procédure de recours. Contrairement à la section 702 du Fisa (cf. *infra*), l'EO 12333 autorise la collecte massive et l'utilisation de renseignements étrangers[17].

Adopté en 2018, le Cloud Act permet aux autorités américaines d'accéder aux données stockées à l'étranger par des entreprises américaines en cas d'enquête criminelle, sans avoir à passer par des procédures d'entraide judiciaire internationale. Ces entreprises doivent fournir des données sur demande des autorités judiciaires, peu importe la localisation des données[18].

Le Cloud Act

Le *Clarifying Lawful Overseas Use of Data Act* (Cloud Act) de 2018 dispose que toute société incorporée aux États-Unis (et toute société qu'elle contrôle) doit communiquer aux autorités américaines, disposant d'un mandat ou de l'autorisation d'un juge, les données de communication qu'elle contrôle sans considération du lieu où ces données se trouvent stockées, c'est-à-dire sans considération de la souveraineté juridique des autres pays à raison du lieu de stockage des données. Cette obligation concerne également des filiales américaines d'entreprises étrangères[19].

Il prévoit la possibilité de signer avec des gouvernements étrangers des accords permettant aux autorités respectives de chaque pays de demander aux fournisseurs de services de communication relevant de la juridiction de l'autre la divulgation des données de communication les intéressant, sans avoir à passer par les procédures beaucoup plus longues de l'entraide judiciaire internationale.

En revanche, le Cloud Act ne fait pas mention du possible cryptage des données et n'impose pas aux sociétés qui y sont soumises de fournir la clé de chiffrement, puisque seules les données stockées – « détenues, contrôlées ou possédées » – par le fournisseur de services peuvent faire l'objet d'une demande de communication.

L'objectif affiché est de rapprocher le temps de l'investigation criminelle de celui de la criminalité. Le Cloud Act organise à l'échelle internationale ce que le projet de règlement E-evidence[20] entend organiser à l'échelle européenne : la possibilité pour les autorités de poursuite d'obtenir la divulgation des données de communication les intéressant dans le cadre de leurs investigations en s'adressant directement aux sociétés traitant ou conservant ces données, c'est-à-dire de manière beaucoup plus rapide que dans le cadre classique de la coopération judiciaire internationale.

Voté en 1978 et amendé en 2008, le *Foreign Intelligence Surveillance Act* (Fisa) autorise, quant à lui, la collecte de données sur des personnes ou entités non américaines à l'étranger, à des fins de sécurité nationale et non dans le cadre d'une enquête criminelle comme

[17] Cette collecte et utilisation massives ont toutefois été par la suite limitées par l'*Executive Order* 14086, pris en 2022 dans le cadre de la négociation du *Data Privacy Framework* entre les États-Unis et l'UE (cf. 1.2.1)

[18] Cette législation extraterritoriale a pour origine un contentieux ayant opposé le gouvernement américain à l'entreprise Microsoft en 2013. Dans le cadre d'un trafic de stupéfiants impliquant un ressortissant non américain, le gouvernement avait demandé à l'entreprise l'accès à des données stockées en Irlande. Microsoft avait refusé, estimant que la demande devait passer par les procédures d'entraide judiciaire internationale au nom de la souveraineté irlandaise. La justice a donné raison à Microsoft, ce qui a conduit le législateur américain à voter le Cloud Act afin d'imposer aux entreprises américaines de se conformer aux demandes des autorités, même pour des données stockées à l'étranger.

[19] C'est par exemple le cas de la filiale OVH US de l'hébergeur français OVHcloud, qui dispose de data centers en Virginie et Oregon, mais aussi des opérateurs Orange et Altice, présents outre-Atlantique. Les maisons mères ne seraient *a priori* pas concernées.

[20] Le règlement E-evidence est entré en vigueur le 17 août 2023 et sera applicable à partir du 17 août 2026.

le Cloud Act. Comme pour ce dernier, la fourniture des données peut être exigée même si elles sont stockées à l'étranger, tant que l'hébergeur est soumis aux juridictions américaines. À la différence de l'EO 1233, le Fisa encadre la recherche d'informations ciblées et non la collecte massive de données.

Initialement, le Fisa visait à autoriser la surveillance pour obtenir des informations de renseignement étranger. Ce texte visait des puissances étrangères et des acteurs étatiques. Il ne s'agissait pas de collecter des informations de particuliers en dehors d'agents étrangers de services de renseignement. L'amendement de 2008 introduit un article 702 qui donne l'autorisation au gouvernement américain de surveiller les communications électroniques de ressortissants étrangers hors du territoire américain, avec l'assistance imposée des fournisseurs de services de communication électronique qui relèvent des juridictions américaines.

L'article 702 du Fisa

Le procureur général et le directeur du renseignement national des États-Unis peuvent autoriser conjointement, pour une période pouvant aller jusqu'à un an, le ciblage de personnes soupçonnées de se trouver en dehors de la zone de compétence de l'État. Les limites sont les suivantes :

- ne peut viser une personne dont on sait qu'elle se trouve aux États-Unis ;
- ne peut viser une personne dont on peut penser qu'elle se trouve hors des États-Unis si l'objectif est de viser une personne, dont on peut penser qu'elle se trouve aux États-Unis ;
- ne peut viser intentionnellement une personne américaine dont on peut raisonnablement penser qu'elle se trouve hors des États-Unis ;
- ne peut acquérir aucune communication dont on sait que l'expéditeur et tous les destinataires prévus se trouvent aux États-Unis ;
- doit être menée conformément au quatrième amendement de la Constitution des États-Unis[21].

Le procureur général et le directeur du renseignement national établissent chaque année des « certifications » autorisant des programmes de surveillance et les soumettent à la Cour de surveillance du renseignement étranger pour approbation. Ces certifications 1) identifient les catégories d'informations de renseignement étranger à recueillir ; 2) contiennent les procédures de ciblage approuvées par le procureur général, visant à garantir que l'acquisition est limitée aux personnes non américaines à l'étranger ; attestent 3) que les procédures de ciblage sont conformes au 4e amendement ; 4) qu'un objectif important du programme est d'obtenir des informations de renseignement étranger ; que le programme 5) utilise un fournisseur de services de communications électroniques américain ; 6) respecte les limitations énoncées par la loi.

L'article 702 n'exige pas que la cible de la surveillance soit un terroriste, ou un agent présumé d'une puissance étrangère mais que les cibles soient des personnes non américaines situées à l'étranger et qu'un « objectif important » de la surveillance soit d'obtenir des « renseignements étrangers » (l'objectif principal de la surveillance peut être entièrement différent).

Dans son bilan annuel 2023, la Cour de surveillance du renseignement étranger (*Foreign Intelligence Surveillance Court* ou FISC) a déclaré avoir reçu 362 demandes : 270 ont été

[21] Le 4e amendement protège les citoyens contre les perquisitions et saisies abusives par les autorités, exigeant un mandat basé sur une cause probable.

accordées, 78 modifiées, 13 partiellement rejetées et une demande a été rejetée en totalité. Elle souligne une baisse des demandes, puisque leur nombre s'établissait à 1 651 en 2018. Le taux de rejet est très faible, oscillant entre 0,28 % (2023) et 2,25 % en 2020.

1.1.3.4 Une difficile appréciation du risque

L'extraterritorialité du droit fait peser un risque sur les données gérées par l'État, notamment les données dites « sensibles » ou les données personnelles des citoyens. Cependant, l'appréciation du risque est difficile. Les actions des services américains au titre de l'*Executive Order* 12333 et de la section 702 du Fisa, motivées par des considérations de sécurité nationale, restent très opaques car hors des canaux judiciaires. Les seuls chiffres disponibles, ceux de la FISC au titre du Fisa, montrent un nombre de rejets très faible des demandes émises par les agences fédérales de renseignement.

Quant aux informations adressées au titre du Cloud Act, il est également difficile d'en connaître l'ampleur même si elles sont transmises sous couvert d'un juge. Les dernières publications en la matière (2024) de quatre grandes entreprises américaines, en l'occurrence Microsoft, Google, AWS et Salesforce, restent vagues.

Au regard des lois extraterritoriales précitées, Microsoft précise qu'elle a contesté avec succès des demandes devant les tribunaux et qu'elle continuera à le faire lorsqu'elle estimera qu'il existe des motifs raisonnables de contestation. AWS indique qu'elle ne divulgue pas d'informations sur ses clients en réponse aux demandes gouvernementales, sauf si elle y est tenue de s'y conformer par une requête juridiquement valable et contraignante. AWS dit s'opposer systématiquement aux demandes excessives ou inappropriées.

Si deux opérateurs - Salesforce et AWS - publient des chiffres sur les requêtes judiciaires provenant de différentes juridictions, américaines ou non, tous communiquent sur les demandes liées à la sécurité nationale des États-Unis, au titre du Fisa ou des « lettres de sécurité nationale »[22]. À cet égard, les opérateurs ne publient, conformément à la réglementation américaine, que des informations parcellaires, en forme de fourchettes allant de [0 à 249] demandes par an (Salesforce) à [500 à 999] par semestre (Google). On constate pour Google une très forte augmentation des comptes touchés, allant de moins de 5 000 avant 2010 à près de 120 000 au second semestre 2023. Le rapport de Microsoft sur les demandes reçues au titre du Fisa témoigne également d'une augmentation du nombre de comptes concernés, passant de moins de 12 000 en 2011 à près de 25 000 en 2023. Ces chiffres apparaissent en contradiction avec les chiffres officiels précités de la FISC, en baisse.

Enfin, dans les deux rapports mentionnant des demandes de données au titre de la coopération judiciaire internationale, les demandes américaines représentent 35,5 % des demandes reçues par AWS (586 sur 1 651) et 94,2 % (98 sur 104) pour Salesforce.

Face à cette situation, il est apparu nécessaire de garantir un cadre de confiance dans les échanges entre l'UE et les États-Unis, ce à quoi s'est attelée la Commission européenne sous le contrôle de la Cour de justice. La France, quant à elle, a renforcé sa législation avec la loi du

[22] Les lettres de sécurité nationale (*National Security Letters*) sont des requêtes administratives émises par des agences fédérales américaines, principalement le *Federal Bureau of Investigation* (FBI), permettant d'obtenir, sans supervision judiciaire, des informations nominatives à des fins de surveillance.

21 mai 2024 visant à sécuriser et réguler l'espace numérique (dite loi SREN), mais sa préoccupation face aux enjeux de souveraineté numérique s'avère encore singulière par rapport aux autres pays de l'UE et face à la Commission.

1.2 En Europe, une France jusqu'ici relativement isolée face au rôle majeur de la Commission européenne

L'UE permet d'imposer des règles uniformes aux opérateurs, comme elle l'a fait sur la protection des données personnelles avec le règlement général sur la protection des données (RGPD). Outre la rationalisation des règles de fonctionnement du marché intérieur, elle est alors en mesure d'infliger de lourdes sanctions aux entreprises qui ne respectent pas ces règles et constitue en cela un bouclier efficace sur ces sujets.

Au sein de l'UE, la Commission est un acteur central des politiques liées au numérique, y compris pour des enjeux liés à la souveraineté des données. Elle dispose ainsi de prérogatives pour encadrer l'échange de données numériques avec des pays tiers, à travers des « décisions d'adéquation ». Si plusieurs ont été annulées par la Cour de justice de l'Union européenne (CJUE), elles ont constitué un cadre légal qui ne privilégiait pas les enjeux de souveraineté (1.2.1). La Commission intervient également pour vérifier que les textes nationaux n'entravent pas le bon fonctionnement du marché intérieur (1.2.2). Ces échanges et arbitrages prennent place en parallèle des travaux sur le schéma de certification européen des services *cloud*, pour lequel la position de la France en matière de souveraineté n'est pas pleinement entendue (1.2.3).

1.2.1 Les décisions d'adéquation européennes : un cadre légal de transmission des données personnelles vers les États-Unis sans prise en compte des questions de souveraineté

La directive 95/46 du 24 octobre 1995 relative à la protection des données personnelles a posé un cadre protecteur pour les citoyens européens vis-à-vis des traitements des données qui les concernent. Face à des législations ou des pratiques de pays extra-européens qui seraient moins exigeantes, cette directive dispose en son article 25 que « *le transfert vers un pays tiers de données à caractère personnel […] ne peut avoir lieu que si […] le pays tiers en question assure un niveau de protection adéquat* ». Lorsque la Commission constate qu'un pays tiers n'assure pas un tel niveau de protection, les États membres doivent alors prendre les mesures nécessaires pour empêcher tout transfert de données vers le pays en cause.

En revanche, lorsque la Commission constate qu'un pays tiers assure un niveau adéquat de protection de la vie privée et des libertés et droits fondamentaux des personnes, en raison de sa législation ou d'engagements souscrits à l'issue de négociations avec la Commission, les États membres doivent alors prendre les mesures nécessaires pour se conformer à la « décision d'adéquation » prise par la Commission.

C'est ainsi que, le 26 juillet 2000, la Commission a adopté la décision d'adéquation 2000/520/CE dite du *Safe Harbour*, permettant les transferts de données à caractère personnel de l'UE vers les États-Unis. Cette décision autorisait notamment les entreprises européennes à transférer des données, sans avoir à évaluer par elles-mêmes le système américain de protection,

vers des entreprises américaines qui déclaraient respecter la législation de l'UE. Néanmoins, quinze ans plus tard et après les révélations faites par Edward Snowden, cette décision d'adéquation a été invalidée par la CJUE par l'arrêt du 6 octobre 2015, Maximillian Schrems c/ Data Protection Commissioner (C-362/14). La Cour de justice a estimé que les recours possibles pour les citoyens européens étaient trop faibles face aux risques de surveillance de masse alors que les autorités américaines pouvaient accéder aux données à caractère personnel transférées à partir des États membres.

À la suite de cette annulation, la Commission a entamé de nouvelles négociations avec les États-Unis, qui ont abouti à une nouvelle décision d'adéquation, dite du *Privacy shield* (décision 2016/1250 du 12 juillet 2016). Cette décision apportait des garanties supplémentaires en instaurant des voies de recours pour les citoyens européens souhaitant intenter une action aux États-Unis en cas de violation du droit de la protection des données personnelles. Par ailleurs, le gouvernement américain s'engageait à ce que l'accès par un tiers aux données personnelles des citoyens de l'UE soit limité aux raisons de sécurité nationale avec la possibilité de saisir un médiateur pour enquêter sur les violations et déterminer si une entreprise agit illégalement. Cette deuxième décision d'adéquation a, elle aussi, été invalidée par la CJUE par un arrêt du 16 juillet 2020 (C-311/18, Data Protection Commissioner / Maximillian Schrems et Facebook Ireland). La Cour de justice relevait que le *Privacy Shield* consacrait la primauté des exigences de sécurité nationale à l'intérêt public et au respect de la législation américaine, rendant ainsi possibles des ingérences dans les droits fondamentaux des personnes dont les données sont transférées vers les États-Unis. Elle estimait que les limitations posées à la protection des données personnelles n'étaient pas encadrées avec des exigences de proportionnalité équivalentes à celles requises au sein de l'UE.

Des négociations ont donc repris entre la Commission européenne et le gouvernement américain, aboutissant à la signature de l'*Executive Order* n° 14086, le 7 octobre 2022, qui renforce la protection des données personnelles traitées par les services de renseignement américains en consacrant les principes de nécessité et de proportionnalité dans le cadre de l'accès des autorités américaines aux données. Ce décret présidentiel introduit un nouveau mécanisme de recours indépendant et impartial auprès d'une Cour de contrôle de la protection des données. À la suite de ce décret, la Commission a adopté une troisième décision d'adéquation, dite *Data Privacy Framework*, le 10 juillet 2023.

Les organismes situés aux États-Unis qui s'engagent à respecter les principes énoncés dans la décision d'adéquation et qui sont référencés par le ministère du commerce américain peuvent ainsi être destinataires de données personnelles, sans qu'il soit besoin d'assortir ces transferts de garanties ou conditions supplémentaires.

Dans son avis, le comité européen de la protection des données avait souligné les progrès réalisés entre le *Privacy Shield* et la nouvelle décision d'adéquation mais avait émis quelques alertes. Il invitait la Commission à suivre de près le fonctionnement pratique de ce mécanisme. Le 9 octobre 2024, un peu plus d'un an après son adoption, la Commission a transmis au Parlement européen un rapport sur le fonctionnement du *Data Privacy Framework*. Elle y estime « *que les autorités américaines ont mis en place les structures et procédures nécessaires pour garantir le bon fonctionnement du cadre de protection des données* », mais reconnaît que cette analyse est nécessairement limitée après une année seulement de mise en œuvre de la décision.

Un premier recours[23] contre le *Data Privacy Framework* a été rejeté en septembre 2025 par la CJUE. La pérennité de la décision suppose que l'administration américaine maintienne les orientations et les moyens de l'agence fédérale indépendante qui garantit le respect de la vie privée et des libertés civiles, le *Privacy and Civil Liberties Oversight Board* et de la cour chargée de la protection des données, le *Data Protection Review Court*.

Tant qu'elle est en vigueur, cette décision d'adéquation crée un cadre pour l'échange de données personnelles entre l'UE et les États-Unis, et facilite le travail des entreprises européennes. Elle ne constitue toutefois pas un rempart sur les enjeux de souveraineté et l'application des lois extraterritoriales, comme cela existe en France pour la sphère publique depuis la doctrine « Cloud au centre » (cf. 3.1.1.) et la loi SREN.

1.2.2 Le décret d'application de la loi SREN, prudente sur les enjeux de souveraineté, n'a pas été bloqué par la Commission européenne

Les enjeux de souveraineté, portés par plusieurs parlementaires, ont amené le Sénat puis l'Assemblée nationale à les introduire dans la loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (dite loi SREN).

L'article 31 de la loi SREN (cf. Annexe n° 2) élève au niveau législatif certaines règles édictées dans la circulaire dite « Cloud au centre » de mai 2023 (cf. 3.1.1). Il encadre les conditions dans lesquelles l'État peut recourir à un service *cloud* fourni par un prestataire privé. Il dispose que des critères de sécurité garantissant notamment la protection des données *« contre tout accès par des autorités publiques d'États tiers non autorisé par le droit de l'Union européenne ou d'un État membre* » doivent être mis en œuvre si le système ou l'application informatique « *traite de données d'une sensibilité particulière* » et – cumulativement – « *si leur violation est susceptible d'engendrer une atteinte à l'ordre public, à la sécurité publique, à la santé ou à la vie des personnes ou à la protection de la propriété intellectuelle* ».

Sont qualifiées de données d'une sensibilité particulière « *les données qui relèvent de secrets protégés par la loi, notamment au titre des articles L. 311-5 et L. 311-6 du code des relations entre le public et l'administration* »[24] et « *les données nécessaires à l'accomplissement des missions essentielles de l'État, notamment la sauvegarde de la sécurité nationale, le maintien de l'ordre public et la protection de la santé et de la vie des personnes* ».

La loi dispose que, dans un délai de six mois à compter de sa promulgation, un décret en Conseil d'État précise les modalités *« notamment les critères de sécurité et de protection, y compris en termes de détention du capital »* dont doit témoigner le prestataire privé fournissant un service *cloud* lorsque l'application qu'il héberge pour les administrations de l'État traite de données sensibles.

[23] Affaire T553-23 Philippe Latombe contre Commission européenne.

[24] Sont notamment considérées comme des données d'une sensibilité particulière, aux termes du L. 311-6, les documents « *dont la communication porterait atteinte à la protection de la vie privée, au secret médical et au secret des affaires, lequel comprend le secret des procédés, des informations économiques et financières et des stratégies commerciales ou industrielles* », « *portant une appréciation ou un jugement de valeur sur une personne physique, nommément désignée ou facilement identifiable* », « *faisant apparaître le comportement d'une personne, dès lors que la divulgation de ce comportement pourrait lui porter préjudice* ».

Cette échéance de six mois fixait la date butoir à fin novembre 2024 pour la publication du décret. Ce n'est toutefois que fin janvier 2025 qu'un projet de décret a été transmis par la France à la Commission européenne, étape préalable à sa publication. Cette procédure d'information vise à empêcher la création d'obstacles au sein du marché intérieur avant qu'ils ne se concrétisent. La période dite de *statu quo* - permettant à la Commission et aux autres États membres d'examiner le texte notifié et de répondre de façon appropriée - durait jusqu'au 28 avril 2025 et aucune opposition n'a été émise dans ce délai.

Ce projet de décret préparé par la Dinum et la direction générale des entreprises (DGE) détaille les critères de sécurité et de protection des données en énonçant les points de vigilance que le prestataire de *cloud* doit mettre en œuvre : sécurité de l'information, gestion du risque, des ressources humaines, sécurité des équipements, sécurité physique, environnementale et logique, gestion des incidents, ainsi que des mesures « *notamment contractuelles, de protection des données traitées ou stockées contre tout accès par des autorités publiques d'États tiers non autorisé par le droit de l'Union européenne ou le droit d'un État membre comprenant en particulier des conditions de détention de capital et des droits de vote dans la société du prestataire et d'établissement du prestataire et de ses éventuels sous-traitants* ».

Le projet de décret renvoie par la suite au référentiel SecNumCloud, élaboré par l'Anssi et qui propose un ensemble de règles de sécurité à suivre par les prestataires de *cloud*, garantissant un haut niveau d'exigence technique, opérationnelle ou juridique (cf. 3.1.2).

Si le périmètre des « données sensibles » selon la loi SREN est plus large que celui du RGPD – qui ne porte que sur les seules données personnelles –, le critère selon lequel leur violation serait « *susceptible d'engendrer une atteinte à l'ordre public, à la sécurité publique, à la santé ou à la vie des personnes ou à la protection de la propriété intellectuelle* » limite les cas où le référentiel SecNumCloud serait imposé aux services de l'État. Une vision trop extensive du recours à ce référentiel risquait de constituer une entrave au marché intérieur et de rendre le référentiel non conforme aux traités.

La conformité à la directive 2000/31 sur le commerce électronique est également un enjeu au cas d'espèce. La CJUE avait rappelé le 9 novembre 2023 (C-376/22, Google Irlande contre le gouvernement autrichien) le principe de libre circulation des services de la société de l'information entre les États membres et la suppression des obstacles que constituent les différents régimes nationaux (principe du contrôle dans l'État membre d'origine). Dans des conditions strictes, un État membre peut néanmoins prendre des mesures dérogatoires afin de garantir l'ordre public, la protection de la santé publique, la sécurité publique ou la protection des consommateurs en les notifiant à la Commission européenne.

Se pose donc la question de la proportionnalité d'un référentiel comme le SecNumCloud, susceptible d'écarter d'appels d'offres publics des entreprises basées dans d'autres États membres. Si la Commission n'a pas bloqué son application en France, cette qualification n'est pas reconnue à ce jour par l'UE, comme en témoignent les discussions en cours autour du schéma de certification EUCS.

1.2.3 La voix de la France difficilement entendue sur la certification des services de *cloud*

Un schéma de certification européen pour les services *cloud* (EUCS, *European Union Cybersecurity Certification Scheme for Cloud Services*) est en cours de discussion entre l'agence européenne pour la cybersécurité et les États membres de l'UE. Une première version a été partagée en décembre 2020. Elle présentait une grille de trois niveaux de certifications (de « *basic* » à « *high* »), avec des niveaux de sécurité adaptés aux usages, de la donnée la moins sensible à la plus sensible. Elle n'intégrait toutefois pas de critères liés à la souveraineté des données. En 2023, a été ajouté dans une version de travail un niveau « high+ » reprenant les exigences du référentiel SecNumCloud (cf. 3.1.2) sur l'exposition aux lois extraterritoriales. À l'époque, cette préoccupation était partagée par d'autres pays que la France :

- l'association Gaia-X, née d'une initiative franco-allemande pour développer un *cloud* européen, avait adopté un cadre de certification en novembre 2021 incluant un niveau élevé avec des exigences en matière d'immunité contre les législations non européennes ;
- lors d'une rencontre à Rome, le 30 octobre 2023, les ministres de l'économie français, allemand et italien avaient « *appelé à une protection efficace des données sensibles en Europe, y compris, en ce qui concerne les données les plus sensibles, contre les législations extraterritoriales* ».

Mais, depuis, l'Allemagne s'était éloignée de cette position, notamment après l'annonce de la société AWS d'investir 7,8 Md€ dans un *cloud* « souverain » dans le land de Brandenburg. Le critère de souveraineté retenu par AWS porte sur le déploiement d'une infrastructure complète d'hébergement au sein de l'UE, répondant aux mêmes critères de sécurité et de performance qu'aux États-Unis. Ces critères ne sont donc pas aussi exigeants que les prérequis de la qualification SecNumCloud, l'entreprise restant soumise aux lois extraterritoriales américaines.

En mai 2023, plusieurs associations professionnelles américaines, dont la *Computer & Communications Industry Association* et la *Business Software Alliance*, ont adressé une lettre au gouvernement américain, dénonçant le futur niveau « *high+* » de l'EUCS comme une menace pour les intérêts économiques et la sécurité nationale des États-Unis.

Aussi, les échanges qui ont suivi au printemps 2024 ont vu ce niveau « *high+* » supprimé. En juillet 2024, la CNIL a alerté sur les risques d'une certification européenne permettant l'accès des autorités étrangères aux données sensibles. Elle a appelé « *à l'inclusion, à titre optionnel, de critères « d'immunité » aux lois extra-européennes, qui peuvent s'inspirer de ceux de la qualification SecNumCloud déjà en place en France, dans le schéma de certification européen EUCS afin d'assurer la plus haute protection des traitements de données personnelles les plus sensibles pour les acteurs industriels européens* ».

Le Conseil supérieur du numérique et des postes[25] a également publié un avis en septembre 2024 attirant l'attention des pouvoirs publics sur l'importance d'intégrer une qualification garantissant une immunité aux lois extraterritoriales, équivalent au SecNumCloud, « *enjeu d'essentiel d'autonomie technologique pour l'Union européenne* ».

[25] Le Conseil supérieur du numérique et des postes est une commission parlementaire mixte, intégrant des personnalités qualifiées.

En 2024, la position française sur l'EUCS apparaissait isolée au sein de l'UE, avant que, début 2025, les relations transatlantiques soient marquées par des revirements sur les questions commerciales. Les discussions européennes n'ont pas repris depuis, dans le contexte du démarrage d'une renégociation du *Cybersecurity Act*, qui traitera également de cette problématique. Dans cette période, la qualification SecNumCloud n'est ni confirmée comme un standard européen, ni écartée, ce qui continue de faire courir le risque qu'il soit considéré comme entravant le marché intérieur.

1.3 Un enjeu encore insuffisamment pris en compte dans la gouvernance des systèmes d'information de l'État

La gouvernance des systèmes d'information de l'État révèle une prise en compte encore insuffisante de l'enjeu de souveraineté. Cette lacune se manifeste à travers un cadre général principalement orienté vers la cybersécurité (1.3.1), des instances interministérielles davantage focalisées sur les questions opérationnelles (1.3.2) et une stratégie en matière de souveraineté numérique qui s'est affirmée tardivement et de manière encore limitée (1.3.3).

1.3.1 Un cadre général axé sur la cybersécurité

En 2025, le cadre général des systèmes d'information de l'État repose sur trois principaux textes, essentiellement consacrés à la sécurité numérique. Quoique celle-ci constitue un prérequis de la souveraineté numérique, l'objet du présent rapport n'est pas d'en examiner spécifiquement les enjeux (pilotage, actions, moyens consacrés à sa mise en œuvre, etc.).

1.3.1.1 La circulaire de 2014 relative à la politique de sécurité des systèmes d'information de l'État

La lettre du Premier ministre qui accompagnait la diffusion de la circulaire de 2014 relative à la politique de sécurité des systèmes d'information de l'État[26] (PSSIE) indiquait que cette politique visait à répondre à la croissance des vulnérabilités dues à l'ouverture et à l'interconnexion croissante des systèmes d'information, ainsi qu'à la multiplication des menaces telles que l'exfiltration de données confidentielles, les atteintes à la vie privée et le sabotage des systèmes.

Elle établissait une base commune pour la sécurité des systèmes d'information de l'État, tout en laissant aux ministères la possibilité d'adapter les mesures en fonction de leurs besoins spécifiques et de l'équilibre à trouver entre réduction des risques et facilitation des usages.

Toujours en vigueur aujourd'hui, la PSSIE définit dix principes stratégiques qui visent à assurer la continuité des activités régaliennes, prévenir la fuite d'informations sensibles et

[26] Circulaire du Premier ministre du 17 juillet 2014 (5725-SG) portant sur la politique de sécurité des systèmes d'information de l'État.

renforcer la confiance dans les téléprocédures. Elle organise les responsabilités des parties prenantes en prévoyant notamment que les services de l'État adoptent leur propre PSSI et mettent en place une organisation spécifique, désignent les acteurs qui en sont chargés et formalisent leurs responsabilités. Elle sert de cadre aux documents plus opérationnels, tels que les chartes internes, guides pédagogiques, notes de sensibilisation, supports de formation, etc.

La PSSIE décline les principes stratégiques en de nombreux objectifs et détaille un socle minimal de mesures de sécurité à respecter pour les atteindre. Les enjeux de souveraineté, ou même simplement d'autonomie, ne sont pas explicitement abordés par la PSSIE. En particulier, elle n'examine pas la question de l'interopérabilité et de la portabilité des technologies retenues par les ministères.

Entre 2015 et 2023, la PSSIE a été régulièrement renforcée, mais est restée centrée sur la sécurité numérique, sans évoquer explicitement l'enjeu de souveraineté.

1.3.1.2 Le décret de 2019 relatif à la gouvernance du système d'information et de communication de l'État

En 2019, un décret[27] a fixé les modalités de gouvernance du système d'information et de communication de l'État (SICE), *« composé de l'ensemble des infrastructures et services logiciels informatiques permettant de collecter, traiter, transmettre et stocker sous forme numérique les données qui concourent aux missions des services de l'État et des organismes placés sous sa tutelle »*. Sa responsabilité incombe au Premier ministre, qui détermine les orientations générales et les règles de sécurité numérique, et par délégation aux ministres (à l'exception de certains services spécifiques). Les directions des systèmes d'information deviennent des directions ministérielles du numérique (DNUM) et la Dinum est créée.

Le décret est complété[28] une première fois en 2022 afin de préciser la gouvernance et les responsabilités en matière de sécurité numérique. Des dispositions prévoient ainsi la désignation dans les ministères de fonctionnaires de sécurité des systèmes d'information (FSSI), qui rendent compte à l'Anssi des éventuels incidents informatiques, et d'autorités qualifiées en sécurité des systèmes d'information. Elles élèvent au rang réglementaire une homologation de sécurité des infrastructures et logiciels de l'État, préalablement à leur mise en œuvre, qui était jusqu'alors mentionnée au sein de la PSSIE.

En 2023, le décret de 2019 est de nouveau modifié[29] afin de renforcer le rôle de la Dinum dans l'accompagnement des administrations ; la gouvernance et l'exploitation des données publiques ; le suivi des projets numériques des ministères ; la politique interministérielle d'achats dans le domaine du numérique. Sans que la notion de souveraineté soit évoquée, la Dinum se voit néanmoins chargée désormais de veiller à « *la maîtrise, la pérennité et l'indépendance* » du SICE et *« d'animer la concertation nécessaire à la constitution et à l'évolution des règles et référentiels en matière d'interopérabilité et d'accessibilité »*.

[27] Décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'État et à la direction interministérielle du numérique, modifié par le décret n° 2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'État et de ses établissements publics.

[28] Décret n° 2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'État et de ses établissements publics.

[29] Décret n° 2023-304 du 22 avril 2023 modifiant le décret n° 2019-1088 du 25 octobre 2019.

Ces textes achèvent donc de consacrer une distinction claire entre les enjeux de sécurité relevant de l'Anssi et les enjeux de performance du SICE, relevant de la Dinum.

1.3.1.3 L'instruction de 2022 sur l'organisation de la sécurité numérique

Fin 2022, une instruction[30] vient décrire plus précisément les rôles et responsabilités associés à la sécurité numérique de l'État. Trois instances interministérielles sont ainsi chargées de définir et de suivre la mise en œuvre de la stratégie de sécurité numérique :

- le comité interministériel du numérique (CIN) est une instance de niveau politique présidée par le Premier ministre ; elle s'est réunie à cinq reprises, soit sous la forme d'une réunion de ministres présidée par le Premier ministre, soit sous la forme de réunions interministérielles réunissant les directeurs de cabinet, sous la présidence du directeur de cabinet du Premier ministre ;
- le comité stratégique interministériel de la sécurité numérique (Cosinus) réunit les hauts fonctionnaires de défense et de sécurité des ministères, la directrice interministérielle du numérique et le directeur général de l'Anssi ; il définit notamment *« les orientations stratégiques en matière de sécurité numérique et la feuille de route associée »* ;
- le comité interministériel de pilotage de la sécurité numérique (Cinus) *« suit la mise en œuvre de la feuille de route […] en proposant une instance de partage et de réflexion sur les difficultés éventuellement rencontrées et l'actualité relative à la sécurité numérique »* ; présidé par le directeur général de l'Anssi, il réunit les fonctionnaires de la sécurité des systèmes d'information des ministères ainsi que des représentants des services de la Présidence de la République, de l'Assemblée nationale, du Sénat et de la Dinum.

Au niveau ministériel, l'instruction établit également des instances de sécurité numérique, notamment l'instance stratégique ministérielle de la sécurité numérique et l'instance ministérielle de pilotage de la sécurité numérique, ainsi qu'une chaîne fonctionnelle de sécurité des systèmes d'information animée par le FSSI. Elle traite par ailleurs la question de la prise en compte de la sécurité numérique dans la gestion ministérielle de crise.

Enfin, l'instruction rappelle que la stratégie numérique de l'État est élaborée et pilotée par la Dinum, et qu'elle *« vise à orienter les actions des administrations […] pour améliorer les services rendus par le SICE »*. Là encore, les enjeux de souveraineté ne sont pas évoqués.

1.3.2 Des instances interministérielles de gouvernance qui traitent essentiellement de questions opérationnelles

Lors de sa mise en place en avril 2019, la stratégie numérique de l'État pour la période 2019 à 2021 dénommée « TECH.GOUV » a été confiée à deux instances interministérielles.

Le comité d'orientation stratégique interministériel du numérique (Cosinum) *« définit la stratégie interministérielle du numérique de l'État et les moyens humains et budgétaires à*

[30] Instruction générale interministérielle n° 1337/SGDSN/ANSSI sur l'organisation de la gouvernance de la sécurité numérique de l'État, approuvée par l'arrêté du 26 octobre 2022.

mobiliser ». Entre 2021 et 2024, ce comité s'est réuni six fois. Le comité interministériel du numérique (Cinum) *« partage l'avancement des missions de TECH.GOUV et des autres chantiers numériques d'intérêt général, et prend les décisions de nature à favoriser leur succès, tout en évoquant les autres projets et problématiques numériques d'intérêt collectif ne relevant pas directement de TECH.GOUV »*. Il prépare les réunions du Cosinum.

L'examen des 38 comptes-rendus des réunions du Cinum intervenues au cours de la période 2021 à 2024 fait apparaître que les échanges se sont concentrés sur les ressources humaines dans le domaine du numérique, en particulier les conditions de recrutement et de rémunération des contractuels, la ré-internalisation des compétences et la formation.

L'enjeu de la dématérialisation des relations avec les usagers a aussi été fréquemment abordé par le Cinum, qu'il s'agisse de la qualité des démarches réalisables en ligne, de leur accessibilité ou de la cohérence de l'expérience utilisateur entre les nombreux sites de l'État. D'autres sujets sont régulièrement inscrits à l'ordre du jour des discussions du Cinum, tels que les questions budgétaires, l'informatique en nuage, le réseau interministériel de l'État et ses évolutions successives, les outils bureautiques, l'administration et l'ouverture des données publiques, le lancement ou le suivi des projets numériques de l'État.

En revanche, les questions de souveraineté opérationnelle n'ont pas été inscrites de manière explicite à l'ordre du jour des réunions. Au fil des comptes-rendus, elle apparaît ponctuellement dans les échanges, souvent pour être abordée de manière assez générale. En septembre 2021, la souveraineté apparaît comme *« un sujet majeur […] qui implique la plus grande vigilance de chacun, dans un contexte d'amélioration de la situation sanitaire »*. En juillet 2022, c'est *« la montée en puissance des sujets de résilience, au-delà de la souveraineté »* qui était relevée.

Les questions de souveraineté ne semblent pas être davantage abordées à l'occasion des réunions du Cosinum, dont l'examen des comptes-rendus laisse apparaître qu'il s'agit en pratique d'une instance de validation des orientations préparées et discutées par le Cinum.

La question de la souveraineté numérique n'est explicitement abordée qu'à une seule occasion, en décembre 2022, pour faire état de *« l'objectif de montée en puissance d'un ensemble de produits collaboratifs pour les agents, s'appuyant prioritairement sur des logiciels libres sans exclure les PME françaises »*.

1.3.3 L'ébauche d'une stratégie de souveraineté numérique

Si depuis le début des années 2000, le numérique était conçu comme un levier majeur de la transformation de l'État, ce n'est qu'en 2019, avec la création de la Dinum que la transformation numérique a pris une place centrale. La Dinum a ainsi hérité des responsabilités de la Dinsic tout en s'en voyant attribuer de nouvelles, notamment la conception et la mise en œuvre de la stratégie numérique de l'État, l'exploitation d'infrastructures partagées (le réseau interministériel, notamment cf. 2.1.3.), la coordination de la stratégie de l'État en matière de données et le conseil au gouvernement sur l'intégration du numérique dans les politiques publiques.

C'est dans ce contexte que le terme de « souveraineté » est finalement apparu de manière explicite autour de la stratégie numérique de l'État, en se distinguant de la notion de « sécurité numérique ».

Ainsi, un rapport sénatorial[31] soulignait en 2019 la nécessité de renforcer la protection des données, de réformer la réglementation et d'agir sur l'innovation et le multilatéralisme pour garantir la souveraineté numérique nationale. Ce rapport percevait la stratégie gouvernementale dans ce domaine comme « dispersée » entre différents impératifs, nécessitant une meilleure coordination. Parallèlement, la Dinsic se dotait d'une nouvelle stratégie triennale dénommée « TECH.GOUV » pour accélérer la transformation numérique du service public. Elle retenait six objectifs prioritaires[32], dont celui consistant à « *accroître l'autonomie et la sécurité numérique de l'État par une meilleure maîtrise technologique* ». Il s'agissait d'assurer la « *maîtrise des systèmes d'information, des architectures et des données afin d'accroître l'autonomie numérique de l'État et sa sécurité, et lui permettre d'opérer des choix éclairés. Renforcer cette maîtrise technologique concourt directement à préserver la souveraineté nationale* ».

En septembre 2021, la stratégie TECH.GOUV était actualisée pour prioriser un nombre plus limité d'objectifs, dont faisait toujours partie celui de souveraineté numérique. Plusieurs chantiers devaient y contribuer, notamment la simplification et la sécurisation de l'accès aux démarches en ligne (FranceConnect, cf. 2.2.1), la protection des données (doctrine « Cloud au centre », politique publique de la donnée[33]) et l'attraction et la fidélisation des talents.

En janvier 2022, cependant, la mise en œuvre de cette stratégie était interrompue. À cet égard, dans un rapport récent [34], la Cour faisait le constat de son échec : *« Cet arrêt soudain montre que cette stratégie n'avait fait l'objet que d'une appropriation très limitée par les agents, les ministères et les administrations partenaires »*.

En mars 2023, la Dinum présentait sa nouvelle feuille de route, qui devait tenir lieu, selon son intitulé même[35], de stratégie numérique pour l'État. Le terme de « souveraineté » y était explicitement repris dans sa quatrième priorité : « *Préserver la souveraineté numérique de l'État en investissant dans des outils numériques mutualisés* ». Six mois plus tard, à l'occasion de la publication de son rapport d'activité[36] pour 2023, la Dinum affichait des réalisations ayant permis selon elle d'accroître la souveraineté de l'État, mais qui avaient principalement trait, en réalité, à sa sécurité numérique (travaux de modernisation du RIE, création en son sein d'une cellule « cyber »). De même, ses engagements pour 2024 se limitaient à la consolidation d'actions déjà lancées (finaliser la modernisation du RIE, accélérer le développement d'outils numériques interministériels, faire monter en puissance la cellule « Cyber »), sans traiter véritablement l'enjeu de souveraineté.

Fin 2024, dans une note interne intitulée « *La maîtrise des systèmes d'information, un enjeu de souveraineté* », la directrice interministérielle du numérique justifiait à nouveau ces orientations. Elle relevait que cet enjeu de maîtrise s'est traduit *« en France par des choix déterminés en matière d'investissements dans les infrastructures (RIE, cloud), dans les*

[31] Sénat, *Rapport fait au nom de la commission d'enquête sur la souveraineté numérique*, octobre 2019.

[32] Simplification, inclusion, attractivité, économies, alliance et maîtrise.

[33] Circulaire n° 6264/SG du 27 avril 2021 relative à la politique publique de la donnée, des algorithmes et des codes sources.

[34] Cour des comptes, *Le pilotage de la transformation numérique de l'État par la direction interministérielle du numérique – Exercices 2019-2023*, juillet 2024.

[35] Direction interministérielle du numérique, *Feuille de route de la Dinum - Une stratégie numérique au service de l'efficacité de l'action publique*, 9 mars 2023.

[36] Direction interministérielle du numérique, *Rapport d'activité 2023 de la Dinum*, septembre 2024.

applications (Tchap, outils collaboratifs) et l'IA », considérant que *« pour maîtriser un système, un domaine, il faut, au moins en partie, l'opérer, y être présent ou l'exercer »*.

Elle y conditionnait la souveraineté d'un actif numérique à sa capacité à satisfaire deux critères : être immunisé aux réglementations extra-européennes ; être conçu de telle manière que tout composant puisse être remplacé par une alternative disponible sur le marché. À cet égard, le recours aux meilleures solutions libres du marché lui apparaissait comme un atout pour la souveraineté et un gage de réussite d'une stratégie de *« réarmement numérique »*, propre à favoriser *« concurrence, transparence, maîtrise et économies »*.

⁂

La notion de souveraineté est donc apparue tardivement dans ce qui a tenu lieu, sous une forme ou sous une autre, de stratégie numérique de l'État et, le plus souvent, prenant la forme de considérations générales, qui ne sont pas suffisamment précises pour guider, au niveau ministériel, la gouvernance et le pilotage des systèmes d'information.

Plus largement, la Cour relevait déjà, dans le rapport précité, que la dénomination même de « feuille de route » montre que *« ce document reste centré sur l'action de la Dinum, sans préciser les rôles ou les cibles pour les autres administrations, laissant présager plus un programme de travail directionnel qu'une stratégie interministérielle »*.

La stratégie numérique de l'État devrait être pensée de manière plus ambitieuse et plus large pour traiter les différents enjeux, en particulier celui de la souveraineté, au niveau interministériel et fournir des orientations claires, stables et partagées aux ministères pour concevoir de manière cohérente leur propre politique en matière de systèmes d'information.

CONCLUSION INTERMÉDIAIRE

L'ambition de l'État en matière de souveraineté numérique, bien que clairement affichée, n'a pas pu être pleinement satisfaite jusqu'à présent. Plusieurs facteurs expliquent pourquoi cette visée stratégique peine à se concrétiser pleinement.

La prise de conscience et la définition même de la souveraineté numérique au sein des ministères ont été progressives, alors que le numérique était d'abord perçu comme un simple moyen de moderniser l'action administrative et d'en accroître l'efficacité.

La notion de souveraineté numérique, apparue dans les années 2010, s'est heurtée d'emblée à la prédominance technologique américaine, rendant complexe sa traduction opérationnelle. L'intégration effective des impératifs de souveraineté dans la transformation numérique de l'État reste aujourd'hui encore un défi.

Ce défi est d'autant plus prégnant avec l'essor rapide de technologies critiques comme le cloud et l'intelligence artificielle. Ces développements accentuent la dépendance de l'État envers des acteurs technologiques étrangers, principalement américains, et soumis à des législations extra-européennes. L'appréciation précise des risques liés à cette dépendance demeure, par ailleurs, délicate.

L'action de la France s'inscrit dans un cadre européen dont les mécanismes encadrent, et parfois contraignent, sa marge de manœuvre, et où elle peine à faire entendre pleinement sa voix. Les discussions relatives à l'application de législations nationales, comme la loi SREN,

ou à la définition de standards européens, telle la certification des services de cloud, illustrent la difficulté de faire émerger une approche européenne alignée sur les ambitions françaises de souveraineté.

Enfin, les limites de la gouvernance interne des SI de l'État contribuent également à cette situation. Le cadre existant, bien que renforcé au fil des ans, reste très axé sur la cybersécurité. Les instances interministérielles dédiées semblent surtout concentrées sur des questions opérationnelles. Une ébauche de stratégie en matière de souveraineté des systèmes d'information de l'État a émergé tardivement et s'est limitée au cloud.

---

2 UNE AUTONOMIE TECHNOLOGIQUE DIFFICILE À ASSURER

La recherche d'une autonomie technologique pour l'État s'avère ardue sur l'ensemble de la chaîne de valeur numérique. Des dépendances persistent sur les infrastructures matérielles et les réseaux (2.1), le défi de la maîtrise de l'identité numérique et la lutte contre les usurpations d'identité sont portés par le dispositif FranceConnect (2.2) mais la souveraineté des applications reste soumise aux évolutions technologiques et aux stratégies des éditeurs (2.3).

2.1 À défaut d'être souverain dans le domaine des matériels et des réseaux, la recherche d'un niveau élevé de confiance dans leur utilisation

La maîtrise de l'infrastructure numérique exige de porter une attention particulière à ses fondations technologiques. À cet égard, la dépendance française est particulièrement marquée au niveau des composants électroniques (2.1.1). Le cadre applicable aux achats publics de matériels informatiques constitue un levier fort pour atténuer les risques liés à cette dépendance (2.1.2). Enfin, le réseau interministériel de l'État constitue une réussite et une infrastructure essentielle, mais sa résilience doit continuer d'être renforcée (2.1.3).

2.1.1 Une dépendance particulièrement marquée vis-à-vis des composants électroniques

Les semi-conducteurs sont indispensables au fonctionnement des technologies numériques. En 2025, ces semi-conducteurs et les composants qui en dépendent (processeurs[37], mémoire, disques durs) sont principalement conçus et produits en dehors de l'UE :

- Intel (États-Unis), AMD (États-Unis), Nvidia (États-Unis) et ARM (Royaume-Uni) conçoivent des architectures de semi-conducteurs et les fabriquent ou les font fabriquer par des entreprises spécialisées en Asie de l'Est, où 80 % des capacités mondiales de production sont concentrées, telles que Samsung (Corée du Sud) et TSMC (Taïwan) ;
- la mémoire vive dynamique (DRAM) est produite par les entreprises coréennes Samsung et SK Hynix ; Micron (États-Unis) détient également une part de marché importante ;
- quelques fabricants se partagent le marché des disques durs, comme les américains Seagate et Western Digital (avec des usines en Chine et en Thaïlande) et Toshiba (Japon).

Certaines entreprises européennes fabriquent des semi-conducteurs ou fournissent des équipements à cette fin aux leaders du marché. Mais, même si elles peuvent exceller sur des segments de marché, elles ne rivalisent pas avec les entreprises américaines ou asiatiques sur le

[37] Notamment microprocesseurs (CPU), processeurs graphiques (GPU), unités de traitement de tenseur (TPU) qui fournissent les capacités de calcul les plus importantes.

marché mondial. Il s'agit notamment de STMicroelectronics (France et Italie), ASML (Pays-Bas), NXP Semiconductors (Pays-Bas) et Infineon Technologies (Allemagne).

Un même constat de dépendance aux industriels américains et asiatiques concerne les équipements réseau, les ordinateurs portables et de bureau, et les smartphones :

- les principaux équipementiers réseau sont Cisco et Juniper (États-Unis) et Huawei (Chine) ;
- les six premiers fabricants d'ordinateurs portables et de bureau se partagent plus de 80 % du marché mondial : Lenovo (Chine), HP (États-Unis), Dell Technologies (États-Unis), Apple (États-Unis), ASUS (Taïwan) et Acer (Taïwan) ;
- près de 70 % des smartphones expédiés dans le monde sont conçus et produits par cinq entreprises : Apple (États-Unis), Samsung (Corée du Sud), Xiaomi (Chine), Transsion (Chine) et Vivo (Chine).

En 2021, la pénurie mondiale de composants électroniques entraînée par la pandémie de Covid-19 a souligné la dépendance des entreprises européennes vis-à-vis de l'Asie. La ministre déléguée chargée de l'industrie avait indiqué que *« l'État a pu échanger avec les autorités taïwanaises, dont est originaire le leader mondial de la fonderie de semi-conducteur et nœud central de cette pénurie, afin d'insister sur la nécessité de servir équitablement les différents secteurs et zones géographiques semi-conducteurs »* [38].

Les pénuries de semi-conducteurs ont conduit l'UE à adopter en 2023 le règlement « *Chips Act* », doté d'un budget de 43 Md€ qui combine des fonds européens, des États membres et du secteur privé et s'ajoute à d'autres instruments de soutien (projets importants d'intérêt européen commun « Microélectronique » et « Microélectronique et connectivité », programme « Horizon Europe »). Faisant le constat d'une *« extrême dépendance, à l'échelle mondiale, de la chaîne de valeur des semi-conducteurs à l'égard d'un nombre très limité d'acteurs dans un contexte géopolitique complexe »*[39], la Commission européenne avait pour ambition de doubler d'ici 2030 la part de marché européenne dans la production mondiale de semi-conducteurs (de 10 % à 20 %) afin de *« renforcer l'avance technologique de l'Europe »*. Cet objectif, qui avait été fixé en mars 2021, apparaît aujourd'hui difficilement atteignable.

Les investissements de la France dans le secteur des semi-conducteurs s'inscrivent dans la logique du « *Chips Act* » et visent à renforcer les capacités nationales en complément des efforts européens. Outre le plan « Nano 2022 » qui soutient à hauteur de 1,1 Md€ des projets de recherche et de développement de composants électroniques innovants, le plan France 2030 doit permettre *« de doubler la production française de composants électroniques, dans un contexte de croissance rapide de la demande de semi-conducteurs dont l'importance stratégique s'accroît à mesure que les rivalités internationales s'accentuent »*[40]. Une enveloppe de 5,2 Md€ est réservée au financement de mesures spécifiques, notamment l'aide à la création ou à l'extension de grandes usines de fabrication (« *Mega Fabs* ») sur le territoire national, en profitant de l'assouplissement des règles d'aides d'État permis par le « *Chips Act* ».

L'essor de l'intelligence artificielle générative a créé une demande très forte en processeurs graphiques (GPU) performants pour les centres de données. Cette révolution

[38] Réponse du 20 mai 2021 à la question de M. Pascal Allizard, sénateur du Calvados, au sujet de la pénurie des semi-conducteurs dans l'industrie.

[39] Site de la Commission européenne, *Règlement européen sur les semi-conducteurs*, septembre 2023.

[40] Comité de surveillance des investissements d'avenir, *France 2030 : Lancement maîtrisé d'un plan d'investissement à impacts majeurs*, juin 2023.

technologique représente *« un enjeu politique, de souveraineté et d'indépendance stratégique »*[41] et rend plus nécessaire pour la France et l'Europe de disposer de ces processeurs hautement spécialisés et performants, qu'elles ne sont aujourd'hui pas capables de produire.

Enfin, la capacité de l'État à assurer sa propre souveraineté numérique dépend aussi de sa capacité à sécuriser ses approvisionnements en matériels informatiques essentiels. Lors de la crise sanitaire, les difficultés d'approvisionnement n'ont pas permis de corriger immédiatement le taux insuffisant de dotation des agents en ordinateurs portables pour leur permettre de télétravailler dans des conditions satisfaisantes.

À l'occasion du Cinum d'octobre 2020, les participants relevaient les *« incertitudes d'approvisionnement en ordinateurs portables, avec de fortes tensions sur le marché Odice de l'Ugap »*. En décembre 2020, la décision était annoncée de *« constituer un stock stratégique de 50 000 portables qualitatifs, à horizon février 2021, permettant de pallier ces difficultés »*. Six mois plus tard, le Cosinum de juin 2021 actait la réussite du dispositif. L'équipement en ordinateurs portables des agents susceptibles de télétravailler ayant atteint un taux de 95 %, il n'a pas été nécessaire, par la suite, de renouveler cette mesure de court terme.

2.1.2 Un cadre applicable aux achats de matériels informatiques qui limite les risques

Fin 2024, les valeurs brute et nette des matériels informatiques et de télécommunication (serveurs, ordinateurs fixes et portables, écrans, terminaux mobiles, etc.) inscrits à l'actif du bilan de l'État[42] s'élevaient respectivement à 3,8 Md€ et 0,9 Md€. Environ 0,3 Md€ de matériels ont été mis en service en 2024.

Sauf exception, les matériels informatiques et de télécommunication de l'État sont conçus et fabriqués à l'étranger, le plus souvent en Asie, avant d'y être aussi assemblés ou acheminés à cette fin en Europe (de l'Est, notamment), voire en France. Cette situation rend l'État dépendant de fabricants étrangers, notamment hors de l'UE. Ces approvisionnements sont vulnérables, car exposés aux événements géopolitiques et tensions commerciales sur les marchés mondiaux, mais aussi au risque de cybersécurité.

Toutefois, la mutualisation interministérielle des achats de matériels informatiques permet de prévenir, jusqu'à un certain point, la survenance de ces risques, tout comme les outils juridiques des marchés publics et les mesures de sécurité mises en œuvre par l'Anssi.

2.1.2.1 La mutualisation restreinte des achats de matériels informatiques

Les marchés publics conclus par les services de l'État sont encadrés par le code de la commande publique et régis par les principes fondamentaux de liberté d'accès, d'égalité de

[41] Déclaration du 9 février 2025 du Président de la République à l'occasion du sommet pour l'action sur l'intelligence artificielle.

[42] Ministère de l'économie, des finances et de la souveraineté industrielle et numérique, *Compte général de l'État, annexe au projet de loi relatif aux résultats de la gestion et portant approbation des comptes de 2024*, avril 2025, page 33.

traitement des candidats et de transparence des procédures. Le respect de ces principes permet d'assurer l'efficacité de la commande publique et la bonne utilisation des deniers publics.

L'animation de la fonction achat est confiée à des responsables ministériels des achats, chargés de mettre en œuvre la politique définie par la DAE tout en l'adaptant aux spécificités de leur ministère. La DAE définit les orientations stratégiques en matière d'achats, élabore des outils méthodologiques, et conseille et forme les acheteurs. Elle passe des accords-cadres ou marchés interministériels, et promeut l'ouverture à d'autres ministères de certains marchés ministériels. Dans d'autres cas, elle en délègue la passation aux ministères ou à l'Union des groupements d'achats publics (Ugap).

Tout en veillant à respecter les orientations de la Dinum et de l'Anssi, la DAE vise à mutualiser les achats informatiques pour créer un effet de levier et obtenir des prix plus avantageux, mais aussi améliorer la résilience et la sécurité des approvisionnements. Cela permet d'homogénéiser le parc informatique de l'État, facilitant la maintenance et la sécurité. Ainsi, dans les ministères civils, les matériels sont acquis dans le cadre de marchés ministériels, sous le contrôle de la DAE, ou interministériels (trois quarts environ des acquisitions), sous la forme d'accords-cadres et marchés à bons de commande passés par l'Ugap.

Fin 2024, la DAE a ainsi passé un marché interministériel de serveurs informatiques x86 pour un montant de 63 M€ sur trois ans, attribué à SCC France. L'Ugap a renouvelé le marché interministériel de postes de travail dit « Odice 2 »[43], qui fait intervenir un système d'acquisition dynamique[44] au bénéfice des principaux ministères et établissements publics.

En dépit de ces efforts de centralisation et de coordination, les ministères restent responsables de leurs systèmes d'information et disposent, en raison de la variété de leurs besoins, d'une grande autonomie dans leurs choix techniques.

2.1.2.2 Des marchés publics permettant un certain degré de sélectivité

Les appels d'offres lancés dans le cadre de marchés publics de l'État sont ouverts aux fournisseurs des vingt-deux pays signataires de l'accord de marchés publics de l'Organisation mondiale du commerce (OMC)[45]. Les distributeurs de matériel informatique qui y répondent ont presque toujours une filiale de droit français implantée en France.

L'inclusion dans les marchés de considérations relatives à la nationalité des répondants aux appels d'offres serait contraire aux règles de l'UE et l'OMC. À défaut, les acheteurs disposent d'outils leur permettant de sélectionner les titulaires des marchés sur des critères dont le respect permet d'obtenir un niveau de confiance élevé. Ces outils recouvrent les critères d'attribution (tels que le prix, la qualité ou l'expérience du fournisseur), leur pondération, les conditions d'exécution (les obligations contractuelles d'exécution du marché), enfin les spécifications techniques auxquelles doivent répondre les offres.

[43] « OrDInateurs Commandés par l'État ».

[44] Technique d'achat, entièrement dématérialisée, qui permet, pour des achats d'usage courant, de présélectionner des opérateurs économiques pour la durée de validité du marché.

[45] L'article L. 2153-1 du code de la commande publique prévoit le principe d'égalité de traitement des opérateurs économiques issus de l'UE avec ceux issus d'États faisant partie de l'accord.

Le cahier des clauses administratives générales des marchés publics de techniques de l'information et de la communication (CCAG-TIC)[46] propose des clauses contractuelles standard applicables aux marchés publics dans le domaine du numérique, y compris la fourniture de matériel informatique. La possibilité de réaliser des audits de sécurité auprès des fournisseurs potentiels permet d'évaluer leur niveau de fiabilité. L'exigence de certifications de sécurité spécifiques peut constituer un critère de sélection pour s'assurer du niveau de sécurité.

Dans le domaine des matériels informatiques, les réponses des candidats aux appels d'offres sont évaluées sur le fondement de critères qui ont notamment trait aux spécificités techniques des matériels, au respect des standards de cybersécurité, à la qualité du support et aux enjeux de développement durable (consommation d'énergie, prévention des déchets, recyclage, etc.). En particulier, les ministères peuvent imposer des exigences en matière de sécurité (cf. *infra*), de garanties de performance et d'accords de niveau de service.

En pratique, cette sélectivité au regard des besoins exprimés permet d'écarter de l'attribution des marchés des distributeurs ou fabricants faiblement implantés sur le territoire national (impliquant un support technique plus limité sur le plan géographique) ou qui ne seraient pas en mesure de satisfaire aux normes techniques les plus exigeantes.

2.1.2.3 La certification et la validation par l'Anssi des matériels achetés

La sécurité informatique est une préoccupation majeure qui conduit les ministères à mettre en œuvre les meilleures pratiques pour protéger leurs actifs numériques et assurer la résilience de leurs systèmes d'information. À cet égard, les référentiels et les recommandations de l'Anssi, tels que le référentiel général de sécurité (RGS)[47], sont des éléments de référence.

La gestion des matériels informatiques – serveurs, ordinateurs, équipements de stockage et périphériques – repose sur des exigences techniques et environnementales précises.

D'une part, la qualité et la performance des équipements sont évaluées conformément aux critères définis dans le RGS et aux normes internationales. D'autre part, les procédures d'homologation et de contrôle de conformité des matériels font l'objet de dispositions réglementaires, en particulier la circulaire du Premier ministre n° 5725/SG du 17 juillet 2014 relative à la politique de sécurité des systèmes d'information de l'État (PSSIE), qui normalise les processus de validation pour chaque acquisition.

Les matériels informatiques acquis au travers des cadres interministériels font l'objet d'exigences techniques élémentaires de sécurité, qui ne sont pas vérifiées directement par l'Anssi. Les visas de sécurité, qui apportent une analyse en profondeur, sont essentiellement limités à des équipements spécialisés assurant une fonction de sécurité, comme les pares-feux, les équipements de chiffrement ou les passerelles de connexion à distance (VPN).

L'Anssi met ainsi à disposition des listes de produits certifiés, classés par type et niveau de sécurité, ainsi qu'une liste similaire pour les produits et services qualifiés.

---

[46] Arrêté du 30 mars 2021 portant approbation du cahier des clauses administratives générales des marchés publics de techniques de l'information et de la communication, modifié par l'arrêté du 29 décembre 2022.

[47] L'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives définit des fonctions de sécurité telles que l'identification électronique, la confidentialité, la signature électronique et l'horodatage électronique.

2.1.3 Un réseau interministériel de l'État, gage d'indépendance, dont la résilience doit continuer d'être renforcée

Le réseau interministériel de l'État (RIE) est un réseau unifié de communications électroniques qui interconnecte les services de l'État sur l'ensemble du territoire national. Sa gestion est assurée depuis 2019 par la Dinum. Avant sa mise en service, en 2015, une trentaine de réseaux ministériels coexistaient avec l'intranet AdER[48], créé en 2000.

La création du RIE a été décidée en 2011 pour faire face à l'insécurité dans un environnement numérique complexe et menaçant, garantir la continuité de l'action gouvernementale en cas de dysfonctionnement grave d'Internet, surmonter la fragmentation des réseaux ministériels et enfin réaliser des économies d'échelle grâce à la mutualisation des investissements et de l'exploitation.

2.1.3.1 Dix ans après, une mutualisation interministérielle réussie

Lors de son inauguration, en janvier 2015, le RIE reliait 5 000 sites. La phase de déploiement s'est poursuivie jusqu'à la fin des années 2010. Aujourd'hui, le RIE assure trois activités principales :

- le cœur du réseau (ou épine dorsale) gère les flux de collecte vers les centres de production informatiques exploitants les applications métiers ;
- la connexion entre les sites utilisateurs et l'épine dorsale est assurée par le réseau de collecte qui transporte des flux de données, reliant un million d'utilisateurs internes à travers environ 14 000 sites ;
- l'interconnexion entre AdER, le réseau inter-États membres de l'Union européenne (TESTA)[49], le réseau national de télécommunications pour la technologie, l'enseignement et la recherche (RENATER)[50], les réseaux partenaires (opérateurs de l'État) et Internet[51].

Le cœur de réseau, dit « dorsale » ou « *backbone* », repose sur des routeurs très haut débit de RENATER, permettant de connecter douze centres informatiques ministériels appelés « points de collecte nationaux ». Il transporte les flux de collecte vers les centres de production informatique hébergeant les applications métier. Les connexions locales[52] au RIE, en revanche, passent par des opérateurs tiers, Orange Business Services et SFR Business Team, dans le cadre d'un accord conclu en mai 2013.

[48] « Administration en réseau », qui permet l'échange de flux entre les ministères (messagerie, annuaires, partage d'applications, etc.)

[49] Le réseau TESTA (*Trans European Services for Telematics between Administrations*) permet de sécuriser les transmissions entre administrations nationales et européennes.

[50] RENATER a été créé en 1993 sous forme de GIP associant l'État, la conférence des présidents d'université et les principaux organismes de recherche. Il a alors fédéré les initiatives qui préexistaient.

[51] La plateforme d'accès à Internet (PFAI), hébergée sur quatre sites en France, assure le cloisonnement du réseau interne avec l'extérieur.

[52] Administrations centrales et déconcentrées de l'État, préfectures, services de police et de gendarmerie, directions régionales et agences régionales de santé, etc.

En 2020, la Cour constatait[53] *« le succès »* du RIE qui avait constitué *« un grand projet compte tenu de sa taille (60 M€), de sa complexité, notamment par le fait que ses instances de conduite devaient associer l'ensemble des ministères. Il a été mené à bien dans un calendrier serré. Son retour sur investissement est assuré depuis 2016, deuxième année d'exploitation. Il génère par rapport aux dispositifs antérieurs une économie annuelle de 19 M€. »*.

Parallèlement, le recours accru au télétravail et aux outils numériques a justifié des investissements importants (40 M€ entre 2021 et 2024) qui ont conduit à doubler l'épine dorsale avec des équipements différents tout en augmentant progressivement les débits de manière significative (passage de 10 à 100 Gbits).

D'autres réalisations significatives sont intervenues dans la période récente, telles que l'accompagnement des 14 000 sites utilisateurs dans la bascule vers la fibre optique et la mise en service des composants de la plateforme d'accès à Internet nouvelle génération. De nouvelles évolutions d'envergure sont à l'étude, comme la possibilité de relier certains *clouds* certifiés SecNumCloud ou d'exploiter le radio réseau du futur (RFF)[54].

2.1.3.2 Une consolidation du RIE à poursuivre

En 2021, le RIE a fait l'objet d'un audit de la mission d'organisation des services du Premier ministre, qui recommandait notamment une adaptation de son organisation et de ses moyens pour mener à bien son projet de modernisation, et répondre aux besoins de connectivité et de sécurité croissants. À ce titre, l'audit concluait que *« cette adaptation passe d'abord par une politique RH plus adaptée aux besoins […]. En outre, les ressources techniques et les applications métiers, obsolètes pour certaines, doivent évoluer rapidement pour atteindre l'état de l'art […] Par ailleurs, le dispositif de sécurité opérationnelle du réseau est toujours en cours de construction et doit être rapidement consolidé […] À moyen terme, les auditeurs estiment qu'un document, à vocation stratégique, doit être rédigé en lien avec les bénéficiaires du réseau et ses donneurs d'ordre interministériels, afin de définir les orientations futures du RIE »*.

Mi-2024, la Cour constatait que ces évolutions n'avaient qu'en partie été menées à leur terme[55]. Elle concluait notamment que *« des premières alertes ont permis d'envisager la réinternalisation des compétences clés pour ce réseau, qui toutefois n'en est qu'à son début. Plus largement, le partage d'informations et de stratégie entre la Dinum et les ministères demeure insuffisant pour un outil essentiel au fonctionnement quotidien des administrations. Une feuille de route partagée, associant davantage les ministères, est nécessaire pour disposer d'une vision pluriannuelle des services à déployer »*.

À cet égard, elle formulait les deux recommandations à l'intention de la Dinum :

- formaliser d'ici 2025 un plan de continuité d'activité (PCA) et un plan de reprise d'activité (PRA) pour le réseau interministériel de l'État ;

[53] Cour des comptes, *La conduite des grands projets informatiques*, juillet 2020, page 91.

[54] Réseau sécurisé de communication mobile très haut débit réservé aux forces de sécurité et de secours, qui s'appuie sur les réseaux des opérateurs téléphoniques ainsi que sur le RIE pour relier ses serveurs entre eux.

[55] Cour des comptes, *Le pilotage de la transformation numérique de l'État par la direction interministérielle du numérique*, juillet 2024, page 79.

- formaliser et réaliser le suivi de la feuille de route pluriannuelle du réseau interministériel de l'État avec des objectifs et jalons actualisés en lien avec les ministères.

À la suite de ces recommandations, la Dinum a indiqué avoir entrepris la rédaction d'un PCA et d'un PRA non pas du réseau proprement dit, le jugeant comme *« intrinsèquement, par construction, hautement résilient »*, mais du système d'information associé et des équipes chargées de son exploitation. Par ailleurs, elle indique que la feuille de route du RIE fait désormais l'objet d'une présentation annuelle aux membres du Cinum. L'année 2025 y est décrite comme *« une année de transition et de consolidation »* des évolutions du RIE.

2.2 La maîtrise de l'identité numérique des citoyens, enjeu de sécurité et de souveraineté porté par FranceConnect

FranceConnect est un téléservice, opéré par la Dinum, qui offre à un usager la possibilité, pour accéder à un service en ligne, d'utiliser une identité numérique qu'il a déjà établie auprès d'autres services. Ces autres services, dits « fournisseurs d'identité », peuvent être opérés par des administrations publiques (impots.gouv.fr, ameli.fr, France Identité du ministère de l'intérieur), des entités parapubliques (l'identité numérique de La Poste, la mutuelle sociale agricole), ou de partenaires privés.

Reconnu par un de ces fournisseurs d'identité, l'usager n'est pas obligé de créer une nouvelle identité numérique auprès du fournisseur de service en ligne. Ses informations personnelles sont automatiquement reprises. Lors d'une connexion via FranceConnect, l'identité de l'usager est systématiquement soumise au Répertoire national d'identification des personnes physiques (RNIPP) de l'Insee pour vérifier son existence et corriger les erreurs éventuelles (ordre des prénoms, traits d'union et accents, etc.).

En 2025, la Dinum revendique 43 millions d'usagers uniques actifs du service FranceConnect, soit 80 % de la population adulte en France. Plus de 1 000 fournisseurs de service sont référencés par la Dinum comme recourant à ce mode d'authentification.

Le déploiement de FranceConnect se justifie par des enjeux de souveraineté mais le pilotage par la Dinum mériterait d'être renforcé (2.2.1). Le dispositif a vu sa sécurité consolidée par le recours à FranceConnect+, permettant d'agir contre la fraude, ce qui justifie *a posteriori* les moyens financiers qui y sont engagés (2.2.2).

2.2.1 Un dispositif nécessité par des enjeux de souveraineté, un pilotage à renforcer

2.2.1.1 Les enjeux de souveraineté au cœur de la démarche de la Dinum

FranceConnect est né en 2014 afin de créer un outil souverain simplifiant l'identification numérique. Il n'existait pas, alors, d'offre unique d'identification numérique et d'authentification. Des acteurs privés développaient d'ores et déjà à grande échelle des modes d'identification, comme Facebook ID et Google ID qui permettent aux utilisateurs de ces plateformes d'accéder à de nombreux services opérés par des tiers sans à avoir se réidentifier.

Dans l'hypothèse où les services d'authentification de ces plateformes américaines étaient devenus les uniques standards, ces entreprises auraient acquis une position incontournable, y compris vis-à-vis des administrations publiques françaises. Recourir à leurs services pour s'authentifier sur des services publics aurait supposé que les utilisateurs y utilisent systématiquement leur identité réelle et que l'administration publique engage un échange avec ces plateformes américaines en cas de divergences d'informations avec le RNIPP de l'Insee. Ces dernières auraient ainsi pu constituer des bases très qualitatives de personnes physiques, nommément identifiées, permettant de mieux cibler encore leur politique commerciale.

La création de FranceConnect a donc permis à l'administration publique de garder la main sur l'authentification des utilisateurs de sites de service public.

Le caractère souverain de FranceConnect se traduit dans le choix d'hébergement de l'application au centre de données des douanes. Une solution de secours est hébergée sur le *cloud* Nubo du ministère des finances. Le stockage des sauvegardes de données est fait chez un opérateur du marché, dans une zone qualifiée SecNumCloud.

Outre les fournisseurs d'identité publics, FranceConnect s'appuie sur deux fournisseurs privés. La Dinum indique être vigilante à ce que ces fournisseurs respectent les principes posés à l'article 16 de la loi pour une République numérique selon lequel les administrations « *veillent à préserver la maîtrise, la pérennité et l'indépendance de leurs systèmes d'information. Elles encouragent l'utilisation des logiciels libres et des formats ouverts lors du développement, de l'achat ou de l'utilisation, de tout ou partie, de ces systèmes d'information* ». Elle indique que FacebookID et GoogleID ne pourraient dès lors pas être référencés comme fournisseurs FranceConnect. Si la Dinum affirme que les fournisseurs d'identité privés font l'objet d'une surveillance en matière de souveraineté, elle reconnaît que ce n'est que récemment que ces entreprises ont été interrogées à ce sujet et que les informations transmises doivent encore être expertisées.

2.2.1.2 Des contrôles déontologiques à renforcer face à une relative dépendance aux prestataires

Le développement et la maintenance de FranceConnect reposent principalement sur des prestataires, avec une équipe de 34 personnes en 2024 dont 27 sont des sous-traitants ou freelances. L'équipe technique est par exemple composée de onze personnes mais seul le directeur est un agent de la Dinum. L'équipe produit est composée de cinq personnes dont trois prestataires. Pour le support, sept personnes sur huit sont des prestataires.

Parmi les risques associés à une telle organisation résident ceux liés à la confidentialité des données. Ainsi, une entreprise sous-traitante du prestataire chargée d'assister les utilisateurs avait fait, sans l'autorisation de la Dinum, une copie de données utilisateurs de FranceConnect, sur son propre système d'information, pour réaliser des statistiques sur le traitement des tickets de leurs collaborateurs. En mars 2023, suite à une attaque informatique, ce sous-traitant s'est fait dérober des données, dont quelques dizaines comportaient des informations nominatives d'utilisateurs de FranceConnect. Cet incident a conduit la Dinum à rédiger un avenant au marché prévoyant des pénalités en cas de défaillance sur la protection des données et à demander à son prestataire de mettre fin à la collaboration avec ce sous-traitant. La qualité du service s'est alors fortement dégradée : le taux de tickets traités pour les demandes usagers est

passé d'une moyenne de 93,3% sur les cinq premiers mois de l'année 2023 à 63,6 % sur les sept mois suivants. La Dinum semble avoir subi cette situation.

De façon générale, les équipes chargées de FranceConnect connaissent un fort taux de rotation : depuis 2018 en moyenne, 40 % des effectifs présents sur le projet chaque année n'étaient pas présents l'année précédente. Ces effectifs peuvent être des prestataires ou des agents de la Dinum, qui, très majoritairement, sont sous statut contractuel. La Dinum indique avoir engagé une démarche de transformation des contrats à durée déterminée en contrats à durée indéterminée afin de fidéliser ses agents. Ces agents contractuels sont soumis aux droits et obligations des fonctionnaires, notamment en matière de déontologie. Néanmoins, il apparaît que la Dinum ne procède pas aux contrôles minimums auxquels elle devrait s'astreindre en tant qu'employeur.

Aux termes de la loi de transformation de la fonction publique du 6 août 2019, le contrôle déontologique de la plupart des agents publics relève de l'administration elle-même. Il doit par exemple s'effectuer en amont d'un départ de l'agent vers une entreprise privée. Ce contrôle est internalisé, dans la mesure où il est effectué par le supérieur hiérarchique de l'agent, qui peut consulter le référent déontologue en cas de difficulté. Le supérieur hiérarchique prend lui-même la décision quant à la faisabilité du projet de reconversion professionnelle de l'agent.

La Dinum n'a pas été en mesure d'attester du respect de ces obligations. En tant que responsable de l'animation de la filière numérique publique, elle devrait se préoccuper de ce sujet au-delà de ses seuls effectifs et mettre en place un processus de traitement adapté, matérialisé par un registre de traitement déontologique. En s'assurant que le savoir-faire développé au sein de l'administration ne profite pas directement à des entreprises étrangères, elle répondrait à l'enjeu de souveraineté qui s'attache aussi à cette préoccupation.

2.2.2 La sécurité du dispositif tardivement durcie pour lutter contre la fraude

2.2.2.1 L'insuffisante anticipation de la cybersécurité n'a freiné que tardivement des fraudes massives

Au-delà de la souveraineté, FranceConnect porte des enjeux en matière de cybersécurité. Aujourd'hui encore, pour les services basés sur une identité de niveau faible, il suffirait, par exemple, qu'une personne malveillante récupère le numéro de sécurité sociale et le mot de passe d'un usager au site ameli.fr pour s'authentifier sur de nombreux autres téléservices.

Ce phénomène de « centralisation des risques » avait été anticipé par la CNIL dans son avis de juillet 2015 préalable à la mise en service de FranceConnect[56]. Selon la CNIL, « *en cas d'usurpation d'identité auprès d'un fournisseur d'identité, le risque d'accès aux autres services, via la facilité offerte par FranceConnect, est démultiplié* ». Elle incitait les porteurs du projet à ajouter des facteurs d'authentification et à informer l'usager par mail ou texto d'une connexion via FranceConnect, ce que la Dinum a mis en place. La CNIL recommandait aussi que les fournisseurs de service et d'identité se conforment à l'obligation de réalisation préalable d'une étude d'impact sur la vie privée afin de traiter des risques de manière proportionnée,

[56] Délibération de la Cnil n° 2015-254 du 16 juillet 2015.

notamment quant au degré d'authentification. Cette recommandation n'a pas été suivie, aucune partie ne se considérant comptable de l'environnement global de FranceConnect. La Dinum n'a, de son côté, pas cherché à vérifier les dispositifs de sécurité anti-hameçonnage mis en place par les fournisseurs d'identité.

Selon le référentiel européen eIDAS[57], FranceConnect apporte un niveau de garantie dit « *faible* » en ce qu'il se fonde sur le recours à un identifiant et un mot de passe. Des usurpations d'identité ont été détectées et relayées par la presse en 2022, notamment pour l'accès au service « *Mon Compte Formation* », qui proposait FranceConnect pour identifier ses bénéficiaires. Ces usurpations, qui préexistaient à l'utilisation du dispositif, ont engendré des fraudes massives sur les formations, poursuivies à moindre échelle en 2023 et 2024.

Pour contrer ces fraudes, l'authentification au dispositif a été renforcée par le recours à FranceConnect+ de niveaux dits « *substantiel* » (pour l'identité numérique de La Poste) et « *élevé* » (pour le service proposé par France Identité). Selon la Dinum, cette bascule vers FranceConnect+ a réduit significativement les tentatives de fraudes à l'identification sur ce service en ligne. Fin 2022, la Dinum constatait que les signalements de tentatives d'usurpation d'identité étaient passées « *de 20 à 30 par jour à 10 en novembre, sans fraude avérée à ce stade* ».

Les démarches sensibles conduisant à une transaction financière, comme MaPrimeRénov, le chèque emploi service universel ou le changement de coordonnées bancaires sur Ameli, ont été soumises à une authentification par FranceConnect+. L'Anssi et la Dinum ont établi une doctrine spécifiant les usages nécessitant des identités de niveau de garantie substantiel ou élevé afin d'orienter les fournisseurs de services sur la solution d'authentification adaptée. Cette doctrine n'est toutefois pas encore systématiquement mise en œuvre.

De leur côté, les fournisseurs d'identité de niveau « *faible* » ont été incités à renforcer l'utilisation d'un identifiant / mot de passe par l'envoi d'un mot de passe à usage unique (dit *One Time Password*, ou OTP) par mail ou par SMS ou par des règles d'authentification multi-facteurs. Ainsi, le fournisseur d'identité Ameli.fr a modifié la technologie employée en ajoutant un OTP par mail en décembre 2023. La technologie doit être généralisée à tous les fournisseurs d'identité proposant une identité numérique de niveau d'authentification faible courant 2025. La DGFiP a indiqué qu'elle le mettrait en place à la fin du premier semestre 2025, après la campagne de déclaration des revenus de l'année 2024 des particuliers.

Après les constats d'usurpations d'identités opérés en 2022, il a fallu attendre 2024 pour que la Dinum mette en place une équipe chargée de mieux détecter ces fraudes, les signaler et y réagir, en partenariat avec les fournisseurs de service et d'identité. Des référents anti-fraude ont été désignés dans les différentes équipes de FranceConnect et un comité de pilotage pour la gestion et le suivi des fraudes a été instauré sur un rythme trimestriel, associant les fournisseurs d'identité et les principaux fournisseurs de service.

En plus de cette organisation interne, la Dinum gagnerait à professionnaliser sa stratégie de lutte contre la fraude en s'inscrivant dans le programme de travail de la mission interministérielle de lutte contre la fraude (Micaf), qui coordonne les administrations et organismes publics en matière de la lutte contre la fraude aux finances publiques et favorise

[57] Issu du règlement européen du 23 juillet 2014 relatif à l'identification électronique, dit eIDAS (electronic IDentification, Authentication and trust Services).

l'articulation des actions administratives et judiciaires. La Dinum pourrait utilement participer aux groupes spécialisés dans la fraude documentaire et à l'identité et dans celui relatif à l'adaptation des moyens d'enquêtes aux enjeux du numérique.

2.2.2.2 Des dépenses directes qui ne reflètent pas le coût complet de FranceConnect

Le coût prévisionnel de FranceConnect n'a pas été établi par la Dinum lors de son lancement en 2014. La première mention d'une estimation du coût total du projet, à hauteur de seulement 4,5 M€, figure dans le rapport annuel de performance pour l'année 2015, déposé au Parlement en mai 2016.

Encore aujourd'hui, le coût du projet FranceConnect n'est pas précisément établi par la Dinum, qui fournit des informations hétérogènes sur le sujet dans les différents documents budgétaires. En recoupant ces informations, le montant des dépenses de fonctionnement et d'investissement réalisées par la Dinum sur la période 2014-2023 peut être évalué à 40 M€, y compris les dépenses de personnel rattachées au projet. Dans une logique de produit, dont les fonctionnalités ont vocation à évoluer, la Dinum continue d'investir sur FranceConnect et y a consacré 4,8 M€ en 2024, auxquels s'ajoutent des dépenses de personnel pour 0,7 M€.

La Dinum met en regard ce coût avec les économies, bien plus élevées, que l'ensemble des produits FranceConnect aurait permises grâce à la lutte contre la fraude. Il faut noter que le service d'authentification renforcée apporté par FranceConnect+ et qui permet d'éviter des usurpations d'identité, n'aurait pas été accessible avec des services d'identification comme ceux fournis par les grandes plateformes américaines, dont les contrôles sont limités.

Mais si FranceConnect est gratuit pour les usagers, il ne l'est pas pour les fournisseurs de services et d'identité qui doivent adapter leur système d'information pour s'arrimer à l'application. Le coût d'intégration est différent pour les fournisseurs de service et pour les fournisseurs d'identité, ainsi qu'entre fournisseurs d'identité selon le niveau de garantie qu'ils doivent respecter pour identifier et authentifier les usagers.

Les fournisseurs de services doivent faire face à des coûts d'intégration et de maintenance. La Dinum relève ainsi que certains fournisseurs, notamment dans les collectivités locales ou les centres hospitaliers, disposent de systèmes informatiques anciens ou peu flexibles, ce qui peut rendre l'intégration de FranceConnect plus complexe. Pour les petites structures, le manque d'expertise technique est susceptible de constituer un obstacle. Celles-ci doivent dès lors faire appel à des éditeurs, une solution potentiellement coûteuse, susceptible de conduire à une certaine dépendance. Enfin, après l'intégration à FranceConnect, la maintenance des certificats, la gestion des mises à jour et la surveillance des systèmes de sécurité représentent une charge supplémentaire.

Calculer le coût moyen d'adhésion à FranceConnect permettrait aux fournisseurs de services d'anticiper leurs dépenses. Cette information permettrait à la Dinum d'adapter l'accompagnement qu'elle procure aux fournisseurs de services, en particulier dans la perspective de la dématérialisation des démarches publiques au sein des collectivités.

De leur côté, les fournisseurs d'identité de niveau « *faible* » font face à un coût technique limité dans la mesure où il s'agit de créer une brique logicielle reliant leurs annuaires à FranceConnect avec une adresse pivot et le mot de passe pour la vérification de l'identité. Les

fournisseurs d'identité de niveau « *substantiel* » ou « *élevé* » doivent quant à eux intégrer des dépenses de vérification d'identité pour valider le compte d'un usager.

Gestionnaire de l'identité numérique de La Poste, Docaposte indique ainsi faire face à un coût de 32 M€ par an pour répondre aux demandes de création et de gestion des identités, qui nécessitent une intervention humaine, que la demande soit faite en ligne ou en bureau de poste. Docaposte envisageait initialement de compenser ces dépenses par la vente de prestations de services pour les entreprises privées. Par exemple, intégrer l'identité numérique pour la création d'un compte bancaire permettrait, selon elle, d'améliorer le taux de transformation de prospect à client, de diminuer les coûts des procédures obligatoires de connaissance de la clientèle, tout en garantissant une conformité à la réglementation bancaire. Toutefois, l'entreprise n'a pas encore trouvé suffisamment de débouchés commerciaux sur cette activité et demande désormais la possibilité de facturer les entités publiques fournisseurs de service au titre de la prestation que l'identité sécurisée et souveraine leur apporte.

Sans auditer le coût allégué par Docaposte, la Dinum a proposé une prise en charge partielle du coût lié à la fourniture d'identité numérique renforcée, qu'elle émane aujourd'hui de Docaposte ou de France Identité, voire demain de fournisseurs d'identité privés. Elle a proposé qu'un budget forfaitaire de 15 M€ soit consacré chaque année à la compensation partielle du coût de gestion de ces deux services, provenant des principales administrations utilisatrices de FranceConnect+ (à ce jour, la Caisse des dépôts pour Mon Compte Formation et l'INPI). Cela porterait le coût du dispositif à une vingtaine de millions d'euros par an, ce qui semble proportionné aux économies permises par le dispositif dans la lutte contre la fraude.

La question d'un recours plus généralisé à FranceConnect+ pour l'accès aux services publics en ligne n'est pas close. Une vigilance doit être maintenue alors que la doctrine d'utilisation édictée par l'Anssi et la Dinum en la matière n'est pas encore pleinement mise en œuvre par les fournisseurs de service.

2.3 Les enjeux de souveraineté des applications amplifiés par les revirements technologiques et commerciaux des éditeurs

Les suites bureautiques et de messagerie sont les outils logiciels les plus répandus. Les ministères ont, pour la plupart, déployé des solutions propriétaires communément utilisées par ailleurs. Si les administrations se tournent désormais vers des solutions libres, ce mouvement s'opère en ordre dispersé (2.3.1). Les enjeux associés aux applications métier portent sur la capacité des administrations à assurer le plein contrôle des outils, et changer si besoin de solution. Le développement à façon de logiciels permet une maîtrise mais engendre des risques sur les coûts et délais de mise en œuvre des solutions. Lorsque l'administration recourt à des logiciels du marché, ces surcoûts et délais se retrouvent en fin de processus si l'administration souhaite changer d'outils (2.3.2).

2.3.1 Les suites bureautiques et les logiciels de communication, outils du quotidien au caractère souverain mal assuré

2.3.1.1 L'enjeu de la bascule des suites bureautiques sur le *cloud*

La suite bureautique Office éditée par Microsoft est un outil qui s'est grandement répandu dans les entreprises et administrations. Avec l'incitation gouvernementale à recourir aux logiciels libres, quelques administrations publiques ont fait le choix d'utiliser des outils fondés sur de tels logiciels – par exemple la DGFiP avec LibreOffice –, mais la plupart sont restées sur les outils de Microsoft. Comme les systèmes d'exploitation des postes de travail (cf. encadré ci-après), ces logiciels sont utilisés au quotidien par les agents et la maîtrise de leurs fonctionnalités fait partie des compétences communément partagées.

La position prédominante de Microsoft Windows sur les postes de travail des agents

Le système d'exploitation Microsoft Windows est installé sur la plupart des postes de travail des administrations françaises. Ce choix s'explique notamment par un écosystème logiciel complet (bureautique et applications métiers) et les habitudes des utilisateurs.

Dans le cas des serveurs informatiques, l'usage de distributions *open source* Linux est en revanche répandu. Leur stabilité, leurs performances et la réduction observée des coûts de licence – malgré la nécessité d'un support technique qualifié – en font une option privilégiée.

Des migrations des postes de travail vers Linux ont été tentées dans des administrations publiques, mais elles ont connu des issues diverses en raison d'obstacles significatifs : compatibilité applicative insuffisante, résistance au changement des utilisateurs et des équipes informatiques, coûts non anticipés de la migration, de la formation et du support technique.

La Gendarmerie nationale a toutefois migré avec succès, entre 2007 et 2014, environ 90 000 postes de travail vers un système d'exploitation libre. Les économies réalisées sur les licences logicielles avaient été estimées à environ 50 M€. Cette expérience de longue date constitue un précédent intéressant pour d'autres administrations.

Par ailleurs, quelques pays tentent de développer des systèmes d'exploitation souverains, malgré les défis techniques. En Chine, d'importants investissements soutiennent le développement de systèmes qui s'appuient sur Linux ou d'autres architectures. En France, l'Anssi a expérimenté entre 2005 et 2020 le développement d'un système d'exploitation basé sur Linux, dénommé ClipOS, conçu pour répondre à des exigences de sécurité très élevées.

Aujourd'hui, l'approche de l'État se veut pragmatique : utiliser les logiciels libres lorsque cela est pertinent, garantir la coexistence et la sécurisation des infrastructures, et concentrer les efforts sur le renforcement de la souveraineté des infrastructures et applications.

La Dinum anime le « Socle interministériel de logiciels libres » afin de rationaliser les choix logiciels de l'administration (suites bureautiques, navigateurs, outils de développement, gestion de contenu ou bases de données, systèmes d'exploitation). L'Anssi publie régulièrement des recommandations pour la sécurisation des systèmes Windows. Des configurations spécifiques et versions durcies de Linux ont été élaborées pour les environnements sensibles.

Si ces démarches visent à renforcer la souveraineté numérique de l'État, elles n'ambitionnent pas le remplacement massif du système d'exploitation actuellement dominant sur les postes de travail de ses agents.

Si Microsoft a, pendant longtemps, commercialisé sa suite bureautique dans le cadre uniquement de licences installées sur les postes des utilisateurs, l'entreprise a introduit, au début des années 2010, une nouvelle version, appelée aujourd'hui Microsoft 365. Cette offre propose, sous forme d'abonnement mensuel, l'ensemble des outils bureautiques et de messagerie en version *cloud*, Microsoft prenant en charge l'hébergement des données et documents.

Depuis, les deux offres cohabitent, mais Microsoft favorise la version *cloud*. Une version traditionnelle continue d'être lancée tous les trois ans environ (la dernière, en 2024), mais elle ne reçoit pas de fonctionnalités nouvelles au fil de l'eau, ni ne permet d'accéder aux autres services *cloud* de la marque, et son support est limité dans le temps.

La bascule vers cette proposition *cloud* entraîne deux conséquences : l'hébergement des documents et données est assuré par Microsoft, entreprise soumise aux lois extraterritoriales américaines ; le modèle économique, fondé sur une amélioration continue des outils, se traduit par des augmentations tarifaires régulières. Ainsi, début 2025, Microsoft a annoncé une hausse de ses tarifs de l'ordre de 30 % avec l'intégration de fonctionnalités d'intelligence artificielle au sein de ses différents logiciels bureautiques.

La suite Microsoft 365 inclut la messagerie Outlook. Dans la lignée de la doctrine « *Cloud au centre* » édictée par le Premier ministre (cf. 3.1.1), la Dinum a écrit dès septembre 2021 aux secrétaires généraux des ministères pour leur spécifier que les messageries électroniques devaient être considérées comme maniant, par essence, des données sensibles. Ce postulat n'était pas argumenté plus avant, mais il a eu pour conséquence de rendre inenvisageable le recours à Microsoft 365.

Certains ministères ont plaidé pour une dérogation et obtenu gain de cause auprès du Premier ministre, comme le ministère de la culture et celui des affaires sociales. La plupart ont toutefois été amenés à renoncer à cet outil, en conservant une version des logiciels de Microsoft, hébergée sur leurs propres serveurs, ou en préparant, pour certains, une migration vers d'autres logiciels respectant le caractère souverain des informations échangées.

Tel a été le cas du ministère de l'éducation nationale (MEN) qui a, dès 2019, initié le programme « *Environnement de travail numérique des agents* » (ETNA) afin de moderniser les outils mis à disposition de ses 1,2 million d'agents. Ce programme vise plusieurs objectifs :

- répondre aux insatisfactions exprimées par les agents sur la qualité et la performance de leurs outils de travail. Un tiers des agents utilisait officieusement des services grand public (type Gmail, Google drive, Dropbox, Doodle, etc.) pour des usages professionnels. Cet usage informel, dit « *Shadow IT* », entraîne des risques, aussi bien en termes de cybersécurité que de protection et de maîtrise des données ;
- transformer les usages numériques des utilisateurs ;
- renforcer le sentiment d'appartenance des personnels au ministère.

Ce programme porte sur les outils de travail collaboratifs et n'inclut pas dans son périmètre les applications métier, outils pédagogiques et espaces numériques de travail.

L'état des lieux réalisé par la direction du numérique pour l'éducation (DNE) avait relevé un éclatement des usages avec seulement cinq outils présents dans toutes les académies, sur plus de 80 logiciels collaboratifs utilisés. Par exemple, 16 outils de visioconférence ont été recensés, alors même qu'un outil (VisioAgents) était utilisé dans toutes les académies.

Tableau n° 1 : répartition des outils de travail collaboratif selon le nombre d'académies qui y recourent

Type d'outil	Présent dans …					Total
	toutes les académies	+ de 80 % des académies	entre 30 % et 80 % des académies	- de 30 % des académies	une seule académie	
Bureautique	1	0	1	2	2	6
Visioconférence	1	2	3	4	6	16
Partage de documents	1	0	2	4	7	14
Espaces collaboratifs	1	0	0	8	8	17
Messagerie instantanée	0	0	1	5	9	14
Messagerie et outils	1	2	1	1	10	15

Source : Cour des comptes à partir de données ministère de l'éducation nationale

L'analyse menée par le ministère sur les usages et attentes des agents a montré le besoin de fonctions collaboratives dans les logiciels bureautiques. Les études comparatives ont porté la direction du numérique pour l'éducation (DNE) vers la solution libre d'édition en ligne Collabora Online.

En 2024, le ministère a décidé d'héberger cette solution, tout comme la messagerie, dans un des centres de données interministériels, afin de maîtriser l'exploitation et rester dans un environnement souverain. Les solutions d'hébergement qualifiées SecNumCloud présentes sur le marché ne répondaient pas aux exigences posées par le ministère, en termes notamment de redondance du stockage. Par ailleurs, le coût d'hébergement d'une telle solution logicielle en environnement SecNumCloud était estimé à 2,9 M€ par an contre un investissement matériel de 3,4 M€ sur une durée de huit ans pour un hébergement en centre de données. Parallèlement au déploiement progressif de Collabora Online, le ministère continue de recourir aux logiciels et services de Microsoft[58].

Le choix du MEN d'évoluer vers une offre libre du marché n'est pas celui qu'a opéré la Dinum. Elle a lancé, en 2023, le programme « *La Suite* » qui est un ensemble d'outils bureautiques classiques (traitement de texte, tableur, outil de présentation) mais aussi une messagerie électronique, un système de visioconférence et de webconférence.

[58] Cf. avis d'attribution de marché n° 25-28385 publié le 14 mars 2025 relatif à la fourniture de diverses solutions et prestations de type Microsoft pour une durée initiale de 12 mois renouvelable jusqu'à 48 mois, comportant plusieurs accords-cadres d'une valeur approximative de 2 M€ pour ce qui concerne les services centraux et déconcentrés du ministère (sur un total de 75 M€ qui inclut 300 opérateurs de l'enseignement supérieur et de la recherche).

En parallèle, la Dinum a engagé, avec le secrétariat d'État allemand au numérique, une coopération en matière de maîtrise des logiciels des administrations publiques, dans une perspective de souveraineté numérique. La déclaration d'intention conjointe, signée le 5 février 2024, visait notamment à exploiter un ensemble de logiciels libres de premier ordre offrant aux agents des espaces de travail numériques souverains. Un des axes de coopération consistait à « *partager la recherche, le design produit et les travaux relatifs aux suites collaboratives libres effectuées en France (La Suite) et en Allemagne (openDesk)* » et à constituer des « *équipes produits à l'échelle européenne* ». Les Pays-Bas ont rejoint cette initiative en septembre 2024.

La Dinum promeut sa démarche dans une logique de maîtrise budgétaire qui repose d'abord sur la recherche d'économies d'échelle, « *rendue possible par la consolidation de besoins jusque-là dispersés, et par la mutualisation de l'infrastructure, de l'expertise et de la maintenance* ». Néanmoins, le MEN estime que la solution de la Dinum, développée postérieurement au choix du ministère de retenir Collabora Online, n'aurait pas été adaptée à une organisation de 1,2 million d'agents, notamment en termes de dimensionnement. Si le MEN intègre certaines applications proposées par la Dinum, la divergence d'approches entre le premier employeur public et la direction interministérielle témoigne de la difficulté de cette dernière à assurer un alignement interministériel sur une composante essentielle de l'offre numérique.

Ce sujet sera examiné plus avant par la Cour dans le cadre du prochain rapport d'initiative citoyenne sur « *le coût des prestations et de licence des outils bureautiques et collaboratifs* ». En tout état de cause, entre l'offre de la Dinum et les solutions du marché, des alternatives solides existent aux solutions de messagerie et de bureautique non souveraines.

2.3.1.2 Le point faible des messageries instantanées et des smartphones

Ces dernières années, les applications de messagerie instantanée ont occupé une place grandissante dans les communications interpersonnelles. Les membres du Gouvernement et des cabinets ministériels avaient notamment recours aux messageries Telegram, basée aux Émirats Arabes Unis, et WhatsApp (Meta). Ces applications permettent de partager tous types d'informations, y compris des données qui peuvent être sensibles.

Dans le panorama des messageries instantanées, Tchap est une application lancée par la Dinum en 2019, issue d'un protocole libre, Matrix. L'application est reliée à l'annuaire interministériel, et permet d'inviter des personnes extérieures à l'administration dans des boucles de discussion. Son développement, accompagné par l'Anssi pour garantir le respect de standards de sécurité, suit une feuille de route qui permet d'en enrichir les fonctionnalités.

En avril 2022, la Dinum demandait de déployer Tchap au sein des cabinets ministériels en soulignant que les outils grand public présentaient « *de sévères lacunes en termes de confidentialité des échanges* ». Malgré la gravité du constat, cette requête n'a pas été suivie et les messageries non souveraines ont continué à être utilisées à tous les niveaux de l'État.

Par circulaire du 22 novembre 2023, la Première ministre a demandé aux membres du Gouvernement et des cabinets ministériels de déployer l'application de messagerie instantanée Olvid, en remplacement de toute autre application déployée hors d'une maîtrise publique. Olvid était alors présentée comme « *la seule plateforme de messagerie privée ayant reçu la certification de sécurité de premier niveau (CSPN) de l'Anssi* ». Cette décision était présentée

comme « *le signe d'une prise de conscience en matière de cybersécurité, mais aussi une plus grande souveraineté technologique française* ».

La circulaire précisait que la solution retenue n'était pas soumise à la règle de la doctrine « *Cloud au centre* », qui porte sur le maniement des données sensibles (cf. 3.1.1). Elle s'appuyait sur le fait que les données circulant via Olvid étaient chiffrées de bout en bout, donc « *illisibles par toute personne ou organisation n'étant ni expéditrice ni destinataire d'un message, et de surcroît supprimées aussitôt la délivrance d'un message* ». La doctrine ne prévoit pourtant pas d'exemption dans les cas où les communications seraient chiffrées.

Pour singulière qu'elle puisse paraître, cette précision était nécessaire dès lors qu'Olvid ne respectait pas l'exigence de souveraineté, en recourant aux services d'une entreprise américaine pour l'hébergement de son serveur de distribution des messages. La Dinum, pour qui cette circulaire relevait d'une décision politique, estime que cette solution constituait un risque dès lors que ce volet d'hébergement ne faisait pas partie de la certification CSPN obtenue par Olvid et que cette solution n'était pas immune au droit extra-européen. La circulaire de la Première ministre présentait Olvid comme complémentaire au déploiement de Tchap auprès des agents publics. Ainsi, les membres du Gouvernement et des cabinets ministériels, à qui il était demandé d'utiliser Olvid, n'étaient pas incités à utiliser la même solution, pourtant souveraine, que le reste de l'administration publique. Ce choix peut s'expliquer par le sentiment que les fonctionnalités et l'ergonomie de Tchap n'étaient alors pas suffisamment abouties. Il traduisait en tout cas un décalage entre les exigences de souveraineté inscrites dans la circulaire et la pratique des autorités.

Malgré l'injonction portée par cette circulaire, le déploiement d'Olvid est resté minime au sein des cabinets ministériels. En janvier 2025, le cabinet du Premier ministre a finalement demandé à l'ensemble des cabinets ministériels d'utiliser Tchap. Il semble que cette application soit désormais plus communément utilisée dans les différentes administrations. En avril 2025, la Dinum y revendiquait 300 000 utilisateurs actifs. Plus de 76 millions de messages ont été échangés via l'application en 2024, en hausse de près de 50 % par rapport à 2023. En juillet 2025, la circulaire n° 6497/SG du Premier ministre a de nouveau demandé aux ministères de renforcer la sécurité des communications de leurs agents par messagerie instantanée en déployant largement Tchap et en favorisant son adoption.

La question des messageries instantanées, outils du quotidien, illustre la porosité entre les usages professionnels des agents publics, qui doivent être strictement encadrés et soumis à des règles de sécurité, et les usages personnels. Tous les agents ne disposent pas d'un téléphone professionnel et beaucoup utilisent leur téléphone personnel pour des usages professionnels. Certains agents qui disposent d'un téléphone professionnel ont renoncé à leur téléphone personnel et combinent l'ensemble des usages sur le même appareil. Cette pratique est en ligne avec les messages de sobriété numérique, mais peut engendrer des risques en termes de sécurité si la flotte d'équipements n'est pas pleinement contrôlée.

Ainsi, en mars 2023, le ministre de la fonction publique adressait une note à l'attention des ministres pour limiter l'usage d'applications récréatives sur les appareils de téléphonie mobile professionnels des agents publics. Il s'agissait d'applications de jeux, de *streaming* ou de réseaux sociaux. La note rappelait que la totalité du répertoire téléphonique peut être accessible aux applications ainsi téléchargées. Elle ciblait notamment l'application TikTok après que la Commission européenne eut interdit son installation sur les appareils professionnels. Selon la Dinum, une majorité de ministères dispose d'outils de gestion centralisée des flottes de téléphones mobiles, ce qui a permis de mettre en œuvre cette directive.

⁂

Bien que la suite bureautique de Microsoft et les messageries grand public dominent le paysage numérique, des alternatives souveraines viables existent. Développées sous logiciel libre, par des entités publiques ou entreprises européennes, elles garantissent que les données sensibles sont à l'abri des législations extra-européennes. L'Anssi recommande la séparation des usages professionnels et personnels, mais la généralisation de flottes de téléphones mobiles professionnels représenterait un coût élevé pour les administrations. Aussi, il conviendrait d'encadrer plus fermement les usages des agents sur leurs équipements personnels.

Recommandation n° 1. (Direction interministérielle du numérique) : Mettre en place en 2026 avec les ministères un calendrier de déploiement d'outils de bureautique et de communication respectant la souveraineté des données.

2.3.2 La souveraineté des applications métier passe par une meilleure maîtrise des logiciels et leur exploitation

Les systèmes d'information de l'État sont principalement composés d'applications métiers qui contribuent à la réalisation des missions des administrations. Ces applications, parfois anciennes, ont pu être développées dans des technologies robustes mais désuètes et, pour certaines, ne sont plus maintenues par leurs éditeurs. Elles contribuent alors à la « *dette technique* » de l'administration publique. Le rapport de la Cour des comptes sur le pilotage de la transformation numérique de l'État soulignait que l'évaluation de la dette technique des acteurs publics constituait *« un chantier complexe sans pilotage établi »*[59].

Même lorsque les logiciels ne sont pas obsolètes, les éditeurs peuvent faire le choix de ne plus les maintenir. L'enjeu de souveraineté réside alors dans la capacité des administrations à assurer le fonctionnement de ces applications et leur évolution pour répondre aussi bien aux dispositions législatives ou réglementaires nouvelles qu'à l'évolution des usages. Il se traduit également par la capacité qu'ont les administrations à changer d'éditeur ou de prestataire.

2.3.2.1 L'arbitrage entre le développement interne et le recours aux logiciels du marché

Deux modèles existent pour la mise en place d'applications métier : le développement sur mesure ou le recours à des logiciels existants, éventuellement adaptés aux spécificités des usages de l'administration. Ces applications sont généralement hébergées dans des centres informatiques internes, avec une exploitation maîtrisée par l'administration. En ce sens, il n'y a pas de risque d'hébergement ou de transfert des données hors de l'UE. Le développement, la maintenance, le support peuvent toutefois être partiellement ou totalement sous-traités.

Le parc applicatif du MEN comporte plus de 400 applications nationales et près de 1 500 applications locales conçues par les équipes académiques avec un faible taux de mutualisation.

[59] Cour des comptes, *Le pilotage de la transformation numérique de l'État par la direction interministérielle du numérique*, avril 2024.

Les applications nationales, qui étaient historiquement diffusées à chaque académie pour mise en production, sont de plus en plus exploitées sur une plateforme d'hébergement mutualisée, dans le centre de données interministériel des douanes ou sur la plateforme d'hébergement académique, hébergée par le ministère de l'agriculture. Ces deux centres de données coexistent avec 36 salles informatiques académiques, mais depuis 2016, la plateforme d'hébergement mutualisée est passée de 23 applications ou services accueillis à plus de 160, incluant les plateformes de parcours étudiants Parcoursup et Mon Master. Cette croissance témoigne du souci d'un plus grand professionnalisme dans l'exploitation des applications, gage de sécurité.

Les principales applications métier sont développées par des équipes ministérielles et des prestataires, sous pilotage interne. Si cette démarche facilite la maîtrise du système d'information, elle est sujette à des dérives de coût et de délais.

Tel a été le cas de Cyclades, qui gère les examens et concours du MEN ainsi que plus de 600 concours d'autres ministères. Dans son rapport de 2020 sur les grands projets numériques de l'État[60], la Cour avait souligné que Cyclades avait reçu un avis défavorable de la Dinsic (ancienne dénomination de la Dinum) au regard de la durée du développement (cinq ans avant la première version), de la fragilité de l'organisation du projet et des risques de dépassement du calendrier et du budget.

De fait, le projet qui était présenté en 2012 avec une durée de cinq ans et un coût prévisionnel de 26 M€ a finalement duré dix ans et engendré 63,8 M€ de dépenses jusqu'en 2022. Par la suite, le ministère a encore consacré 5,2 M€ en 2023 puis 4,3 M€ en 2024 pour le maintien en conditions opérationnelles et les évolutions de l'application, soit un total de 73,3 M€ à date.

Le ministère explique le dépassement du coût du projet notamment par des réformes des examens non prévues à son lancement avec la réforme du diplôme national du brevet en 2017 et celle du baccalauréat à partir de 2019 (+7,4 M€) et par une modernisation non anticipée des processus comme la mise en œuvre de la dématérialisation des copies du bac et leur correction (+6,3 M€). Ces montants ne représentent toutefois qu'une partie des dépassements constatés.

Développer des logiciels sur mesure permet de répondre aux besoins spécifiques des administrations publiques, *a fortiori* lorsque, comme dans le cas de Cyclades, aucune alternative existe sur le marché. Cela permet aussi une meilleure maîtrise des fonctionnalités et de l'exploitation, contribuant ainsi à renforcer le caractère souverain de ces logiciels. Mais cette expérience, comme tant d'autres au sein des administrations publiques dont la Cour a pu se faire l'écho, montre que cette démarche entraîne des risques élevés de dérives de délais et de coût.

Pour d'autres applications, le choix a été fait de recourir à des progiciels éprouvés du marché, sans renoncer à une maîtrise de l'exploitation. Tel est le cas du système d'information comptable et financier de l'État, Chorus, hébergé dans deux datacenters de l'administration : le principal se trouve au ministère des finances à Paris et celui de secours est opéré à Toulouse par le ministère de l'agriculture. L'exploitation du progiciel est assurée par la DGFiP, mais plusieurs prestataires - dont les maisons mères sont françaises ou européennes - interviennent.

L'Agence pour l'informatique financière de l'État (AIFE), qui assure la maîtrise d'œuvre de Chorus, précise que les marchés de support et maintenance, d'une durée de six ans,

[60] Cour des comptes, *La conduite des grands projets numériques de l'État*, juillet 2020.

sont renouvelés à chaque échéance via des appels d'offres. Le lotissement de ces marchés permet de diversifier les prestataires, hormis SAP, éditeur du progiciel, qui est le seul à pouvoir assurer le support et la maintenance des licences dans les conditions exigées par l'AIFE.

L'analyse menée par l'AIFE en amont de la migration de Chorus vers la nouvelle version S/4Hana a montré que d'autres options que SAP étaient alors envisageables, mais pour une durée de déploiement plus longue (six ans au lieu de quatre ans et demi) et un coût complet entre 110 % et 160 % supérieur, surcoût notamment lié au travail des équipes de l'AIFE en cas de changement d'éditeur, avec une surcharge évaluée à 234 000 jours-hommes, soit 64 M€.

L'étude menée par l'AIFE a montré que l'État était en mesure de procéder à un changement d'éditeur si les conditions d'exécution du marché l'exigeaient, par exemple en cas de revirement de l'éditeur sur sa politique technique ou commerciale. Néanmoins, le prix de l'indépendance – qui se traduirait par la capacité à changer de solution – est élevé.

2.3.2.2 La capacité à renoncer à un logiciel ou un éditeur, gage de souveraineté

2.3.2.2.1 Le cas d'un logiciel d'analyse de données et d'aide à la décision

La nécessité de se séparer d'un éditeur a été éprouvée dans le cas de logiciels propriétaires d'analyses de données et d'aide à la décision, utilisés dans de nombreux services de l'État. Fin 2022, un éditeur historiquement présent a souhaité imposer des conditions drastiques de renégociation des marchés portant sur les licences annuelles du produit.

Depuis 2017, afin de limiter sa dépendance et maîtriser les coûts, la DGFiP avait engagé une trajectoire de sortie de ces produits propriétaires, au profit de solutions sous logiciel libre. La position de la société, fin 2022, et la perspective de la fin du marché de support l'ont conduite à programmer cette sortie à l'horizon de fin 2025, et à la prioriser en conséquence.

La solution avait été mise en œuvre au sein de la direction générale selon des modalités différenciées suivant les structures et leurs besoins. Aussi, la DGFiP a-t-elle porté un programme de sortie et apporté un soutien, informatique et métier, aux projets concernés pour les accompagner dans la définition et la trajectoire de leur solution cible de sortie. La démarche engagée visant à sortir de cet écosystème captif a été de concevoir une solution cible plus modulaire, maîtrisée autant que possible en interne, et garantissant également des traitements des données conformes au RGPD, en s'appuyant notamment sur des logiciels libres et un *data lake*, ou lac de données[61], développé par la DGFiP.

Le coût complet d'installation de la solution cible – dont les usages d'analyse de données et d'aide à la décision ne représenteront qu'une partie – est évalué par la DGFiP à 16 M€ avec un coût d'exploitation de 1 M€ par an. En contrepartie, elle n'aura plus à supporter le coût de la solution propriétaire, d'un montant de 4,1 M€ en 2025, incluant le prix des licences qui a augmenté de 46 % en deux ans.

À la suite de l'Insee, qui avait ouvert la voie, la sortie du logiciel a également été engagée depuis quelques années par la direction de la recherche, des études, de l'évaluation et

[61] C'est-à-dire un référentiel centralisé qui permet de stocker de vastes quantités de données brutes, dans leur format d'origine, sans schéma prédéfini et pour un coût souvent moins important.

des statistiques (Drees) du ministère des affaires sociales. Cette migration vers des outils développés sous le logiciel libre R représente un enjeu stratégique pour la direction. Même si cela suppose un changement profond d'habitudes de travail pour ses agents, la Drees indique qu'elle est très bien avancée, avec la bascule, mi-2024, de deux-tiers des projets. Le terme de la migration est fixé à fin 2026.

Des licences propriétaires perpétuelles avaient été achetées par la Drees en 2024, bénéficiant d'une offre commerciale avantageuse pour ce type de licences. Ce choix permet à la direction de sécuriser la finalisation de la migration. En outre, avoir la possibilité de rejouer des programmes anciens non migrés pour répondre à des demandes d'actualisation sur données récentes d'études conduites dans le passé reste utile.

Ainsi, même sur des applications propriétaires, pour lesquelles un éditeur est en position de force, les administrations publiques peuvent reprendre la main lorsque les modalités d'utilisation des logiciels deviennent défavorables. Une telle migration s'effectue sur plusieurs années, requiert un profond changement d'habitudes de travail et n'est pas toujours aisée.

2.3.2.2.2 Le cas du logiciel de virtualisation VMware

L'exemple des logiciels développés par la société VMware est à cet égard significatif et a perturbé plusieurs administrations publiques. VMware est une entreprise qui a développé des logiciels dits « de virtualisation », essentiels aux infrastructures informatiques de nombreuses entreprises. Ces logiciels permettent de diviser les éléments matériels d'un seul ordinateur (processeurs, mémoire, stockage, etc.) en plusieurs machines virtuelles. Chacune de ces machines se comporte comme s'il s'agissait d'une machine physique indépendante, ce qui permet notamment une meilleure utilisation des ressources et facilite leur allocation dynamique aux différentes applications. Même s'il ne constitue pas un logiciel métier en tant que tel, VMware est un élément central des infrastructures techniques de plusieurs ministères.

Broadcom, nouveau propriétaire de VMware depuis décembre 2023, a décidé de changer radicalement de politique commerciale, en passant de 168 types de licences différentes à deux et de mettre fin aux licences perpétuelles. Pour certains clients, ce changement de politique commerciale a pu se traduire par une multiplication des prix des licences allant jusqu'à un facteur sept. Pour l'AIFE, le coût total projeté en 2024 pour la reconduction d'un marché triennal VMware aboutissait à une hausse de plus de 35 % du prix pour un périmètre fonctionnel en réduction.

Au ministère de l'éducation nationale, le marché de fournitures de licences et maintenance des logiciels VMware avait été notifié en novembre 2021 pour une durée maximum de quatre ans. Son renouvellement est donc attendu pour novembre 2025. Mais le ministère a également négocié, avec le titulaire du marché en 2023 et la société Broadcom, un accord promotionnel relatif à l'acquisition ou la location, la maintenance et le support de droits d'usages des solutions VMware pour une durée de trois ans pour l'ensemble de la sphère éducation / enseignement supérieur / recherche, aussi bien en administration centrale que déconcentrée. Cet accord représente une remise commerciale globale de 86 % par rapport aux prix du marché, qui présentait déjà des tarifs avantageux pour le secteur éducatif au regard des autres secteurs publics ou privés.

Les conditions ainsi obtenues, divisant par sept le coût des nouvelles licences, sont similaires à celles qui prévalaient avant le rachat de VMware par Broadcom. Saisie par les

administrations sur cette problématique, la Dinum a recommandé de ne pas précipiter une sortie de l'environnement VMware, soulignant que la valeur ajoutée des alternatives est limitée et suppose un effort de migration conséquent. Il s'agirait donc, dans un premier temps, d'optimiser l'usage fait de ces logiciels et négocier au mieux les prix. Selon la Dinum, c'est en assurant une migration vers certaines offres *cloud* que les administrations pourront s'affranchir de leur dépendance à VMware. Elle souligne, en effet, que les *clouds* internes interministériels (Nubo, Pi), l'infrastructure de la société Outscale ou la version SecNumCloud proposée par l'entreprise OVH ne reposent pas sur cette solution.

Contrairement aux logiciels d'analyse de données et d'aide à la décision pour lesquels les administrations ont pu engager une politique de décommissionnement, la situation vis-à-vis de VMware montre la difficulté à se défaire d'outils propriétaires lorsque les alternatives ne sont pas suffisamment répandues.

⁂

Alors que les enjeux de souveraineté numérique sont devenus majeurs pour l'État, la Dinum doit renforcer son rôle de pilote interministériel en définissant et déclinant une stratégie, dans les domaines matériels, logiciels et opérationnels. Cela permettra d'établir le montant des investissements nécessaires pour l'État, mais aussi les économies qui peuvent en résulter. Elle devra procéder à des audits réguliers de la correcte mise en œuvre de cette stratégie.

Recommandation n° 2. (Direction interministérielle du numérique) : À l'occasion de la révision de la feuille de route de la Dinum, intégrer une stratégie de souveraineté numérique qui définisse, notamment, les modalités de développement et d'exploitation des applications informatiques de l'État, et procéder à son chiffrage.

CONCLUSION INTERMÉDIAIRE

Pour l'État, être autonome sur l'ensemble de la chaîne de valeur numérique se révèle difficile, avec des défis complexes à relever.

S'agissant des matériels, la dépendance aux fournisseurs étrangers est notable. Faute de pouvoir atteindre une souveraineté dans ce domaine, les services de l'État concentrent leurs efforts sur la recherche d'un niveau de confiance élevé. Pour atténuer les risques inhérents à cette dépendance, les leviers de la commande publique sont mobilisés. La mutualisation des achats, l'utilisation des outils juridiques des marchés publics et la validation des matériels par l'Anssi constituent des mécanismes essentiels pour limiter les vulnérabilités.

Parallèlement, le RIE est une infrastructure clé et une réussite en termes de mutualisation et d'indépendance. Cependant, sa consolidation et le renforcement continu de sa résilience demeurent des impératifs pour garantir sa robustesse face aux menaces.

Par ailleurs, la maîtrise de l'identité numérique des citoyens est une problématique centrale de sécurité et de souveraineté qui a justifié la création de FranceConnect. Son pilotage doit toutefois être ajusté pour réduire la dépendance vis-à-vis des prestataires et inclure la réalisation de contrôles déontologiques. La sécurité du dispositif, insuffisamment anticipée, a dû être durcie pour contrer des fraudes massives. Bien que les dépenses directes apparaissent soutenables, le coût complet du dispositif s'avère significativement supérieur.

Enfin, les évolutions technologiques et les stratégies commerciales parfois changeantes des éditeurs amplifient les enjeux de souveraineté concernant les logiciels de l'État, qu'il s'agisse des outils bureautiques ou des applications métier. Pour les suites bureautiques, le caractère souverain n'a longtemps pas été garanti, avec désormais l'enjeu majeur de la migration vers le cloud. La souveraineté des applications métier passe par une maîtrise plus affirmée des logiciels et de leur exploitation, avec un arbitrage entre développement sur mesure et recours aux solutions du marché, dont il faut le cas échéant être en mesure de se défaire.

---

3 UNE PRIORITÉ MISE SUR LA MAÎTRISE DES DONNÉES AU DÉFI DE LA RÉALITÉ DES USAGES ET DU MARCHÉ

Bien que la maîtrise des données soit devenue une priorité politique majeure, notamment incarnée par la doctrine « Cloud au centre », sa traduction concrète rencontre des difficultés. L'adoption de l'informatique en nuage souveraine par les administrations reste limitée (3.1), les *clouds* internes de l'État peinent à atteindre une échelle suffisante (3.2) et la conciliation entre les exigences de souveraineté et les impératifs de performance s'avère complexe (3.3).

3.1 Un usage de l'informatique en nuage qui tarde à se développer

L'enjeu de souveraineté a pris une nouvelle dimension avec le développement de l'informatique en nuage (*cloud computing*) qui constitue un nouveau mode de fonctionnement des systèmes d'information. Il diffère du modèle d'informatique traditionnel qui consiste à héberger et traiter les données sur des serveurs locaux (cf. Annexe n° 1). Il est fondé sur des serveurs externes et basé sur des techniques de virtualisation qui permettent de distribuer à la demande des ressources numériques et de ne facturer que leur utilisation effective.

Le recours à l'informatique en nuage entraîne une dépendance accrue vis-à-vis du fournisseur. Il fait peser un risque sur les données dans la mesure où celles-ci sont stockées sur des serveurs distants, parfois opérés depuis l'étranger ou par un tiers étranger.

Pour cette raison, l'État s'est doté à la fin des années 2010 d'une doctrine pour encadrer l'usage de l'informatique en nuage par ses services et ses opérateurs, dont la mise en œuvre a nécessité de l'ajuster à plusieurs reprises (3.1.1). Elle encourage notamment l'hébergement des données sensibles sur les *clouds* commerciaux qualifiés SecNumCloud, mais ceux-ci sont encore peu nombreux (3.1.2). À cet égard, après plus de cinq ans, la doctrine de l'État a eu un effet réel, mais néanmoins modeste, sur le secteur français de l'informatique en nuage (3.1.3).

3.1.1 Une doctrine *cloud* récente, mais déjà révisée à plusieurs reprises

3.1.1.1 La doctrine de 2018

La première doctrine en matière de *cloud* visait notamment à tirer les conséquences pour les services de l'État de la situation, alors peu satisfaisante, de l'offre de *cloud* française. En effet, le projet de « *cloud* souverain », porté par les pouvoirs publics à partir de 2011 dans le cadre d'un investissement de 150 M€, s'est soldé par un échec en 2017. Ce projet dit « Andromède » visait la création d'une plateforme souveraine, garantissant un stockage des données sur le territoire national. Il a débouché sur la création de deux sociétés, Cloudwatt et Numergy, soutenues par l'État, mais qui n'ont jamais réussi à atteindre leurs ambitions sur les plans technologique et financier. Les participations de l'État ont été définitivement soldées en janvier 2017, ce qui s'est traduit pour ce dernier par une perte financière de 38 M€.

Par ailleurs, plusieurs opérateurs privés français de *clouds* ont émergé au cours de la décennie, sans toutefois pouvoir concurrencer les acteurs américains en termes d'offre de service. De même, les deux *clouds* internes à l'État (cf. *infra*) ne sont devenus opérationnels qu'à la fin des années 2010, pour n'offrir que des services limités (IaaS).

C'est dans ce contexte que le choix a été fait d'encadrer l'usage du *cloud* par les services de l'État. Ainsi, en novembre 2018, la circulaire n° 6049/SG du Premier ministre a formalisé des éléments de doctrine en la matière. Son objectif était d'en encourager l'utilisation du *cloud* au sein de 1'administration, tout en intégrant l'enjeu de souveraineté. La circulaire précisait que les données les plus sensibles devaient être hébergées dans les *clouds* internes de l'État (1er cercle), tandis que les autres données sensibles devaient être portées par une offre spécifique construite en partenariat avec l'État et proposée par un industriel (2e cercle). En revanche, les données « non sensibles » pouvaient être confiées à des prestataires de *cloud* commerciaux.

3.1.1.2 La doctrine « *Cloud au centre* » de 2021

En mai 2021, le Gouvernement lance une « Stratégie nationale pour le *cloud* » en deux volets. Le premier prévoit un soutien direct à des projets industriels dans le cadre du 4e programme d'investissements d'avenir et de France Relance, à hauteur de 1,8 Md€ (667 M€ de financement public, 680 M€ de cofinancements privés et 444 M€ de financements européens).

Le second volet met l'accent sur la notion de « *cloud* de confiance », qui se substitue à la notion de « *cloud* souverain » et ne vise plus une solution française, mais une solution permettant d'assurer une protection des données, à la fois au niveau technique (risque cyber) et au niveau juridique (risque d'application de lois extraterritoriales). Pour cela, la stratégie se fonde sur la qualification « SecNumCloud », créée en 2016 par l'Anssi, qui définit les exigences et bonnes pratiques en matière de management de la sécurité de l'information, et ajoute de nouvelles exigences additionnelles spécifiques aux acteurs *cloud*.

Déclinaison opérationnelle de la stratégie nationale, la doctrine dite « Cloud au centre », est établie par la circulaire du Premier ministre n° 6282-SG du 5 juillet 2021. Le *cloud* a vocation à devenir l'environnement par défaut de tout nouveau projet informatique. Chaque ministère doit identifier les obstacles à l'adoption du *cloud*, et élaborer un plan d'action. La bonne application de la doctrine est vérifiée par la Dinum à l'occasion des avis qu'elle rend préalablement au lancement des grands projets ou lorsqu'elle est amenée à les auditer.

Les règles en matière de protection des données et de souveraineté sont précisées : l'adoption du *cloud* ne doit pas *« entraver l'autonomie de prise de décision ni d'action de l'État, (sa) maîtrise des données et des traitements qui lui sont confiés, le respect des règles européennes en matière de protection des données à caractère personnel, et ce, alors que l'empreinte des acteurs extra-européens en matière de cloud est prédominante* ».

Les données « sensibles » de l'État doivent être hébergées sur ses *clouds* internes (cf. § 3.2) ou un *cloud* qualifié SecNumCloud (cf. 3.1.2) immunisé contre les réglementations extracommunautaires, les deux solutions étant jugées équivalentes. Le concept de « 2e cercle » de la circulaire de 2018 laisse place à la qualification SecNumCloud, les données « *non sensibles* » pouvant être hébergées sur un *cloud* commercial. La notion de « *données sensibles* » fait alors référence aux données personnelles des citoyens français, aux données économiques des entreprises françaises ou aux applications métiers relatives aux agents publics de l'État.

3.1.1.3 La réactualisation de la doctrine en 2023

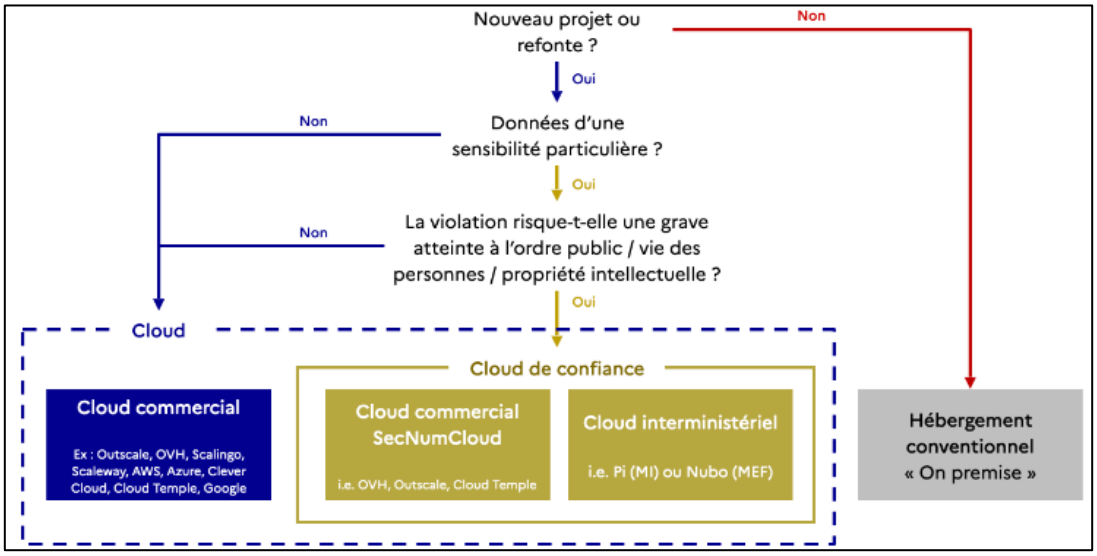
En septembre 2022, la « Stratégie nationale pour le *cloud* » fait l'objet d'une actualisation avec notamment un accompagnement des PME vers l'obtention de la qualification SecNumCloud et la création d'un Comité stratégique de filière « numérique de confiance » pour « *participer à l'émergence d'une offre française compétitive dans les prochaines années* ».

Dans ce contexte, la doctrine *cloud* de l'État est à nouveau mise à jour par la circulaire n° 6404/SG du 31 mai 2023 afin, notamment, de préciser la notion de « *données sensibles* » qui doivent relever de la qualification SecNumCloud. Selon la circulaire, elles recouvrent :

- les données qui relèvent de « *secrets protégés par la loi* », qui comprennent notamment les secrets liés aux délibérations du Gouvernement, à la défense nationale, à la sûreté de l'État, ainsi que le secret de la vie privée, le secret médical et le secret des affaires ;
- les données nécessaires à l'accomplissement des missions essentielles de l'État, notamment la sauvegarde de la sécurité nationale, le maintien de l'ordre public et la protection de la santé et de la vie des personnes

La circulaire ajoute la condition cumulative que leur violation soit *« susceptible d'engendrer une atteinte à l'ordre public, à la sécurité publique, à la santé et à la vie des personnes, ou à la protection de la propriété intellectuelle »* restreignant ainsi le champ des « données sensibles ».

Graphique n° 1 : arbre de décision en matière d'hébergement des données informatiques selon la doctrine « Cloud au centre »[62]



Source : Dinum

[62] Il est à noter que la circulaire « Cloud au centre » ne fait pas mention de « gravité » et requiert la qualification SecNumCloud pour toute donnée d'une sensibilité particulière, dont la violation est susceptible d'engendrer une atteinte à l'ordre public, à la vie des personnes ou à la propriété intellectuelle

Cette définition circonscrit la notion de données sensibles nécessitant un environnement qualifié SecNumCloud. L'objectif était de consolider la doctrine sur le plan juridique en limitant les risques de recours par des opérateurs étrangers au regard de l'Accord sur les marchés publics de l'OMC, qui pose un principe de non-discrimination, mais permet des exceptions au titre des mesures nécessaires à la protection « *de l'ordre public ou de la sécurité publique, à la protection de la santé et de la vie des personnes (…) ou à la protection de la propriété intellectuelle* ».

3.1.2 Une qualification SecNumCloud encore peu répandue

La stratégie nationale pour le *cloud* de 2021 a introduit le concept de *cloud* de confiance, qui repose sur les *clouds* interministériels de l'État (cf. *infra*) et les offres commerciales qualifiées SecNumCloud[63]. SecNumCloud est un référentiel[64] d'exigences techniques, opérationnelles et juridiques qui concerne les prestataires de services *cloud*. Cette qualification a été créée par l'Anssi pour garantir un niveau élevé de sécurité et de fiabilité pour les services de l'État, les opérateurs d'importance vitale (OIV) et les opérateurs de services essentiels (OSE), qui souhaiteraient héberger des données sensibles dans le *cloud*.

3.1.2.1 Un parcours de qualification rigoureux

SecNumCloud comporte 360 exigences distinctes à satisfaire regroupées dans quatorze domaines clés (gestion des risques, organisation de la sécurité, sécurité des ressources humaines, gestion des actifs, gestion des identités, cryptologie, etc.).

Un apport essentiel de la version 3.2 est l'accent mis sur la souveraineté (chapitre 19.6). Les exigences relatives à l'immunité aux lois non européennes, comme le Cloud Act ou le Fisa, y sont, en effet, explicitement renforcées : le siège social du prestataire doit être situé dans l'Union européenne ; une entité non européenne ne doit pas détenir à elle seule plus de 24 % du capital et des droits de vote du prestataire et, collectivement, plus de 39 % ; enfin la majorité des activités d'administration et de maintenance doivent être basées en Europe.

Ainsi, un prestataire ayant sa maison mère aux États-Unis, même si ses serveurs sont situés en France, ne pourrait pas obtenir la qualification SecNumCloud.

Le processus de qualification se déroule en quatre étapes. La première étape (Jalon 0) consiste en la soumission d'un dossier de candidature à l'Anssi, qui évalue l'éligibilité du prestataire. Si la candidature est validée, le prestataire apparaît sur la liste des entités en cours de qualification. La deuxième étape (Jalon 1) est la définition de la stratégie d'évaluation, en collaboration avec un prestataire d'audit de la sécurité des systèmes d'information accrédité par l'Anssi. Cette stratégie détaille le plan d'audit et les modalités de l'évaluation. La troisième étape (Jalon 2) est la réalisation de l'évaluation initiale, qui comprend des audits sur site pour vérifier la conformité aux exigences du référentiel. À l'issue de cet audit, un rapport est transmis

[63] SecNumCloud a évolué à partir du label « *Secure Cloud* » lancé par l'Anssi en 2014. La première version a été publiée en 2016 et la version actuelle, (3.2) a été publiée en mars 2022.

[64] ANSSI, *Prestataires de services d'informatique en nuage (SecNumCloud) – Référentiel d'exigences*, version 3.2 du 8 mars 2022.

à l'Anssi. Si des non-conformités sont identifiées, le prestataire doit mettre en place des mesures correctives. Enfin, la dernière étape (Jalon 3) est la décision de qualification par l'Anssi, sur la base du rapport d'évaluation. Si tous les critères sont remplis, l'Anssi délivre la qualification SecNumCloud, pour une durée maximale de trois ans, avec des audits de surveillance annuels.

3.1.2.2 Une offre encore limitée de services de *cloud* qualifiés SecNumCloud

En juillet 2025, seize services informatiques en nuage, pour l'essentiel de type IaaS et SaaS, opérés par neuf entreprises étaient qualifiés SecNumCloud, ainsi que le détaille le tableau suivant. Le coût et la complexité perçus comme élevés de la qualification (cf. *infra*) expliquent sans doute ce nombre relativement faible par rapport au marché *cloud* dans son ensemble.

Tableau n° 2 : liste des services ayant obtenu la qualification SecNumCloud (juillet 2025)

Service	Entreprise	Type	Date de début de qualification	Date de fin de qualification
IaaS Cloud On Demande	Outscale	IaaS	30 novembre 2023	30 novembre 2026
Hosted Private Cloud powered by VMware	OVHcloud	IaaS	28 décembre 2023	29 décembre 2026
Whaller Donjon SaaS	Whaller	SaaS	2 août 2024	2 août 2027
CegNumCloud Secured IaaS	Cegedim	IaaS	4 décembre 2024	4 décembre 2027
Oodrive Work, Oodrive Work Share, Oodrive Meet	Oodrive	SaaS	20 janvier 2025	25 janvier 2028
PaaS OpenShift IaaS Secure Temple	Cloud Temple	PaaS IaaS	30 mai 2025	30 mai 2028
Bare Metal Pod	OVHcloud	IaaS	24 mars 2025	24 mars 2028
Wordline Cloud Services	Worldline	IaaS	24 mars 2025	31 mars 2028
Pronote, Hyperplanning, EDT, Pronote Primaire	Index Éducation	SaaS	5 mai 2025	18 juin 2027
Cloud Avenue Eolas	Orange Business Services	IaaS	11 juillet 2025	11 juillet 2028

Source : Anssi

Au moins[65] douze autres services étaient en cours de qualification, dont les deux projets de *clouds* adossés à des technologies américaines : S3NS (développé par Thalès en association avec Google) et Bleu (initiative conjointe entre Orange et Capgemini avec Microsoft Azure).

[65] Seuls les projets de qualification que les prestataires concernés ont accepté de rendre publics sont mentionnés sur le site de l'ANSSI.

Compte tenu de l'exigence croissante de souveraineté de la part des pouvoirs publics et des entreprises, ces deux projets industriels ont été lancés en 2022 pour proposer des services de *cloud* hybrides. Tout en recourant à des technologies américaines éprouvées, ils offriraient des garanties en termes de souveraineté grâce aux montages techniques et juridiques qui les distinguent dans le paysage du *cloud* : portage par une société de droit français au capital exclusivement ou majoritairement détenu par le partenaire français, hébergement des données sur le territoire national et dans des centres de données distincts de ceux du partenaire américain.

Leur objectif est ainsi de proposer le niveau de services et de montée en charge des *datacenters* américains à grande échelle spécialisés dans la fourniture de grandes quantités de puissance de calcul et de capacité de stockage, dits *hyperscalers*, dans des conditions qui protègent les données de leurs clients de l'application de lois extraterritoriales.

L'éventuel surcoût – par rapport aux offres standards des *hyperscalers* – avec lequel ces solutions hybrides seront commercialisées, si elles parviennent à obtenir la qualification, n'est cependant pas encore connu avec précision.

3.1.2.3 Une qualification de haut niveau, onéreuse pour les fournisseurs et les clients

La qualification SecNumCloud vise à établir la confiance et la sécurité au sein de l'écosystème du *cloud* français. Incidemment, elle règle, selon la Dinum, *« le problème de la prolifération de dénominations "cloud souverain" qui n'apportaient pas de garanties satisfaisantes et brouillaient la lecture de l'offre commerciale »*.

Pour les administrations publiques, l'utilisation d'une solution qualifiée SecNumCloud, répond d'abord aux prescriptions de la doctrine « Cloud au centre » en matière d'hébergement et de protection des données sensibles.

Pour les fournisseurs de services informatiques en nuage, l'obtention de la qualification SecNumCloud démontre un engagement important en matière de sécurité, propice à instaurer la confiance des clients et des partenaires. La qualification permet surtout de se différencier de la concurrence et d'accéder à des marchés requérant une sécurité et une souveraineté élevées, tels que le secteur public, la défense et la santé.

Toutefois, l'obtention de la qualification SecNumCloud est un processus exigeant, nécessitant un effort et un investissement importants en termes de temps, de ressources et d'expertise, tout comme le maintien de la qualification exige un effort continu de la part des prestataires. Le coût des certifications, des mises à niveau d'infrastructure, du personnel spécialisé et du processus d'audit peut représenter une barrière pour les plus petits acteurs.

Selon certaines estimations, l'investissement pour obtenir la qualification SecNumCloud pourrait atteindre 1 à 2 M€ sur une période de 18 mois environ. Ce coût s'explique par la nécessité d'opérer, une mise à niveau technique, une refonte significative des politiques et procédures de sécurité, de produire une documentation détaillée et de mettre en œuvre des contrôles poussés. À cet égard, l'État a mis en place des dispositifs de soutien à l'obtention de la qualification SecNumCloud, notamment dans le cadre de France 2030[66].

[66] L'appel à projets « Accompagnement à la qualification SecNumCloud » opéré par Bpifrance a été lancé fin 2022 et a conduit à attribuer 3,6 M€ à une vingtaine de projets.

Ce coût se répercute nécessairement sur les tarifs des offres qualifiées SecNumCloud, qui subissent un surcoût par rapport aux offres non qualifiées d'un même prestataire estimé entre +25 % et +40 % selon les sources. Au surplus, le fait de recourir à des offres SecNumCloud peut, dans certains cas, conduire à se priver de services « *clés en main* » autrement disponibles et à devoir les développer soi-même, ce qui augmente encore le coût total.

Néanmoins, le surcoût lié à la sécurité accrue et à la souveraineté doit être mis en regard du coût et des dommages réputationnels qu'entraîne une violation de données, délibérée ou non. Il doit aussi être rapporté au coût de la dépendance à des fournisseurs étrangers en position dominante sur leur marché, susceptibles d'imposer des augmentations significatives de tarifs.

3.1.3 Un effet réel, mais modeste, de la doctrine « *Cloud au centre* »

Dans le bilan de la doctrine « Cloud au centre » dressé début 2025, la Dinum rappelle que la stratégie nationale du *cloud* de mai 2021 cherchait, dans son volet relatif à la consolidation industrielle dans ce secteur, à *« faire émerger un nombre très limité de champions afin qu'ils puissent acquérir une taille critique, à la fois parmi les acteurs commerciaux, mais aussi parmi les solutions de cloud internes à l'État »*. À cet égard, elle note que *« la doctrine cloud au centre contribue également à cet objectif en augmentant la commande publique et la capacité pour les industriels de se projeter et d'investir. »*.

La mesure de la dépense publique dans ce domaine est difficile à réaliser, pour des raisons de périmètre (les établissements publics de santé sont concernés, tout comme les universités, mais leurs choix individuels en matière de numérique ne sont pas centralisés) et de multiplication des centrales et des marchés qui supportent ces achats.

Dans le cas de l'État, le recours aux *clouds* commerciaux, SecNumCloud ou non, devrait se traduire par une diminution des achats d'infrastructures dans les centres informatiques. Pour le vérifier, la Dinum indique travailler à améliorer la mesure de ces dépenses en examinant l'empreinte liée aux datacenters (nombre, capacité, consommation d'énergie) et les achats d'équipements et de services *cloud*, sans certitude, selon elle, *« que toutes ces dépenses sont correctement identifiées dans Chorus »*, le progiciel budgétaire et comptable de l'État.

Cette difficulté à connaître précisément les dépenses numériques des services de l'État et à les consolider a conduit à des alertes régulières par le passé, encore dans la période récente :

- en 2020, la Cour constatait qu'il est *« difficile d'avancer des chiffres précis sur les dépenses informatiques de l'État et encore moins sur celles liées à la conduite des projets numériques »*[67] ;
- en 2021, une mission d'information de l'Assemblée nationale recommandait *« de créer un document de politique transversale dédié aux politiques numériques, afin d'unifier leur suivi et de consacrer encore davantage leur importance lors des débats au Parlement sur le projet de loi de finances annuelle »*[68] ;

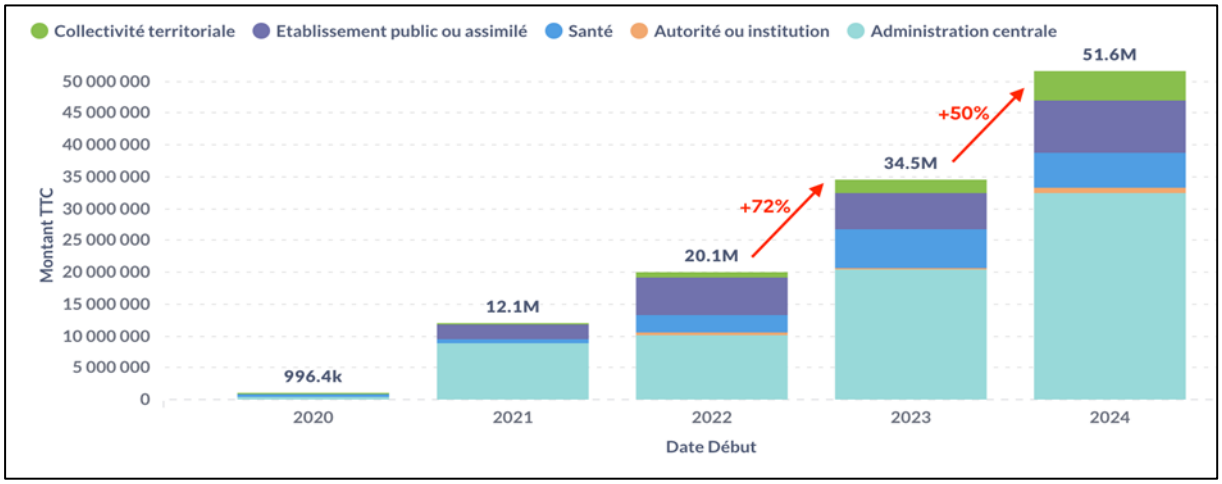
[67] Cour des comptes, *La conduite des grands projets numériques de l'État,* communication à la commission des finances du Sénat, juillet 2020, pages 35 et suivantes.

[68] Assemblée nationale, *Bâtir et promouvoir une souveraineté numérique nationale et européenne*, rapport d'information n° 4299, 29 juin 2021, page 134.

- en 2024, la Cour constatait que *« la constitution d'une vision consolidée de la dépense numérique de l'État apparaît un préalable indispensable au pilotage et à l'évaluation de sa stratégie numérique »*[69] et formulait une recommandation en ce sens.

Sous ces réserves qui conduisent sans doute à minorer les chiffres de la Dinum, la mise en œuvre de la doctrine « *Cloud au centre* » s'est traduite par une hausse de la commande publique, passant de 1 M€ en 2020 à 52 M€ en 2024, soit 120 M€ au total sur cette période répartis sur plus de 300 entités et 900 projets. Les seuls services de l'État ont commandé pour 32 M€ de services *cloud* en 2024, soit près des deux tiers de la commande publique totale.

Graphique n° 2 : évolution des commandes en matière de *cloud* par les administrations publiques



Source : Dinum ; l'administration centrale recouvre ici les services de l'État et certains de ses opérateurs

Sur cette période, l'enjeu de souveraineté semble avoir été bien pris en compte, puisque les fournisseurs français ont représenté 63 % de la commande publique, ainsi que l'illustre le graphique page suivante. La part restante, celle des fournisseurs américains, est nettement moins importante que leur part de marché au niveau national.

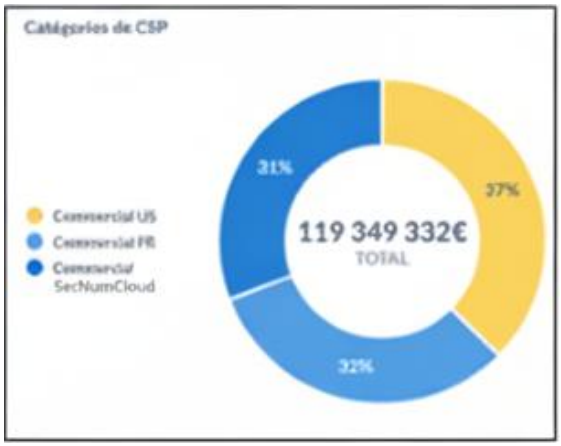
Près d'un tiers des offres retenues concernent l'hébergement SecNumCloud de services publics aussi variés que la dématérialisation de la démarche d'inscription sur les listes électorales (Diles), le SI-Samu, qui permet aux Samu de répondre à leurs missions de prise en charge des demandes de soins, ou encore le portail public de facturation.

Si la progression de la commande publique de l'État dans le *cloud* est encourageante, elle reste très modeste rapportée à ses dépenses informatiques annuelles, de l'ordre de 3 Md€[70].

[69] Cour des comptes, *Le pilotage de la transformation numérique de l'État par la direction interministérielle du numérique*, juillet 2024, page 88.

[70] Inspection générale des finances et Conseil général de l'économie de l'industrie, de l'énergie et des technologies, *Les ressources humaines de l'État dans le numérique*, janvier 2023, pages 11 et 12.

Graphique n° 3 : offres *cloud* retenues par catégories de fournisseurs entre 2020 et 2024 (en volume TTC de commande)



Source : Dinum

Ce constat peut s'expliquer par le caractère encore récent de la doctrine « *Cloud au centre* », qui ne s'applique qu'aux projets informatiques lancés après sa mise en place. Il s'explique aussi par le fait qu'une large part des systèmes d'information de l'État restent opérés sur des infrastructures traditionnelles. Dans son bilan de janvier 2025, la Dinum note que *« pour les grands projets de l'État, les manques de conformité à la doctrine portent toujours sur le fait de rester en hébergement conventionnel (on-premise), plutôt que d'aller dans le cloud »*.

Enfin, quoiqu'ils fassent l'objet d'une demande encore faible sur le plan interministériel, les *clouds* internes de l'État hébergent certaines de ses applications et données sensibles.

3.2 Des *clouds* internes de l'État à l'épreuve du passage à l'échelle

Le développement de *clouds* internes à l'État s'est inscrit dans un objectif de renforcement de la souveraineté de ses systèmes d'information. Issue de projets engagés il y a dix ans dans le cadre des programmes d'investissements d'avenir, leur mise en place a représenté une marche technologique difficile à franchir. Aujourd'hui, deux *clouds* sont gérés dans les centres de données de l'État, en s'appuyant sur des technologies et des architectures similaires (3.2.1). Bien que la Dinum encourage leur utilisation interministérielle, les applications hébergées restent principalement issues de leur ministère d'origine (3.2.2).

3.2.1 Deux *clouds* interministériels similaires sur lesquels l'État a peu investi

À la suite de la présentation du plan « *Investir pour la France* » en juillet 2013, la loi de finances pour 2014 a créé le programme « *Transition numérique de l'État et modernisation de l'action publique* » doté de 150 M€ de crédits pour financer des projets innovants, notamment ceux susceptibles de permettre la rationalisation et la mutualisation des infrastructures informatiques.

Le projet annuel de performances de la mission indiquait que *« le développement de nouveaux services numériques partagés et innovants passe par la mise en place de centres informatiques mutualisés et d'infrastructures banalisées de grande capacité dont l'État doit se doter. La mise en place d'infrastructures de ce type permet en outre une rationalisation des processus d'exploitation des systèmes d'information et une réduction des impacts écologiques des services numériques. Des crédits pourront ainsi être consacrés au cofinancement, aux côtés des administrations qui les portent, de projets de mutualisation et de rationalisation du parc de centres informatiques de l'État et à la mise en place d'un 'Cloud privatif' de l'État »*.

Dans ce contexte général, deux *clouds* internes ont été développés et mis en service :

- opéré par la DGFiP, le *cloud* « Nubo » a démarré en 2016 et a été mis en service mi-2018 ;
- le *cloud* « Pi » du ministère de l'intérieur a débuté en 2015 et est devenu pleinement opérationnel en 2017.

Dans les deux cas, l'offre de service est orientée IaaS, c'est-à-dire que les composants clés (ressources de calcul, de stockage et de réseau) sont fournis, mais qu'il n'est pas proposé d'environnement de développement (PaaS), ni de services de gestion logicielle (SaaS).

Nubo et Pi sont destinés à accueillir des services, données et traitements sensibles au sens de la doctrine. Pi peut, en outre, héberger des données faisant l'objet d'une diffusion restreinte (DR). Quoique n'étant pas formellement certifiés SecNumCloud, la doctrine « *Cloud* au centre » les met au même niveau que cette qualification en termes de sécurité. Sur le plan technique, les deux *clouds* présentent des capacités équivalentes, ainsi que l'illustre le tableau suivant. Nubo s'appuie sur des technologies libres, contrairement à Pi qui dépend en partie de Red Hat, société spécialisée dans l'*open source* rachetée en 2019 par IBM.

Tableau n° 3 : comparaison des caractéristiques techniques de Nubo et Pi (fin 2024)

	Nubo	Pi
Socle technique	OpenStack[71] (version libre) GNU/Linux (Debian)	OpenStack (version Red Hat) GNU/Linux (Debian, Ubuntu)
Caractéristiques physiques	346 To de mémoire 4 Po de stockage	328 To de mémoire 3,4 Po de stockage
Machines virtuelles	Près de 13 500	Près de 13 300
Espaces réservés[72]	Près de 2 000	Près de 1 800
Équipe technique	Près de 40 personnes	Près de 40 personnes

Source : Cour des comptes, à partir des informations communiquées par la DGFiP et la Dinum

Sur le plan opérationnel, les deux *clouds* se distinguent par leur support.

[71] Plateforme qui permet de créer et gérer des *clouds* à partir de pools de ressources virtuelles. Les outils qu'elle fournit assurent les principaux services d'informatique en nuage : calcul, mise en réseau, stockage, gestion des identités et des images.

[72] Ressources (machines virtuelles, bases de données, réseaux, etc.) allouées à une application spécifique, un environnement (développement, test, production), une équipe ou une initiative particulière.

Tableau n° 4 : comparaison des caractéristiques opérationnelles de Nubo et Pi (fin 2024)

	Nubo	Pi
Modèle de résilience	Deux sites en Île-de-France. Chaque site dispose de deux infrastructures indépendantes (l'une exposée au RIE, l'autre à Internet) comportant chacune deux zones de disponibilité	Deux sites en Île-de-France. Chaque site dispose de deux zones de sensibilité (usuelle et DR) et de trois zones de disponibilité
Disponibilité théorique minimum	98 % par site	98 % à 99,9% selon les composants (portail, API, etc.).
Niveau de support	8 h à 20 h, jours ouvrés (24 h sur 24, 7 jours sur 7 à compter de mi-2025)	24 h sur 24, 7 jours sur 7

Source : Cour des comptes, à partir des informations communiquées par la DGFiP et la Dinum

Les feuilles de route pour 2025 des deux *clouds* (cf. Annexe n° 3) prévoient des évolutions comparables visant à accroître leurs capacités et à enrichir leur offre de services.

Sur le plan financier, les dépenses d'investissement et de fonctionnement entre 2016 et 2024 pour Nubo se sont élevées à 55,8 M€ (dont 29,2 M€ en prestations, notamment pour l'exploitation en production), financées aux trois quarts par les crédits de la DGFiP[73]. Depuis 2022, ces dépenses sont stables et s'établissent à environ 7,5 M€ par an. Dans le cas de Pi, les coûts sont d'un ordre de grandeur comparable. Dans les deux cas, il s'agit de dépenses d'un niveau modeste au regard du budget que l'État consacre chaque année à ses systèmes d'information et sans commune mesure avec les investissements observés dans le secteur privé (par exemple, pour la seule année 2024, OVHcloud a investi environ 350 M€ dans ses propres infrastructures).

3.2.2 Une utilisation interministérielle encore beaucoup trop faible

En juin 2021, la Dinum constatait que *« bâtir et maintenir des offres cloud performantes nécessite une masse critique de ressources humaines et financières. Disperser les énergies sur des offres multiples et non coordonnées dans plusieurs ministères ne peut que conduire à un échec à moyen terme, et la perte de toute chance pour l'État de conserver un socle d'hébergement ayant un minimum de performance et de souveraineté. Le collectif du numérique de l'État a donc la responsabilité d'assurer une convergence des énergies compétentes dans le domaine, qui sont par ailleurs trop rares »*[74].

À ce titre, seules deux offres de *cloud* interne devaient être conservées, Nubo et Pi, et faire l'objet de ces efforts communs. En contrepartie, la mise en commun de plusieurs volets des deux *clouds* devait être recherchée, tout comme une plus grande attractivité *« pour les ministères clients (attention aux besoins, facilité de consommation, service de qualité) afin de développer leur volume d'usage et donc leur rentabilité pour l'État »*. Enfin, les

[73] Le reste provient de financements interministériels (9 M€ environ au total) et de redevances des autres services de l'État en qualité d'utilisateurs (de l'ordre de 1,2 M€ par an).

[74] Dinum, *Note « Mise en œuvre de la doctrine Cloud au centre »*, Cosinum, 3 juin 2021.

investissements d'équipes techniques d'autres ministères dans un *cloud* interne restaient possibles, *« à la condition stricte que ces investissements servent uniquement à enrichir l'une ou l'autre des offres Pi et Nubo »*.

Près de quatre ans après, ces impératifs n'ont pas été satisfaits : si la taille des deux *clouds* a progressé, c'est pour l'essentiel en raison de la consommation qu'en font leurs ministères d'origine. Les autres ministères préfèrent toujours conserver ou développer leurs propres infrastructures, dans un contexte où la tarification interministérielle de l'usage de Nubo et Pi est dissuasive et où les services qu'ils offrent doivent encore s'améliorer.

3.2.2.1 Des *clouds* interministériels essentiellement utilisés par leurs promoteurs

Dans son bilan de janvier 2025 de la doctrine « *Cloud* au centre », la Dinum relève que *« la part d'interministériel pour les clouds Pi et Nubo plafonne à 5 % »*.

Alors même que le nombre de projets hébergé a été multiplié par quatre en cinq ans, Nubo reste aujourd'hui utilisé à plus de 90 % par la DGFiP pour les besoins de ses applications métiers, le reste se partageant entre des services du ministère des finances et d'autres ministères (Dinum, direction générale de l'administration et de la fonction publique, ministère de la culture). De même, Pi est essentiellement utilisé par les services du ministère de l'intérieur et, subsidiairement, par quelques autres (notamment le ministère des affaires étrangères pour ce qui concerne France Visas).

Bien que, dans le cadre de la doctrine « *Cloud au centre* », les *clouds* interministériels concernent aussi bien les services de l'État que les organismes placés sous sa tutelle, ces derniers n'y recourent pas. En effet, si la fourniture des services de Nubo et Pi à d'autres personnes morales de droit public est possible sur le plan juridique, l'exercice par l'État d'une activité économique sur un marché concurrentiel, tel que celui du *cloud*, doit se faire dans le respect des règles de la concurrence et de la procédure des marchés publics (sauf dans le cas où les services seraient fournis à titre gratuit).

Dès lors, il n'est pas apparu possible à la DGFiP de contractualiser directement avec d'autres personnes morales publiques éventuellement intéressées, telles que la plateforme des données de santé dans le cadre de l'anticipation de sa migration. Le cas échéant, ces dernières devraient lancer un appel d'offres et il reviendrait à la DGFiP d'y répondre.

3.2.2.2 Des ministères qui préfèrent conserver ou développer leurs propres infrastructures

Si Nubo et Pi sont présentés comme des *clouds* interministériels, leur gouvernance et leur pilotage ainsi que la définition de leur feuille de route restent à la main de leurs promoteurs. La Dinum réunit trimestriellement les référents *clouds* des ministères pour présenter et promouvoir l'usage de Nubo et Pi, mais ce ne sont pas des réunions décisionnelles.

Dans le bilan précité, la Dinum note que *« les ministères […] disposant de moyens plus importants, et donc de plus d'inertie, prennent tous le premier virage (principe de développement cloud-native), mais ne peuvent ou ne veulent pas dépendre d'autres ministères et développent chacun leur propre cloud interne. Or, faire un cloud n'est pas à la portée d'un ministère individuellement, quelle que soit sa taille »*.

Par le passé, certains ministères ont, en effet, lancé des projets de *clouds* interministériels, qui n'ont pas abouti. En particulier :

- le projet « Oshimae » du ministère de l'agriculture se voulait une plateforme interministérielle proposant des offres de services d'hébergement et d'infrastructures à la demande ;
- le programme « Alpha » visait à faire migrer vers le cloud l'infrastructure socle du ministère de la justice, dont les lacunes en termes de performances et de cybersécurité étaient devenues un frein à sa transformation numérique.

Interrogés sur leurs cibles d'hébergement à cinq ans, les ministères ont confirmé lors du Cinum d'avril 2024 leur absence d'intérêt pour les *clouds* interministériels, à l'exception du ministère de la culture (cible de 5 %) et du ministère des affaires sociales (cible de 30 %). La DGFiP elle-même se fixe un objectif d'hébergement sur Nubo de 30 % seulement à horizon 2027, privilégiant l'hébergement dans ses centres de données conventionnels pour ses applications métier.

Tableau n° 5 : état de la mise en œuvre de la doctrine dans les ministères (janvier 2025)

Politique d'hébergement	Périmètre ministériel	Doctrine « Cloud au centre »		Autres clouds et infrastructures assimilés
		Clouds interministériels	Clouds commerciaux	
Alignée totalement ou partiellement avec la doctrine	Affaires étrangères	Pi (France Visas)	Non	Non
	Culture	Nubo	Oui	Non
	Économie et finances	Nubo (principal utilisateur)	Oui (1er utilisateur de clouds commerciaux)	Part très élevée d'hébergement sur site
	Intérieur	Pi (principal utilisateur)	nd	Non
	Justice	Réflexion en cours pour utiliser Pi	Non	Non
	Services du Premier ministre	Nubo et Pi	Oui	Non
	Travail, santé, solidarités et familles	Non	Oui	Non
Non alignée avec la doctrine	Agriculture	Non	Oui	Oshimae
	Éducation nationale et recherche	Non	Oui	Cloé
	Transition écologique	Non	Non	Éco

Source : Cour des comptes, à partir des informations transmises par la Dinum

Si les ministères ont bien intégré les enjeux de transformation associés à l'adoption du *cloud* en tant que modèle de production de services numériques, la Dinum constate qu'ils ne

sont pas tous alignés sur la doctrine « *Cloud au centre* », relevant par ailleurs que *« les moyens de mesure font défaut pour connaître avec précision les orientations prises par les administrations dans le champ d'application de la doctrine cloud, sachant que les administrations sont en l'état libres de leurs engagements »*.

La mise en place de la doctrine supposait que les ministères n'investissent plus dans leurs hébergements conventionnels, en dehors de ceux qui hébergent des systèmes d'information anciens, souvent affectés d'une obsolescence technique et fonctionnelle qui oblige à les conserver sur site.

Cet objectif a été seulement en partie atteint, puisque, selon la Dinum, une vingtaine de datacenters de l'État ont été fermés entre 2017 et 2023, pour s'établir à un peu moins de quatre-vingts[75]. Toutefois, trois ministères poursuivent le développement d'infrastructures d'hébergement et de développement qui offrent des services assimilables pour leurs utilisateurs à ceux d'un *cloud* :

- le ministère de l'agriculture et de la souveraineté alimentaire dispose d'une plateforme interne d'hébergement issue du projet Oshimae et située à Auzeville-Tolosane (Haute-Garonne), qui offre des services IaaS et CaaS à l'aide de la solution OpenStack ;
- le ministère de l'éducation nationale opère la plateforme Cloé, qui fournit des services IaaS, PaaS et CaaS (cf. encadré page suivante) ;
- le ministère chargé de la transition écologique développe une plateforme de type PaaS dénommée Éco, située à la Défense et gérée dans OpenStack Wallaby.

La plateforme Cloé du ministère de l'éducation nationale

En 2018, la direction du numérique pour l'éducation (DNE) a mis en place une plateforme dénommée Cloé afin de transformer le modèle d'hébergement pour le développement des applications nationales du ministère.

En s'appuyant sur les technologies des éditeurs VMware et Rancher Labs, elle fournit aujourd'hui des services IaaS, PaaS et CaaS aux équipes projet et leur permet de préfigurer le déploiement et le fonctionnement de leurs applications sur la plateforme d'hébergement mutualisée (PHM), qui porte les systèmes d'information nationaux du ministère (160 applications fin 2024). Cette évolution a permis, selon la DNE, de réduire les délais, sécuriser les développements pour le compte des académies et diminuer les investissements d'infrastructures.

La plateforme Cloé est maintenue par une équipe technique du ministère (3 ETP) et hébergée dans le centre informatique des douanes situé en région parisienne. En mars 2025, Cloé comptait 4 400 machines virtuelles, 1,2 Po de stockage, 53 To de mémoire (soit 30 % environ des capacités de Nubo dans les deux premiers cas, et 15 % dans le dernier). Au total, entre 2017 et 2024, les dépenses (matérielles, logicielles, prestations) consacrées au développement et à l'exploitation de cette plateforme se sont élevées à 10 M€.

[75] Ce mouvement a cependant été lancé bien avant la définition de la doctrine, puisqu'une soixantaine de sites avaient déjà été fermés entre 2012 et 2017.

3.2.2.3 Une tarification interministérielle dissuasive

L'utilisation des *clouds* interministériels de l'État se fait selon un mode de facturation à l'usage et une tarification convenue en 2017 avec la Dinum. Cette tarification a été établie pour prendre en compte l'ensemble des éléments de coûts, tels que les acquisitions de matériels, le coût d'exploitation et de support, le coût de l'hébergement et de l'énergie, etc.

Cependant, selon les estimations disponibles, elle conduirait à une facturation nettement supérieure au coût de revient d'un *cloud* comme Nubo, que la DGFiP estime « rentable » à partir de 10 000 environnements virtuels (« point mort » désormais dépassé). Ainsi, pour 12 000 machines virtuelles, la facturation aux tarifs actuels serait supérieure de 75 % au coût matériel et humain de leur exploitation. Pour 60 000 machines virtuelles, la facturation interministérielle représenterait un facteur multiplicatif de 5,4 par rapport au coût de revient.

Bien que la comparaison soit rendue difficile du fait de la grande diversité des offres et de la complexité des grilles tarifaires, et bien que les qualités de service ne soient pas identiques, le tarif actuel pour utiliser Nubo serait inférieur à celui d'une offre commerciale équivalente qualifiée SecNumCloud. Dans le cas de Pi, le tarif pratiqué serait légèrement inférieur à celui d'une offre techniquement comparable d'un prestataire privé, mais plus élevé, là encore, que son coût de revient.

Pour accroître l'attractivité auprès des administrations des *clouds* interministériels de l'État, il apparaît donc indispensable que leur tarification soit fixée à un niveau qui corresponde mieux à la réalité des coûts supportés par leurs promoteurs.

3.2.2.4 Une offre de services qui doit impérativement progresser

Au-delà du souhait des ministères de conserver le contrôle de leurs infrastructures et d'une tarification interministérielle excessive, plusieurs raisons sont susceptibles d'expliquer l'utilisation encore marginale que fait la communauté interministérielle de Nubo et Pi.

En premier lieu, tous les usages ne requièrent pas ou ne se prêtent pas à l'informatique en nuage. Une part significative des systèmes d'information est ancienne et n'a pas vocation à migrer sur le *cloud* à brève échéance. Dans d'autres cas, les bénéfices d'une telle migration, à supposer qu'elle soit réalisable, ne s'imposent pas de manière évidente.

Par exemple, le progiciel de gestion intégré Chorus (SAP S4/Hana), au cœur des processus budgétaires et comptables de l'État, est hébergé sur site, car il nécessite d'être installé sur des serveurs spécifiques certifiés par SAP dont Nubo n'est pas équipé. Ce n'est cependant pas davantage le cas des *clouds* commerciaux. En effet, à la Dinum, qui recommandait de *« mener sans tarder une réflexion en faveur de la cloudification de Chorus à long terme »*, l'AIFE soulignait qu'*« il n'existe toujours pas d'offre Cloud qui respecte à la fois nos exigences de sécurité (SecNumCloud), les exigences de certification par SAP des matériels pouvant supporter S/4HANA et les exigences techniques de Chorus liées à la taille de sa base HANA »*. Au surplus, les *clouds* qualifiés SecNumCloud ne peuvent pas encore se connecter au réseau interministériel de l'État, qui est le seul accès possible à Chorus.

Par ailleurs, Nubo et Pi ont été avant tout bâtis pour les besoins spécifiques de la DGFiP et du ministère de l'intérieur, qui conservent des données particulièrement sensibles, notamment dans le domaine fiscal et de la sécurité intérieure. Dès lors, leur utilisation peut

nécessiter des adaptations contraignantes. Ainsi, la messagerie Tchap, qui était initialement hébergée chez Cloudwatt (Orange), n'a pu être migrée sur Pi qu'après avoir satisfait des exigences de sécurité supplémentaires qui ne seraient pas nécessairement imposées autrement.

En outre, les *clouds* interministériels offrent une gamme de services comparable à celle des *clouds* commerciaux qualifiés SecNumCloud, du type IaaS, mais pas des autres *clouds*, en particulier ceux des *hyperscalers* qui dominent le marché. Or, pour les ministères, il n'y a pas de gains significatifs d'un passage sur un *cloud* interne qui n'offre pas des services managés (bases de données, orchestration de conteneurs, *monitoring*, etc.), mais des investissements supplémentaires à réaliser. De la même manière, les deux *clouds* interministériels commencent à peine à proposer l'utilisation de cartes graphiques de dernière génération, pourtant essentielles pour permettre le développement de services innovants faisant appel à l'intelligence artificielle.

Par comparaison, la plateforme Cloé fournit, selon le MEN, des services de type PaaS aux équipes projets leur permettant de disposer d'environnements de développement avec des composants préinstallés, ce qui garantit leur conformité et leur cohérence, et facilite la mise en production, le moment venu. Le bail associé à ces environnements, d'une durée d'un jour à trois mois, assurerait en outre une forte rationalisation des infrastructures et des gains énergétiques. Enfin, le niveau d'intégration et d'automatisation des services de la plateforme offrirait aux équipes un niveau d'agilité et d'autonomie que Nubo n'est pas encore en mesure de proposer.

Depuis septembre 2024, la Dinum et la DGFiP travaillent à faire évoluer ce dernier afin qu'il propose de la « conteneurisation »[76] (CaaS) ainsi qu'un niveau d'automatisation supérieur.

⁂

L'ensemble de ces constats dépeint une situation qui n'est pas satisfaisante, pour des *clouds* dits interministériels entrés en service depuis la fin des années 2010. Il est désormais indispensable de progresser, au minimum en engageant leur convergence, avec une tarification mieux corrélée au coût de ces infrastructures. En septembre 2025, une mission a été confiée par le Gouvernement à l'inspection générale des finances et au conseil général de l'économie afin d'évaluer l'adéquation de l'offre d'hébergement actuelle face aux besoins des ministères et explorer la piste d'un *cloud* interministériel.

Recommandation n° 3. (Direction interministérielle du numérique, Direction générale des finances publiques, Secrétariat général du ministère de l'intérieur) : Définir la trajectoire de convergence des *clouds* interministériels pour les rendre plus performants et augmenter significativement leur utilisation mutualisée par l'ensemble des ministères civils.

[76] Un conteneur est une unité logicielle complète (code, outils, bibliothèque) permettant d'exécuter de manière autonome une application.

3.3 Concilier les critères de souveraineté dans le *cloud* avec un niveau adapté de performance des systèmes d'information

L'application des critères de souveraineté définis par la doctrine « *Cloud* au centre » peut entrer en tension avec les ambitions de performance des systèmes d'information. Cette difficulté de conciliation est particulièrement prégnante pour certaines catégories de données sensibles, dont le traitement optimal pourrait nécessiter des solutions technologiques qui ne répondent pas toujours aux standards de souveraineté, qu'il s'agisse de données de l'État (3.3.1), des entreprises (3.3.2), des données de santé (3.3.3) ou de celles liées à l'exercice d'une politique publique, mais détenues par des opérateurs privés (3.3.4).

3.3.1 Une interprétation de la doctrine par le ministère de l'éducation nationale qui privilégie la performance au détriment de la souveraineté pour ses données RH

Bien que maniant des données sensibles, certains systèmes d'information gérés par l'État sont susceptibles de ne pas entrer dans les critères de souveraineté tels qu'actuellement définis par la loi. Le système d'information de gestion des ressources humaines (SIRH) du ministère de l'éducation nationale constitue en cela un exemple typique.

3.3.1.1 Recourir à un service *cloud* comme gage de performance

En 2018, le programme SIRHEN de gestion dématérialisée des ressources humaines de l'éducation nationale, engagé en 2007, a été abandonné après un investissement de 400 M€. Les projections initiales prévoyaient un développement en cinq ans pour un budget prévisionnel de 60 M€. Cet échec, après celui d'autres SIRH au sein de l'État, a témoigné de la grande difficulté que rencontrent les administrations publiques pour mener à bien de tels projets.

En octobre 2019, le comité d'orientation stratégique du MEN a arrêté une nouvelle trajectoire SIRH. Un service à compétence nationale, le service de modernisation des systèmes d'information des ressources humaines (SEMSIRH) est créé pour porter les projets de SIRH ministériels. Le comité choisit de ne plus systématiquement recourir à des développements informatiques internes et décide d'opter, au cas par cas, entre un développement spécifique, une solution logicielle interministérielle (comme l'application RenoiRH portée par le centre interministériel des ressources humaines), ou une solution commerciale du marché. La spécificité du MEN, déjà évoquée pour les enjeux liés aux messageries électroniques, est de gérer 1,2 million d'agents. Tous les systèmes d'information ne sont pas à même de traiter une telle masse d'information.

Le projet Virtuo est l'un des quatre projets majeurs de la nouvelle trajectoire SIRH du MEN, visant à la mise en place d'une solution de gestion RH qualitative, c'est-à-dire portant sur les six enjeux suivants : le recrutement et la mobilité interne ; la gestion de la formation ; la gestion des compétences ; l'évaluation ; la revue des agents ; la gestion prévisionnelle des emplois et gestion des compétences. Après analyse de ses besoins, le ministère a fait le choix

de s'appuyer pour cela sur une solution du marché, en mode SaaS (*Software as a Service*), qui puisse proposer ces différentes fonctionnalités de manière éprouvée et pleinement intégrée.

3.3.1.2 Un processus d'appel d'offres percuté par la doctrine « *Cloud au centre* »

Le MEN a lancé début 2021 une première consultation pour sélectionner un prestataire susceptible de proposer ce service. Deux groupements ont répondu à cet appel d'offres. La procédure a toutefois été déclarée sans suite pour motif d'intérêt général : entre le lancement de la procédure et la possible notification du marché, la première circulaire « Cloud au centre » avait été diffusée par le Premier ministre, le 5 juillet 2021.

Virtuo avait vocation à manier des « *données personnelles des citoyens français* », qualifiées d'une « *sensibilité particulière* » par la circulaire de juillet 2021. Le ministère a pris acte que cette dernière impose le recours à une offre de *cloud* souveraine.

Une deuxième consultation a donc été lancée en novembre 2021. Le nouveau cahier des charges précisait que « *les prestations et l'hébergement des données doivent être réalisées dans le respect de la qualification SecNumCloud (ou une qualification européenne d'un niveau au moins équivalent). Toute transmission de données à des tiers, y compris au bénéfice d'entités établies hors de l'Union européenne, qui ne serait pas conforme à la réglementation en vigueur est formellement prohibée* ».

En réponse à cette nouvelle consultation, une des deux offres reçues a été rejetée sans être analysée, bien qu'elle se prévalût de la qualification SecNumCloud. Le motif de ce rejet était que son prix dépassait le montant maximum du marché.

Le choix du ministère s'est porté sur la seule offre considérée comme recevable, répondant aux exigences techniques et fonctionnelles du cahier des charges mais émanant d'un éditeur de logiciel américain et ne bénéficiant dès lors pas de la qualification SecNumCloud pourtant requise. En choisissant cette offre, le ministère est volontairement passé outre les avis négatifs de l'Anssi et de la CNIL, saisis en avril 2022. L'Anssi indiquait que les engagements du candidat ne pouvaient être considérés comme suffisants pour atteindre un niveau SecNumCloud notamment concernant les exigences de son chapitre 19.6 relatif à la protection vis-à-vis du droit extra-européen. La CNIL soulignait que les technologies de chiffrement ne garantissaient pas que les données soient rendues inaccessibles au prestataire d'hébergement.

En réponse à une demande de précision du ministère sur la protection vis-à-vis de réglementations extra-européennes, le groupement reconnaissait qu'il pouvait faire l'objet de demandes d'accès aux données clients, mais soulignait qu'elle en recevait relativement peu « *en raison de la nature de ses activités* ». Le groupement s'engageait à informer ses clients de ces demandes d'accès aux données, « *sauf si la loi l'interdit* ».

Par ailleurs, il indiquait que « *pour répondre à certains problèmes techniques ou de service, une équipe dédiée d'administrateurs de la base de données (basée hors Union européenne) peut, à l'occasion, nécessiter un accès à distance aux tables de la base de données sur lesquelles sont hébergées les données personnelles en suivant des contrôles d'accès et de surveillance stricts. Les opérations peuvent impliquer l'accès aux données brutes, sans contexte, contenues dans la base de données* ».

Si l'enjeu de souveraineté n'est pas pleinement couvert par le titulaire du marché, le MEN considère que les enjeux de cybersécurité sont mieux pris en compte avec l'infrastructure retenue qu'avec d'autres dispositifs. Il souligne notamment les aspects suivants :

- une architecture dimensionnée pour gérer la volumétrie cible du ministère de plus d'un million d'utilisateurs au niveau des performances, de la résilience, de l'extensibilité et de la disponibilité de la plateforme ;
- des certifications européennes C5 (Allemagne) et ENS (Esquema Nacional de Seguridad, Espagne) qui sont comparables au SecNumCloud pour les enjeux de cybersécurité, bien qu'elles ne garantissent pas une immunité aux lois extraterritoriales ;
- un chiffrement des données aux niveaux applicatifs renforcé par un module de sécurité complémentaire assurant une meilleure couverture du chiffrement dont les clés de chiffrement sont uniquement détenues par le ministère.

Outre ces exigences de cybersécurité, le ministère a choisi de privilégier l'amélioration de la performance de sa gestion des ressources humaines au respect des règles en matière de souveraineté, dont le risque pouvait paraître moins tangible.

Dans une note au directeur de cabinet du Ministre, la secrétaire générale du ministère soulignait que « *aucune autre offre d'un éditeur respectant les besoins du ministère et les exigences complètes SecNumCloud n'est disponible sur le marché. Seule une solution développée en interne 'sur mesure' permettrait de répondre aux besoins exprimés par les directions métiers, tout en gérant la volumétrie. Toutefois, cette solution qui consisterait à faire un projet d'une nature et d'une ampleur similaire à 'SIRHEN' sur le volet qualitatif de la GRH ne serait pas sans risques, tant sur les délais de réalisation (au minimum 4 à 5 ans) que sur le plan budgétaire (estimation d'une enveloppe 4 fois supérieure à une solution Saas pour la partie investissement)* ».

L'accord cadre du marché Virtuo a été notifié en décembre 2022. Les travaux ont été lancés en janvier 2023.

3.3.1.3 Le surcoût de la souveraineté estimé entre + 25 et + 40 %

Le coût prévisionnel du marché était de 13,6 M€ TTC, montant équivalent à celui porté par le même groupement lors de la première consultation. Au regard de la complexité des projets de SIRH que l'État a portés jusqu'ici, ce montant pouvait apparaître comme raisonnable.

Entre la première et la seconde consultation, le groupement n'a pas modifié l'architecture technique de sa proposition malgré l'ajout d'une demande de qualification SecNumCloud à laquelle il ne pouvait pas répondre.

L'autre groupement, dont la candidature n'a pas été examinée, avait renforcé les engagements en matière d'hébergement afin de se conformer à cette demande, en recourant à une infrastructure SecNumCloud. Le surcoût lié à cette nouvelle architecture ne peut pas se déduire aisément de l'offre financière, dont le prix résulte de nombreux paramètres. La société estime toutefois que l'impact brut de l'hébergement souverain est de +25 %. Mais le recours à une offre SecNumCloud suppose de mettre en place également des procédures d'installation et d'administration des plateformes. L'impact net d'une solution souveraine est évalué à +40 %.

Deux ans après la notification du marché, le ministère assure que la trajectoire financière du projet reste conforme à ce qu'il avait projeté. Le calendrier de déploiement de l'outil est organisé par module, avec une structure pilote avant une généralisation. Le premier module mis en place a été celui dédié au recrutement. Deux pilotes académiques (Versailles et Aix Marseille) ont démarré en novembre et décembre 2023. La généralisation à l'ensemble des académies s'est faite en avril et mai 2024. Ainsi, le paramétrage et le déploiement de ce module dans l'ensemble des académies ont été menés en 16 mois à compter du démarrage du projet.

Le MEN se montre satisfait du choix opéré, qui s'est traduit par une durée de déploiement et un coût bien inférieurs à ce que les projets de SIRH connaissent habituellement.

3.3.1.4 Une offre que le ministère estime avoir été régularisée *a posteriori* par l'évolution de la doctrine « *Cloud au centre* »

Lorsque le marché Virtuo a été notifié, l'obligation de recourir à un service qualifié SecNumCloud était inscrite dans la première circulaire du Premier ministre alors en vigueur et avait même justifié le lancement de cette seconde consultation. La notification du marché s'est avérée contraire à ce cadre réglementaire.

Depuis, les critères exigeant le recours au SecNumCloud ont été affinés dans la deuxième circulaire « Cloud au centre » du 31 mai 2023 et repris dans la loi SREN de mai 2024. Le recours à cette qualification est désormais requis si deux critères cumulatifs sont observés : que le système d'information traite de données d'une sensibilité particulière, mais aussi que leur violation soit « *susceptible d'engendrer une atteinte à l'ordre public, à la sécurité publique, à la santé ou à la vie des personnes ou à la protection de la propriété intellectuelle* ».

À cette aune, le MEN considère que les données traitées par Virtuo, bien que comportant des informations personnelles et confidentielles sur les enseignants, ne relèvent pas de cette obligation. L'analyse des risques réalisée par le MEN - formalisée dans le cadre du suivi des 50 principaux projets numériques de l'État par la Dinum - décrit les données comme « non sensibles » et ne mentionne aucun risque lié à une nécessaire application de critères de souveraineté. Ainsi, la seconde version de la circulaire « Cloud au centre » de mai 2023 aurait levé l'obligation de recours à une plateforme SecNumCloud qu'avait imposée celle de juillet 2021. Elle aurait donc, *a posteriori*, rendu Virtuo conforme à la réglementation. Ces mêmes critères, repris dans la loi SREN, permettent au MEN de considérer que le recours à la solution d'une entreprise américaine est conforme à la législation, alors même que la sensibilité des données traitées par Virtuo ne fait aucun doute.

Cette analyse n'engage toutefois que le MEN : en dehors des avis qu'elle rend au titre de la procédure de l'article 3[77], la Dinum laisse les ministères apprécier si une application nécessite de recourir - ou non - à une plateforme SecNumCloud et n'entend pas interférer avec leurs choix. Concernant le projet Virtuo, la Dinum n'avait été saisie au titre de l'article 3 par le MEN qu'en mars 2024. Constatant que cette saisine était postérieure au choix du prestataire et à une première vague de déploiement, la Dinum n'avait alors pas rendu d'avis.

[77] Article 3 du décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'État et à la direction interministérielle du numérique.

Le 22 avril 2025, trois ministres – chargés de l'action publique, des comptes publics et du numérique – ont adressé une note à l'ensemble des membres du Gouvernement rappelant la nécessité de se conformer aux dispositions de la loi SREN concernant le recours à un *cloud* souverain. Pour s'assurer de la pleine mise en œuvre des dispositions de la loi, ils donnent consigne aux contrôleurs budgétaires et comptables ministériels de refuser tout achat qui n'aurait pas reçu l'avis préalable de la Dinum au titre de l'article 3. Cela ne tranche toutefois pas la question de l'interprétation que peut faire un ministère d'être concerné, ou non, par le critère cumulatif édicté dans la loi.

3.3.2 Des données sensibles des entreprises à protéger, malgré le coût et les délais d'une migration vers une solution souveraine

3.3.2.1 Le portail public de facturation et la plateforme Piste

Le calendrier de généralisation de la facturation électronique interentreprises a été fixé au 1er septembre 2026 pour les grandes entreprises et les entreprises de taille intermédiaire, et au 1er septembre 2027 pour les petites et moyennes entreprises et les très petites entreprises[78]. Dès lors, toutes les entreprises assujetties à la TVA en France devront émettre, transmettre et recevoir des factures sous forme électronique et transmettre les données de facturation et de transaction à l'administration fiscale.

Dans ce cadre, l'AIFE a été chargée de la construction du portail public de facturation, s'inspirant de Chorus Pro, plateforme utilisée depuis 2020 pour la facturation électronique entre les entités publiques et leurs fournisseurs. Ce portail assure la fonction d'annuaire, permettant le routage des factures, et concentre la transmission des données de facturation et de transaction à l'administration fiscale. Il met également à la disposition des entreprises qui le souhaitent, en complément des plateformes de dématérialisation privées, un service minimum permettant l'émission ou la réception de leurs factures.

Le portail a été entièrement construit sur une infrastructure SecNumCloud. L'option de recourir au *cloud* interne Nubo a été étudiée par l'AIFE avec la DGFiP au démarrage du projet en 2022, mais le dimensionnement du portail et le niveau de disponibilité exigé n'étaient pas compatibles avec les caractéristiques de Nubo. Par un hébergement sur une plateforme SecNumCloud, la problématique de souveraineté numérique a, en tout état de cause, pleinement été prise en considération.

Le portail public de facturation est basé essentiellement sur des API, qui sont des interfaces de programmation permettant à deux applications distinctes de communiquer entre elles et d'échanger des données. L'AIFE a choisi de recourir à la plateforme d'intermédiation des services pour la transformation de l'État (Piste[79]) comme gestionnaire de ces API.

Avant le déploiement du portail public de facturation, Piste était installée sur les centres d'hébergement de Chorus, dans deux datacenters de l'administration. Toutefois, le niveau de

[78] Article 91 de la loi n° 2023-1322 du 29 décembre 2023 de finances pour 2024.

[79] Piste, lancée par l'AIFE en 2018, permet aux acteurs publics de partager des services API. 35 millions de requêtes y transitent en moyenne chaque jour.

service attendu par le portail public de facturation ne pouvait pas être atteint par ces infrastructures internes. Ces exigences ont conduit à basculer Piste sur une infrastructure *cloud*, labellisée SecNumCloud.

Cette bascule d'un hébergement interne à l'administration à des serveurs SecNumCloud permet par ailleurs de comparer le coût et les modalités de chaque solution.

Le passage sur un serveur SecNumCloud a représenté pour l'AIFE un surcoût d'exploitation et d'hébergement évalué à 2,3 M€ par an : de 0,52 M€[80] dans la configuration précédente à 2,85 M€ en SecNumCloud. Cet écart, modeste dans l'absolu, représente un facteur multiplicatif de 2,5 pour le volet d'hébergement, entre les centres de données de l'État et un environnement SecNumCloud du marché. Il faut toutefois noter que la comparaison ne porte ni sur le même niveau de performance, ni sur le même périmètre : le taux de disponibilité de Piste en hébergement SecNumCloud est de 99,9 % (versus 99 % précédemment) et sa capacité est deux fois supérieure. Du point de vue des effectifs, l'exploitation SecNumCloud ne mobilise plus que 0,7 ETP de la DGFiP contre 3,85[81] précédemment.

3.3.2.2 La protection des données de l'achat public

En octobre 2024, trente-trois députés ont adressé un courrier au ministre de l'économie et des finances alertant sur le choix qu'aurait fait l'administration du ministère de confier désormais à une société nord-américaine la gestion la plateforme Place, par laquelle transitent les appels d'offres de l'État. Visant une entreprise canadienne, ils soulignaient qu'une telle décision poserait « *une grave question de souveraineté voire de sécurité nationale* », soulignant que « *les informations qui circulent via cette plateforme sont parfois hautement sensibles* », les offres techniques et financières des entreprises y étant déposées.

Cette interpellation témoigne de la grande sensibilité du sujet de la souveraineté y compris pour des informations qui ne relèvent pas directement de l'État, mais du monde économique. Elle montre que cette préoccupation, désormais inscrite dans la loi, n'avait pas, jusqu'alors, guidé l'administration dans les choix opérés sur le devenir de l'application.

La plateforme Place est gérée par l'AIFE. Elle a été développée par une société française, liée à l'État par un marché de tierce maintenance applicative passé pour une durée de quatre ans, avec échéance fin 2024[82].

L'application est hébergée par une société française, dans un environnement *cloud* privé, qui n'est pas qualifié SecNumCloud. Parmi les autres prestataires intervenant sur cette application, une autre société française assure, depuis mai 2021, la tierce maintenance technique, c'est-à-dire la maintenance logicielle et du socle technique, ainsi que l'exploitation de Place.

Déposé au printemps 2024, le projet de loi sur la simplification de la vie économique prévoit, en son article 4, de faire obligation aux personnes publiques autres que les collectivités territoriales, d'utiliser un unique profil d'acheteur mis à leur disposition sur la plateforme Place. Cette mesure d'harmonisation vise à simplifier la gestion des appels d'offres pour les

[80] 9 % du coût total de l'exploitation et hébergement de Chorus, évalué à 5,8 M€ par an.
[81] 9 % des 42,5 ETP dédiés à Chorus.
[82] Ce marché a finalement été prolongé jusqu'à la fin mai 2025.

entreprises. Si elle était définitivement adoptée, elle supposerait de développer des interfaces entre Place et les systèmes d'information amont et aval des entités publiques tierces, et de procéder à un redimensionnement applicatif. Ainsi, le projet de loi ouvre la voie d'une nécessaire refonte de la plateforme Place, avec une échéance de mise en œuvre à la fin 2028.

Au printemps 2024, l'AIFE s'était inscrite dans la perspective d'un vote rapide du projet de loi, déposé selon la procédure accélérée, avant que la dissolution de l'Assemblée nationale n'en modifie le calendrier. Elle estimait que le besoin de prestations d'évolution de Place relevait d'un expert en dématérialisation et dépassait celui de prestations plus générales de maintenance préventive et corrective dans le domaine applicatif.

Afin d'anticiper la fin du marché et les nouvelles exigences portées par le projet de loi de simplification de la vie économique, l'AIFE s'est tournée vers le marché cadre « assistance à la dématérialisation » passé par l'Ugap, dont la filiale française d'un groupe canadien est titulaire. L'AIFE indique que le renouvellement des marchés de maintenance intervenant en 2028 pour ses autres systèmes d'information, le recours aux supports contractuels de l'Ugap a été privilégié pendant cette période intermédiaire.

L'objet de cette assistance est la future refonte de la plateforme. Pour assurer la continuité du service, cette filiale d'un groupe canadien est secondairement chargée de la maintenance applicative. C'est ce volet qui a suscité l'inquiétude des parlementaires : cette maintenance suppose un accès aux données sensibles, telles que la composition des groupements d'entreprises qui répondent à un appel d'offres. Que l'hébergement soit chez un opérateur français n'est donc pas un gage suffisant pour assurer que les informations ne soient pas accessibles par une entreprise dont le siège est basé hors de l'UE.

Néanmoins, l'AIFE assure que les accès de la filiale du groupe canadien se limitent aux données fictives des environnements dédiés aux développements et aux tests. Elle précise que si *« un accès aux données réelles de l'environnement de production lui était indispensable pour mener une investigation destinée à résoudre des dysfonctionnements, celui-ci ne serait autorisé que de manière temporaire, circonscrite et tracée, sur la base d'une demande argumentée, avec toutes les exigences de confidentialité qui s'imposent* ».

Par ailleurs, l'échéance de refonte de la plateforme Place étant fin 2028, le logiciel actuel continuera d'être utilisé pendant plus de trois ans. En complément d'une prestation d'assistance à la dématérialisation, l'AIFE aurait pu choisir de recourir à un autre support contractuel de l'Ugap de « tierce maintenance applicative », qui semblait mieux adapté à ce besoin et dont les titulaires sont, par ailleurs, des entreprises et groupes français. L'agence n'a pas souhaité recourir à deux supports différents de l'Ugap pour la transformation de la plateforme, son évolution et sa maintenance au regard des risques et des coûts de coordination induits. Bien que cela n'ait pas été initialement envisagé, l'AIFE indique toutefois qu'elle souscrira finalement à ce marché interministériel de maintenance à compter du mois de juin 2025. La maintenance sera donc opérée par une société française.

Enfin, bien que concernant des données considérées par la loi SREN comme sensibles et alors qu'il pourrait être considéré que leur violation est susceptible d'engendrer une atteinte à l'ordre public ou à la protection de la propriété intellectuelle, l'hébergement n'est pas assuré sur un système qualifié SecNumCloud. Même si la plateforme est hébergée dans une entreprise française qui n'est pas exposée à des lois extra-européennes, l'ensemble des critères de sécurité du SecNumCloud ne sont pas appliqués.

L'AIFE avait mené, en 2022, une étude portant sur la migration de l'hébergement de Place vers une plateforme SecNumCloud. Au-delà des surcoûts d'exploitation liés à un tel hébergement, une telle migration supposait de faire évoluer l'application et nécessitait un travail d'une vingtaine de mois et une prestation comprise entre 1 500 et 2 000 jours hommes.

L'AIFE indique qu'une telle migration vers un dispositif SecNumCloud sera mise à l'étude si la loi de simplification de la vie économique maintient la nécessité de refondre la solution. Au-delà d'une possible « mise à l'étude » – qui semble témoigner d'un certain détachement de l'AIFE vis-à-vis des exigences de souveraineté –, il conviendrait qu'une bascule vers un hébergement SecNumCloud soit formellement programmée.

⁂

À travers la dernière version de la doctrine « *Cloud au centre* » et la loi SREN, l'État a cherché à concilier une ambition en matière de souveraineté numérique et le respect d'un cadre européen encore incertain. Ce difficile équilibre a ouvert aux ministères une marge d'interprétation des exigences de souveraineté. Une doctrine interministérielle plus précise devrait être édictée par la Dinum et l'Anssi, en lien étroit avec les autorités qualifiées de la sécurité des systèmes d'information de chaque ministère, concernant les catégories de données et applications sensibles qui nécessiteraient d'être hébergées de manière souveraine.

Recommandation n° 4. (Direction interministérielle du numérique, Agence nationale de la sécurité des systèmes d'information) : Veiller à ce que chaque ministère cartographie en 2026 l'ensemble de ses données sensibles à héberger de manière souveraine.

3.3.3 Le choix d'un opérateur non souverain réputé pour sa performance qui a, paradoxalement, freiné le déploiement de la plateforme des données de santé

3.3.3.1 Les forts enjeux liés aux données de santé publiques

Les données de soins utilisées pour la rémunération des professionnels et des établissements de santé sont susceptibles de donner lieu à d'autres utilisations. Ce potentiel a notamment été mis en avant en juillet 2014 par le rapport de la commission *open data* en santé[83] qui a identifié trois intérêts majeurs à l'exploitation de ces données : alimenter le débat public en informations statistiques fiables ; améliorer l'efficience de la gestion du système de soins ; permettre aux chercheurs de mener des études sur l'impact de nouveaux médicaments ou dispositifs médicaux par des rapprochements ou recoupements d'informations.

Ce rapport a également souligné *« le consensus existant sur les impacts positifs d'une plus grande ouverture et d'une meilleure utilisation des différents types de données produites par le système de santé, qui permettent d'attendre de nombreux bénéfices en termes de*

[83] Lien : https://drees.solidarites-sante.gouv.fr/publications/rapports/rapport-de-la-commission-open-data-en-sante.

démocratie sanitaire, de renforcement de l'autonomie des patients, de développement de la recherche et de l'innovation, d'efficacité de l'action publique et d'amélioration des pratiques professionnelles. » tout en rappelant que « *La principale limite à cette ouverture étant la nécessité de garantir la protection de la vie privée des patients* ».

Pour trouver cet équilibre, ce rapport préconisait une approche à trois étages : un accès totalement libre (*open data*) pour les données strictement anonymes, c'est-à-dire à risque nul d'identification ; une procédure simplifiée (arrêté ministériel) validée par la Cnil pour les données présentant un très faible risque de réidentification du fait de la granularité limitée des informations ; enfin un canal unique d'autorisation délivrée par la Cnil pour les données détaillées, emportant de ce fait un risque plus important de réidentification.

Ce travail a nourri les débats qui ont abouti à la loi du 26 janvier 2016 de modernisation de notre système de santé qui a créé le système national des données de santé (SNDS).

En 2017, la Cour avait rappelé la contribution que pouvait apporter l'utilisation des données de masse en santé au pilotage et à l'amélioration de l'efficience du système de santé en identifiant des besoins non satisfaits et des marges de progrès[84]. Elle avait signalé l'enjeu du traitement des données massives en termes d'évaluation des thérapies et modèles de soins, de personnalisation des traitements, d'amélioration de veille sanitaire et de contribution à la recherche médicale.

3.3.3.2 Le système national des données de santé et ses limites

Créé par la loi précitée du 26 janvier 2016, le système national des données de santé (SNDS) est un ensemble de bases de données issues principalement des organismes publics et placé sous la co-responsabilité de la Cnam et de la plateforme des données de santé (PDS)[85].

Le SNDS comporte peu de données médicales. À titre d'exemple, seules des données d'activité liées aux séjours hospitaliers y figurent, mais pas celles provenant des soins ambulatoires. N'y figurent pas non plus des données telles que l'indice de masse corporelle, les habitudes en matière de consommation d'alcool ou de tabac. En cela, il se démarque de bases étrangères comme au Royaume-Uni ou au Danemark qui, moins complètes en termes de populations couvertes, comportent de telles données médicales. Une problématique du même ordre porte sur les données relatives à la situation économique ou sociale des personnes prises en charge par l'assurance maladie.

Pour alimenter davantage le SNDS en données médicales, la loi du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé prévoit son élargissement.[86]

Néanmoins, un écart important demeure entre la base principale telle que prévue par les textes et son contenu effectif. Malgré l'évolution du cadre légal, la base principale du SNDS

[84] Cour des comptes, *L'avenir de l'assurance maladie. Assurer l'efficience des dépenses, responsabiliser les acteurs*, novembre 2017.

[85] Également nommée *Health Data Hub*.

[86] Données destinées aux professionnels et organismes de santé recueillies à l'occasion des activités de prévention, de diagnostic, de soins ou de suivi social et médico-social ; données relatives à la perte d'autonomie ; données à caractère personnel des enquêtes dans le domaine de la santé, dès lors qu'elles sont appariées avec celles citées précédemment ; données recueillies lors des visites médicales et de dépistage en milieu scolaire

est toujours principalement composée des données médico-administratives originelles. Toute personne ou structure, publique ou privée, à but lucratif ou non lucratif, peut, depuis avril 2017, accéder aux données du SNDS sur autorisation de la Cnil, en vue de réaliser une étude, une recherche ou une évaluation présentant un intérêt public (cf. Annexe n° 4).

La complétude du SNDS en matière de données de santé et la capacité à les exploiter constituent un enjeu essentiel avec le développement de l'intelligence artificielle (IA). Ces nouvelles potentialités ont été mises en exergue dans un rapport de 2018[87] sur la base duquel une stratégie nationale pour l'IA a été adoptée. La mise à disposition de données, dûment structurées ou annotées, permet l'entraînement d'algorithmes pouvant faire émerger des corrélations qui pourront faire l'objet de recherches médicales.

D'autres freins juridiques, procéduraux et techniques limitent l'utilisation du SNDS par l'IA. Lever ces freins fait partie des attributions du comité stratégique des données de santé institué par un arrêté du 21 juin 2021. Constitué auprès du ministre de la santé, sa présidence est assurée par le directeur de la Drees et la vice-présidence par la directrice générale de la recherche et de l'innovation (DGRI).

3.3.3.3 La création d'une plateforme des données de santé dédiée à la recherche médicale

Parallèlement à l'élargissement des données contenues par le SNDS, le législateur a prévu, par la loi du 24 juillet 2019, la constitution d'un groupement d'intérêt public, la Plateforme des données de santé (PDS), également dénommée « *Health Data Hub* ». Son objet est de mettre à disposition des chercheurs et porteurs de projets d'étude, ainsi que du secteur privé, le vaste ensemble de données du SNDS à des fins de connaissance et d'innovation.

3.3.3.4 L'incapacité à répondre aux besoins en dépit d'une amélioration en cours

Alors que la législation de 2019 a confié à la PDS le soin de mettre les données issues du SNDS à la disposition des demandeurs lorsqu'ils ne disposent pas d'un accès permanent pour les obtenir, c'est dans les faits à la Cnam que cette tâche échoit encore largement en 2025. Le code de la santé publique[88] définit pourtant les missions respectives de la PDS et de la Cnam, désignés responsables conjoints du SNDS.

En dehors même de la question de la détention d'une copie de la base principale et du catalogue par la PDS, il apparaît que les responsabilités sont pour le moins imbriquées alors que l'ambition était de faciliter l'accès à ces données de santé en déchargeant la Cnam de cette mission spécifique qui n'entre pas dans son cœur de métier (la gestion du système de soins).

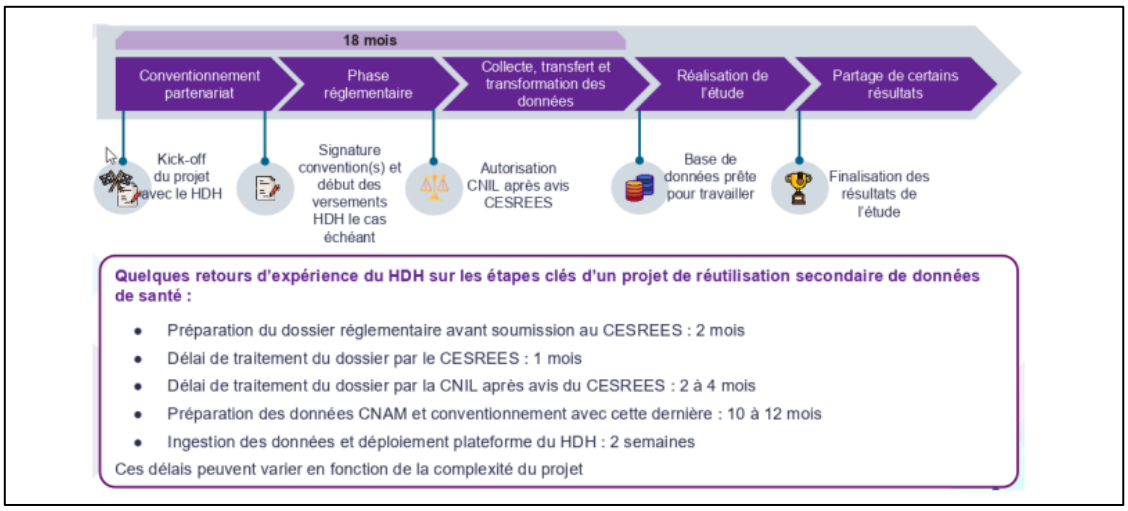
Même si d'autres facteurs sont en cause, il résulte de cette complexité que le délai entre la soumission du projet de recherche et la mise à disposition effective des données est évalué, en moyenne, à 18 mois, comme l'illustre le schéma suivant.

---

[87] *Donner un sens à l'intelligence artificielle. Pour une stratégie nationale et européenne*, mission confiée par le Premier ministre à M. Cédric Villani, mathématicien et député de l'Essonne, mars 2018.

[88] Cf. article R. 1461-3.

Schéma n° 1 : les grandes étapes d'un projet de recherche à partir de données de santé en France



Source : Rapport Igas Fédérer les acteurs de l'écosystème pour libérer l'utilisation secondaire des données de santé *de décembre 2023 / Plateforme des données de santé*

À titre de comparaison, en Finlande, l'accès aux données personnelles de santé varie de six à onze mois et en Allemagne, le centre de données de recherche a prévu de mettre à disposition des porteurs de projets les données qu'ils sollicitent dans un délai de trois mois. Au Royaume-Uni, le délai moyen entre le dépôt de demande d'accès et l'extraction des données par UK Biobank était inférieur à quatre mois en 2022.

Ces délais très longs en France ont des conséquences sur le nombre de demandes déposées de la part d'acteurs privés. De l'ordre d'une centaine par an entre 2018 et 2020, elles ont diminué jusqu'en 2022 (54 demandes) avant de revenir en 2023 à près d'une centaine. Pour autant, les chiffres pour 2024 montrent une nette amélioration de la situation. Selon la PDS, les délais moyens seraient passés de 18 à 4 mois (hors délais de la Cnil[89]) en 2024.

Dans le contexte du blocage de la copie de la base principale du SNDS sur la plateforme de la PDS, cette amélioration s'explique tout d'abord par la mise à la disposition de la Cnam de certains personnels de la PDS[90] afin de l'appuyer dans la réalisation d'opérations techniques de préparation de données (extractions, ciblages, etc.).

Cette évolution positive s'explique aussi par la signature en novembre 2023 d'une convention de co-responsabilité de traitement du SNDS entre les deux acteurs précités. Celle-ci donne à la PDS l'autonomie de la signature des contrats avec les porteurs de projets. La plateforme peut ainsi valider le périmètre des données en autonomie sur ses projets, ce qui peut faire gagner plusieurs mois. Pour autant, elle reconnaît que les performances en matière de délai pourront être évaluées avec le temps, *« le champ de cette convention étant encore limité à un faible nombre de projets »* (une dizaine). Des discussions sont en cours avec la Cnam pour élargir le périmètre de cette convention de co-responsabilité de traitement. D'ores et déjà,

[89] Les délais d'instruction par la Cnil des demandes d'autorisation pour des traitements de données de santé sont passés en moyenne de 73 jours en 2023 à 65 jours en 2024, 33 % ayant été traitées en moins d'un mois (contre 29 % en 2023), alors même que ces demandes ont connu une hausse de 20 % en 2024 (619 dossiers reçus).

[90] Les effectifs de la plateforme des données de santé sont passés de 34,9 équivalents temps plein travaillés (ETPT) en 2020 à plus de 100 en 2023.

toujours selon la plateforme, le portefeuille de projets a progressé de 60 % en 2024 (183 projets en cours d'accompagnement en juin 2025) et un taux de satisfaction moyen des chercheurs de 4,6/5 quant à l'accompagnement offert par la PDS.

En conclusion, accroître l'utilisation du SNDS, conformément à ce que prévoient les pouvoirs publics, implique donc non seulement qu'il comporte davantage de données cliniques, mais aussi que les délais de mises à disposition des données soient mieux maîtrisés. La situation présente est d'autant plus insatisfaisante que la PDS a été précisément constituée à cette fin.

3.3.3.5 Un choix d'hébergement des données qui bloque la pleine exploitation de la plateforme

Le choix d'un hébergement des données de la PDS par Microsoft Azure a été fait après une étude de marché puis en recourant au marché passé par l'Ugap, immédiatement disponible. Les courriers de la Drees du 13 février et du 4 mars 2019 insistaient sur la question des délais afin de réaliser la plateforme le plus rapidement possible, dès lors que la santé faisait partie des secteurs prioritaires définis par le président de la République à la suite du dépôt du rapport Villani.

Ce primat donné à la rapidité de mise en place de la plateforme ne permettait pas de lancer un projet souverain pour deux raisons majeures : les opérateurs nationaux n'offraient pas en 2019, selon la Drees, un niveau de service équivalent à celui des *hyperscalers* américains et un tel choix aurait nécessité le lancement d'un appel d'offres, prenant plusieurs mois.

Pour autant, une alternative aurait pu être davantage explorée, au minimum comme solution intermédiaire avant qu'une offre souveraine plus performante n'émerge. Si le Centre d'accès sécurisé aux données (CASD) n'a été certifié hébergeur des données de santé (HDS) qu'en décembre 2019, soit après la signature du contrat avec Microsoft en octobre, cette plateforme dédiée à la recherche (y compris en santé) était en production depuis 2010 et déjà partiellement interfacée avec le SNDS. Très sécurisée, elle est autorisée par la Cnil à travailler sur des données sensibles depuis 2014 et est potentiellement mobilisable sans appel d'offres et sous conditions au titre d'un contrat public-public de coopération ou d'une quasi-régie conjointe[91].

Le CASD ne présentait pas tous les prérequis attendus en 2019 pour héberger une copie du SNDS, mais les freins ne semblaient pas insurmontables : amélioration de la « scalabilité »[92] par un dimensionnement des capacités visant à faire face à des pics de charge ; mise à niveau d'outils comme les cartes graphiques ; développement d'un module de sécurité matériel (HSM), etc.

Des progrès ont été réalisés depuis 2019. En décembre 2023, la délégation au numérique en santé (DNS) évaluait la « conformité fonctionnelle » du CASD comme « élevée »[93] au

[91] Cf. articles L. 2511-1 à L. 2511-5 du code de la commande publique.

[92] La scalabilité, ou extensibilité, désigne la capacité d'un système à gérer une augmentation rapide de la charge de travail en ajustant ses ressources, sans compromettre les performances ou la fiabilité.

[93] En comparaison, les offres de cloud françaises analysées ne dépassaient pas 51 % « de conformité à date ».

regard des besoins du projet européen d'entrepôt multicentrique de données de santé dit « EMC2 » dont la réalisation a été confiée au GIP PDS[94].

Les fonctionnalités requises pour le projet européen sont moins ambitieuses que celles de la PDS et des développements complémentaires seraient assurément encore nécessaires pour disposer d'une telle conformité sur l'ensemble des besoins de la PDS. Mais cette capacité du CASD à « monter en gamme », inexploitée en 2019, est confirmée *a posteriori*.

En dehors de la priorité donnée aux délais, il convient de rappeler que le choix de Microsoft Azure fin 2019 s'inscrivait dans un contexte particulier. Les questions de souveraineté numérique étaient moins prégnantes, la doctrine « cloud au centre » n'avait pas encore été élaborée et les données des Européens étaient toujours régies par l'accord d'adéquation *Privacy Shield* qui n'a été invalidé par la Cour de justice de l'Union européenne que le 16 juillet 2020 à travers l'arrêt Schrems II.

Par ailleurs, l'hébergement par Microsoft Azure n'était considéré, dès le départ, que comme une solution temporaire. Le courrier de la Drees à la ministre de la santé en date du 4 mars 2019 mentionne que *« la contractualisation d'une telle solution serait limitée à la durée du prototype et prévoirait des clauses fermes de réversibilité*[95] *»*. La Drees ajoute que *« cela ne compromet en aucun cas le choix d'une autre solution pour une version future de la plateforme prenant en compte le développement de services managés*[96]*. En particulier, le prototype pourra parfaitement migrer vers une solution d'État lorsque cette dernière sera mature. Dans cette attente, il est essentiel de ne pas compromettre deux années de fonctionnement du* Health Data Hub. *»*

Si cette contractualisation avec Microsoft Azure répondait à une volonté de célérité afin que la France rattrape son retard en matière d'IA en santé, force est de constater que cette solution transitoire a déclenché de nombreux blocages et recours juridiques (cf. Annexe n° 5) qui ont *in fine* entravé la mise en place de la plateforme et, surtout, sa capacité à répondre aux besoins des chercheurs. Ces recours comme les polémiques associées ont bloqué le transfert d'une copie du SNDS à la PDS depuis 2019, laissant à la Cnam une charge administrative conséquente qui a entraîné un goulet d'étranglement au regard des sollicitations reçues.

Dans l'attente de ce transfert, le décret du 29 juin 2021 relatif au traitement du SNDS autorise la PDS et la Cnam, sous couvert de la Cnil, à mettre à disposition des données de cette base projet après projet, quel que soit le moyen technique mobilisé. De cette organisation résulte la réalisation sur l'année 2024 de plus de 300 extractions, 32 appariements directs et indirects, six ciblages de populations d'étude ou témoin.

Cependant, si des transferts de données ont désormais lieu au cas par cas du SNDS aux chercheurs via la PDS, en fonction des projets validés par la Cnil, la position de l'autorité

[94] La PDS a remporté l'appel d'offres lancé par l'Agence européenne du médicament (EMA) fin 2021.

[95] Si le contrat avec Microsoft ne mentionne pas de clauses de réversibilité, le plan d'assurance qualité de l'accord-cadre détaille sur 6 pages les modalités qui s'imposent en la matière aux prestataires choisis. En informatique, la réversibilité désigne la capacité pour un client ayant externalisé la gestion de son système d'information à un prestataire de récupérer ses données, logiciels et infrastructures à la fin ou en cas de rupture de contrat. Cette notion est à distinguer des clauses de résiliation qui définissent les conditions de fin du contrat sans garantir la récupération des données et des infrastructures par le client.

[96] Les services managés constituent un modèle d'externalisation informatique à travers lequel une entreprise délègue la gestion et l'administration de son système informatique à un fournisseur externe spécialisé. Ce dernier peut gérer un large éventail de services : la surveillance et la maintenance des systèmes informatiques ; la gestion des réseaux ; le support technique ; des services cloud.

administrative indépendante est restée intangible, y compris après la décision d'adéquation prise en juillet 2023 par la Commission européenne (*Data Privacy Framework*). La Cnil rappelle que les *« conditions de stockage doivent être conformes au code de la santé publique et les données ne peuvent pas être transférées en dehors de l'UE, sauf dans des cas très particuliers (projets de recherche impliquant un acteur extra-européen par exemple) »*. Pour ce qui a trait à la PDS, elle précise qu'elle *« souhaite que son hébergement et les services liés à sa gestion puissent être réservés à des entités relevant exclusivement des juridictions de l'UE ou bénéficiant de certifications de type SecNumCloud »*.

3.3.3.6 Vers une alternative souveraine à compter de 2026 ?

En accord avec la position de la Cnil précitée, le ministère de la santé souhaite que la PDS utilise une solution technique souveraine. Dès 2020, le ministre s'était prononcé pour la migration de la plateforme vers un *cloud* souverain afin de pouvoir copier toute la base principale du SNDS ainsi que le catalogue[97]. La ministre déléguée chargée du numérique a réaffirmé en avril 2025 la volonté du gouvernement d'enclencher un appel d'offres afin de mettre en conformité l'hébergement des données de santé avec les exigences de souveraineté fixées par la loi SREN et de migrer l'hébergement d'une copie du SDNS par la PDS vers un hébergeur sécurisé et souverain.

La mission Marchand-Arvier mise en place pour élaborer une feuille de route sur l'utilisation secondaire des données de santé estimait, dans son rapport déposé le 5 décembre 2023, que 24 mois constituaient une *« échéance ambitieuse, mais crédible à ce stade »* pour basculer la copie de la base principale du SNDS sur un *cloud* SecNumCloud. C'est également le délai minimal envisagé par le GIP PDS dans son calendrier de migration.

Il est regrettable que, depuis la publication de ce rapport, le GIP PDS n'ait pas entrepris de démarches volontaires pour engager cette bascule. Le GIP précise que ses équipes « *réalisent régulièrement des points de situation avec la Dinum et restent à l'écoute des industriels pour anticiper la migration de la plateforme technologique* ». Dès lors, la migration de la plateforme vers un environnement SecNumCloud paraît difficilement envisageable avant la fin de l'année 2026 et à la condition du maintien d'une volonté politique forte et constante comme d'un suivi rigoureux du plan de migration par le ministère de la santé, ministère de tutelle du GIP PDS.

D'ici là, un appel d'offres pour une « *solution intercalaire* » a été lancé début juillet 2025 par le GIP afin de sélectionner un prestataire souverain pour héberger une copie du SNDS. L'objectif de cette solution est de réduire les délais d'accès aux données de la base principale du SNDS pour les projets de recherche des différents acteurs publics et privés.

[97] Le catalogue est une collection de bases de données qui peuvent être ajoutées au SNDS, comme la base de résumés des passages individuels aux urgences, la base de données relative à la cohorte de patients infectés par le virus de l'hépatite B ou C ou la base relative à la cohorte de patients atteints de la maladie d'Alzheimer.

3.3.4 Un hébergement de données sensibles par des opérateurs privés qui mériterait d'être encadré pour concilier souveraineté et performance

La qualification SecNumCloud s'impose à l'État pour l'hébergement de ses données sensibles, au titre de la loi SREN. Dans certains domaines, comme l'éducation ou la santé, des entreprises privées opèrent des services, qui pourraient relever de la puissance publique et manient de telles données. Ces entreprises ne sont pas soumises à la même obligation que l'État, mais peuvent bien sûr s'y conformer. L'Anssi souligne par ailleurs que, au-delà de la qualification SecNumCloud, les produits et services de cybersécurité sont d'une grande sensibilité et que leur maîtrise, qui passe notamment par le dispositif de contrôle des investissements étrangers, est également un enjeu de souveraineté.

3.3.4.1 Le marché des applications de gestion de la vie scolaire contrôlé par des entreprises françaises

Le MEN dispose de compétences dans le domaine du numérique qui lui permettent de développer de nombreuses applications métiers. Il a ainsi proposé aux établissements, libres de leurs choix en vertu de leur autonomie pédagogique et éducative, l'outil Siècle[98], module de gestion administrative, pédagogique et financière des élèves dans les établissements du second degré. Mais les modules, appelés Siècle+, dédiés à la vie scolaire se sont avérés très peu utilisés comparativement aux services proposés par des prestataires privés. Seuls 36 établissements y recouraient à la rentrée scolaire 2024. La DNE a décidé d'abandonner Siècle+ à la rentrée 2025, constatant son échec à rivaliser avec des logiciels du marché.

Des acteurs français ont, de fait, développé des solutions numériques pour la vie scolaire qui se sont très largement imposées. Index Éducation, à l'origine une start-up fondée à Marseille en 1992, s'est ainsi rapidement développé sur ce marché avec la conception de logiciels d'emploi du temps, de gestion de planning et de vie scolaire tels que Pronote, EDT ou Hyperplanning.

À la suite d'un rapport de la Cour publié en 2019[99] mentionnant le manque de maîtrise par l'Éducation nationale *« de données importantes, qui expose le dispositif scolaire national à des risques de gravité diverse, de la perturbation du déroulement d'une rentrée scolaire (attaques malveillantes), à des traitements croisés à des fins qui lui sont étrangères (profilage), voire à une situation de dépendance envers des Gafam (hypothèse de rachat d'Index-éducation) »*, l'État a souhaité confier à un acteur français et souverain la destinée d'une entreprise spécialisée dans la gestion numérique des établissements scolaires français, présente sur les trois cycles de l'enseignement (primaire, secondaire et supérieur). Dans ce contexte, Docaposte, filiale numérique du groupe La Poste, s'est porté acquéreur en 2020 d'Index Éducation.

En complément de ses offres historiques, Index Éducation propose également des solutions à destination des collectivités territoriales et leurs délégataires, des ministères et de leurs services déconcentrés. Non seulement Index Éducation offre des solutions variées pour

[98] Système d'information pour les élèves des collèges, des lycées et pour les établissements.
[99] *Le service public numérique pour l'éducation*, Cour des comptes, juillet 2019.

tous les acteurs du monde de l'éducation, mais il occupe en outre une position importante dans le secondaire[100]. Outre Index Éducation, plusieurs entreprises françaises se disputent ce marché, notamment Axess Éducation, Kosmos et Aplim très implantée dans l'enseignement privé avec la solution EcoleDirecte.

Même si les données ne sont pas gérées directement par le MEN, car confiées à des opérateurs privés, elles apparaissent à ce stade sous contrôle au regard du risque lié à l'extraterritorialité du droit, notamment américain. En effet, Index Éducation est un produit d'une entreprise publique, Docaposte, qui a fait le choix de recourir de sa propre initiative à une infrastructure qualifiée SecNumCloud pour les produits d'Index Éducation depuis juin 2024. Quant à Aplim, si son offre n'est pas qualifiée SecNumCloud, la société affirme dans sa communication être *« un éditeur de logiciel dont tous les produits et services sont réalisés en France, que ce soit le développement, l'assistance, l'hébergement, les formations. »*

La maîtrise des données et la souveraineté numérique sont par ailleurs des préoccupations affichées par le ministère. Dans sa stratégie en la matière publiée en janvier 2023[101], la volonté de soutenir des « communs numériques » fondés sur des logiciels libres est affichée afin de fournir aux professeurs et à leurs élèves, *« conformément à la stratégie de souveraineté numérique du Gouvernement. »*, différents outils à travers la plateforme de services « apps education.fr »[102]. La cadre technique de référence pour les services numériques éducatifs défini par le ministère et publié en juillet 2024[103] confirme cette approche en mentionnant que ce cadre permet *« aux usagers et aux sociétés de la filière industrielle du numérique éducatif de bénéficier de services innovants, mais aussi en souveraineté en excluant toute solution non respectueuse des règles édictées, notamment en matière d'éthique et de protection des données. »*

L'État met ainsi à disposition de la communauté éducative des services « socles » nationaux assurant un certain nombre de fonctions utiles voire nécessaires au bon fonctionnement d'ensemble des solutions numériques utilisées (authentification, circulation des données d'organisation pédagogique, gestion des accès aux ressources et de suivi de la fréquentation par exemple), fonctions qui relèvent chacune d'un service national de référence permettant *« de garantir à la fois la bonne circulation et la souveraineté des données. »*

Les établissements bénéficient néanmoins d'une grande liberté dans le choix de leurs outils numériques du fait de leur autonomie pédagogique et éducative définie par le code de l'éducation. Aussi la responsabilité du traitement de ces données leur incombe, et plus particulièrement à la personne ayant la capacité juridique de représenter l'établissement, notamment en justice dans l'éventualité d'un recours. Dans les établissements publics locaux d'enseignement du second degré, qui ont la personnalité juridique, le chef d'établissement est

[100] Cette société fournit ainsi en 2025 des outils à 340 écoles primaires sur 48 220 ; 10 300 établissements du secondaire (collèges et lycées) et plus de 320 établissements du supérieur ou centres de formation dans 128 pays. Sur 12 497 établissements du secondaire publics et privés en France (collèges et lycées), les logiciels d'Index Éducation ont ainsi une part de marché de 70 % pour EDT (logiciel d'emploi du temps) et 61 % pour Pronote (vie scolaire).

[101] Ministère de l'éducation nationale, *Numérique pour l'éducation 2023-2027, la vision stratégique d'une politique publique partagée*, janvier 2023.

[102] À titre d'exemple, le ministère propose des outils de collaboration ou de communication comme « classes virtuelles » et « visio-agents », fondés tous deux sur le logiciel libre BigBlueButton, ou encore des outils permettant le partage de fichiers ou la publication de vidéos hébergées sur des infrastructures françaises.

[103] Ministère de l'éducation nationale, *Doctrine technique du numérique pour l'éducation*, juillet 2024.

responsable des traitements mis en œuvre à son niveau. En revanche, les directeurs d'école n'ayant pas cette capacité juridique dans le secteur public, ce sont les directeurs académiques des services de l'éducation nationale (Dasen), agissant sur délégation des recteurs d'académie, qui sont responsables de ces mêmes traitements.

Les données générées par les outils utilisés par les établissements scolaires revêtiraient un grand intérêt pour le ministère pour piloter le service public de l'éducation. Mais récupérer ces données puis les consolider à des fins de pilotage supposerait de les verser dans les applications ministérielles tout en garantissant leur protection conformément au RGPD. En l'absence de cadre réglementaire, Docaposte refuse d'effectuer ces versements. L'entreprise estime que si elle venait à décider de communiquer toutes les données à caractère personnel souhaitées par le ministère sans l'accord des chefs d'établissement, elle agirait alors en illégalité, ce qui l'exposerait à une amende maximale de 4 % du chiffre d'affaires du Groupe La Poste et affecterait la confiance des utilisateurs. Docaposte considère également que les critères techniques ne sont pas toujours respectés, la majorité des exports pouvant être réalisée en clair sous la forme de fichiers XML.

Le blocage de l'utilisation des données de vie scolaire

Par un courrier en date du 14 janvier 2025, les associations Avicca[104], Régions de France et Départements de France ont écrit à la ministre de l'éducation nationale afin qu'elle garantisse la circulation des données nécessaires au fonctionnement et à la bonne gestion du service public de l'éducation. En effet, les collectivités dépendent de ces données, fabriquées et hébergées par des outils qu'elles cofinancent, pour faire fonctionner des services tels que les espaces numériques de travail (ENT), la communication avec les familles, l'optimisation de la gestion des bâtiments (taux d'occupation des salles, entretien, chauffage, aération, etc.), des transports, etc.

Face au blocage de la transmission de ces données essentiellement issues, pour ce qui concerne le public, des logiciels opérés par des entreprises, ces acteurs demandent au ministère *« de tout mettre en œuvre, et notamment des moyens financiers et humains, pour que les conditions juridiques et techniques soient rapidement et définitivement mises en place afin de garantir la circulation des données détenues par des acteurs tiers. »*

En réponse, dans un courrier du 8 avril 2025, la ministre rappelle qu'une doctrine technique du numérique pour l'éducation a été publiée à l'été 2024, coconstruite avec les différents acteurs concernés, dont les éditeurs afin de garantir l'interopérabilité des outils. Conformément à cette doctrine, elle mentionne que le ministère opère un service d'infrastructure Scope[105] qui organise la circulation des données scolaires entre les différentes solutions : « *Techniquement opérationnel, Scope couvre une dizaine de cas d'usage, dont la remontée des emplois du temps dans les ENT et la gestion énergétique des bâtiments scolaires* ». Par ailleurs, elle souligne que *« le ministère soutient activement les solutions libres d'ENT, en particulier la plateforme ÉLEN[106] […] construite pour communiquer nativement avec les logiciels d'emploi du temps et de vie scolaire,*

[104] L'association des villes et collectivités pour les communications électroniques et l'audiovisuel (Avicca) a été créée en 1986. Elle regroupe des collectivités territoriales engagées dans le développement numérique, notamment dans les domaines des réseaux, de l'équipement, du numérique éducatif, des territoires intelligents, et de l'audiovisuel local.

[105] Service outillant la circulation de l'organisation pédagogique de l'établissement, Scope est porté par le système d'information ministériel Siècle de l'établissement.

[106] Environnement libre pour enseigner avec le numérique.

et d'ores et déjà déployée avec succès par les collectivités de Bretagne et des Pays de la Loire. » Enfin, elle propose la mise en œuvre par décret de l'opposabilité juridique de la doctrine technique du ministère pour l'ensemble des acteurs et la création d'un GIP partagé entre l'État et les collectivités territoriales volontaires *« de nature à porter durablement une offre numérique commune (notamment la plateforme « ÉLEN » citée plus haut). »*

L'éducation nationale souhaite ainsi imposer aux éditeurs son cadre technique afin de sécuriser juridiquement la remontée des données sans avoir à contractualiser avec chaque EPLE et faire émerger à terme une alternative publique qui finisse par s'imposer, ce que le ministère a déjà tenté en vain avec Siècle.

3.3.4.2 L'hébergement de données de santé par des éditeurs privés

Si le débat sur les risques que fait peser l'extraterritorialité du droit sur la protection des données de santé se focalise, concernant les acteurs publics, sur la PDS à des fins de recherche, il ne faut pas oublier les données hébergées par l'ensemble de l'écosystème du soin en France pour son fonctionnement courant.

Pour être autorisés à gérer ces données, les prestataires numériques du secteur sont tenus d'être certifiés HDS, obligation prescrite par l'article L. 1111-8 du code de la santé publique. Pour autant, cette certification, qui permet d'attester de la bonne mise en œuvre d'un système de gouvernance de la sécurité de l'information, ne prémunit pas contre les risques inhérents à l'extraterritorialité du droit. Parmi les très nombreux[107] hébergeurs certifiés figurent les *hyperscalers* américains. Or, les acteurs de la santé conventionnés avec l'assurance maladie n'échappent pas à la tendance qui est à l'externalisation de l'hébergement des données. Le rapport de la Cour intitulé *La sécurité informatique des établissements de santé*, publié en janvier 2025, montre une prépondérance de l'hébergement externalisé dans le secteur : 55 % pour le public, 58 % pour le privé lucratif, 78 % pour le privé non lucratif.

Dans ce contexte, le ministère de la santé a attribué en janvier 2021 à trois sociétés – Doctolib, Maiia et Keldoc – le marché lié à l'organisation de la campagne de vaccination après un appel d'offres lancé par l'Ugap. Doctolib a ainsi rapidement équipé 1 500 centres sur tout le territoire. Sur l'ensemble de l'année 2021, ce sont 81 millions de rendez-vous de vaccination contre la Covid-19 qui ont ainsi été pris sur sa plateforme.

En février et mars 2021, des associations et syndicats professionnels de la santé ont toutefois demandé au juge des référés du Conseil d'État de suspendre le contrat conclu entre le ministère de la santé et Doctolib. Ceux-ci estimaient que l'hébergement des données de Doctolib par la filiale d'une société américaine comportait des risques au regard de demandes d'accès par les autorités américaines.

Cette contestation s'inscrivait dans la suite de l'arrêt « Schrems II » de la CJUE du 16 juillet 2020 qui a jugé que la protection des données transférées vers les États-Unis par le *Privacy Shield* était insuffisante au regard du droit européen. Or, en l'absence d'une nouvelle décision d'adéquation, un transfert de données personnelles hors UE devait être accompagné de garanties appropriées. Cela supposait qu'un niveau de protection équivalent des personnes

[107] 302 en 2024 selon le site de l'agence du numérique en santé.

concernées soit assuré dans l'État destinataire des données, y incluant à la fois la protection accordée par le RGPD et celle de la Charte des droits fondamentaux de l'Union européenne.

Afin de satisfaire aux exigences posées par cet arrêt, le juge des référés du Conseil d'État a examiné le niveau de protection assuré lors du traitement des données en tenant compte de leur nature, de ce que prévoit le contrat conclu entre Doctolib et une entreprise américaine ainsi que du droit applicable à cette société.

Le juge des référés a estimé que le niveau de protection des données concernées n'était alors manifestement pas insuffisant au regard du risque invoqué par les associations et syndicats requérants, et compte tenu de la nature des données en cause. Il a notamment relevé que les données transmises à Doctolib dans le cadre de la campagne de vaccination ne comprenaient pas de données sur les motifs médicaux d'éligibilité à la vaccination, mais portaient uniquement sur l'identification des personnes et la prise de rendez-vous, ces données étant par ailleurs supprimées au plus tard à l'issue d'un délai de trois mois à compter de la date de rendez-vous. Il a, dès lors, rejeté leur demande.

Depuis 2021, les services proposés par Doctolib ont toutefois été enrichis. Le suivi des rendez-vous médicaux a été complété par le partage de documents (comptes-rendus, résultats d'examens, etc.) qui comportent désormais des données de santé personnelles, par nature sensibles.

Si l'hébergement des données de l'entreprise par un *hyperscaler* n'est, pour l'heure, pas remis en cause juridiquement, le ministère de la santé travaille à une sensibilisation des hébergeurs certifiés HDS aux enjeux de souveraineté. La dernière feuille de route du numérique en santé 2023-2027 a inscrit dans ses priorités *« la cybersécurité dans les établissements, notre souveraineté sur l'hébergement et notre résilience face aux futures crises sanitaires »*. Elle préconise un renforcement du cadre réglementaire définissant les conditions d'hébergement.

Ainsi, la nouvelle version du référentiel HDS, publiée en mai 2024, stipule que lorsque l'hébergeur, ou l'un de ses sous-traitants, est soumis à la législation d'un pays tiers n'assurant pas un niveau de protection adéquat au sens du RGPD, il doit indiquer contractuellement :

- la liste des réglementations extra-européennes en vertu desquelles l'hébergeur, ou l'un de ses sous-traitants, serait tenu de permettre un accès non autorisé par le droit de l'UE aux données de santé à caractère personnel, au sens de l'article 48 du RGPD ;
- les mesures mises en œuvre par l'hébergeur pour atténuer les risques d'accès non autorisé à ces données, induits par ces réglementations extra-européennes ;
- la description des risques résiduels d'accès non autorisés à ces données via des réglementations extra-européennes qui demeureraient malgré ces mesures.

L'hébergeur doit aussi rendre publique et mettre à jour la cartographie des transferts des données de santé à caractère personnel vers un pays n'appartenant pas à l'Espace économique européen où ces données doivent désormais être exclusivement localisées. L'hébergeur doit mettre ces informations à la disposition du public de manière lisible.

Par ailleurs, une matrice de correspondance avec les exigences du référentiel SecNumCloud a été annexée au référentiel HDS afin de faciliter la qualification SecNumCloud des solutions des hébergeurs déjà certifiés HDS.

La feuille de route du numérique en santé prévoit que, à horizon 2027, *« dès qu'un consensus européen aura émergé sur les exigences du niveau 3 du futur schéma de certification européen sur les services en nuage (EUCS), et qu'une offre souveraine suffisamment large sera*

disponible, la certification HDS fixera de nouvelles exigences en termes de souveraineté. Les acteurs sont incités à anticiper, en commençant le plus tôt possible avec leurs nouveaux projets. »

⁂

Eu égard à leur sensibilité, la protection des données de santé revêt une importance majeure pour la puissance publique, du point de vue tant de la sécurité informatique que de leur étanchéité vis-à-vis de l'extraterritorialité du droit.

Par conséquent, il convient de poursuivre et d'achever le rapprochement du certificat HDS avec les exigences du SecNumCloud en matière de souveraineté.

Recommandation n° 5. (Délégation au numérique en santé) : Assurer la souveraineté de l'hébergement des données de santé en alignant la certification « Hébergeur de données de santé » sur les exigences de la qualification SecNumCloud en matière de protection vis-à-vis du droit extra-européen.

CONCLUSION INTERMÉDIAIRE

La doctrine « Cloud au centre » a permis une augmentation de la commande publique malgré les obstacles liés à la bascule des infrastructures traditionnelles sur le cloud. Le nombre restreint de services qualifiés SecNumCloud et les coûts élevés associés à cette qualification soulignent les défis persistants pour le développement d'une offre compétitive.

Les clouds internes de l'État, Nubo et Pi, n'ont bénéficié que de modestes investissements comparativement aux budgets alloués aux systèmes d'information de l'État et aux investissements du secteur privé. Ils restent encore peu utilisés en interministériel, du fait d'une gamme et d'un niveau de services limités et de tarifications dissuasives.

Aussi, les enjeux de souveraineté et de protection des données sensibles restent majeurs pour les systèmes d'information civils de l'État. Avec le projet Virtuo, visant à moderniser sa gestion des ressources humaines, le ministère de l'éducation nationale a privilégié les critères de performance et de coût à ceux de souveraineté bien que l'application manie des données d'une particulière sensibilité.

Au ministère des finances, le portail public de facturation et la plateforme Piste montrent l'importance de la souveraineté numérique pour les données des entreprises avec un recours à des infrastructures SecNumCloud. Cependant, ces exigences ne sont pas suivies dans tous les cas, comme avec la plateforme Place, où des données sensibles recourent à des environnements non qualifiés.

De fait, il n'existe pas d'inventaire interministériel formalisé des données sensibles à héberger de manière souveraine. Or, la non maîtrise par l'État de certaines données sensibles, fussent-elles personnelles et non directement liées à la sécurité nationale, fait peser un risque sur la souveraineté du pays, car la collecte en masse de données est un enjeu majeur pour les grandes puissances afin, notamment, de développer leurs capacités en intelligence artificielle.

Malgré la nécessité de recourir à une infrastructure souveraine, la plateforme des données de santé est hébergée depuis plus de cinq ans auprès d'une grande entreprise américaine du numérique. Bien qu'offrant un service théoriquement plus performant, ce choix a généré des blocages qui ont ralenti son déploiement et, au final, réduit la qualité de service.

Certains opérateurs privés opèrent des applications très populaires maniant des données sensibles des citoyens. Pour autant, ils ne sont pas soumis aux mêmes obligations que les services de l'État. Dans le domaine de la santé, une certification existe (hébergeur de données de santé), mais n'inclut pas encore d'exigences en matière de souveraineté.

Dans le domaine du numérique, la recherche d'un degré très élevé de performance peut conduire à retenir des spécifications techniques que des solutions non souveraines sont souvent seules en mesure de satisfaire. Aussi, les administrations publiques devraient viser une performance de leur système d'information strictement adaptée à leurs besoins, pour assurer la parfaite prise en compte des enjeux de souveraineté.

ANNEXES

Annexe n° 1. Comparaison entre les différents modèles d'informatique

Le modèle d'informatique traditionnel consiste pour une entité à héberger son infrastructure informatique sur le même site que celui où elle gère ses activités opérationnelles. Cette infrastructure comprend les serveurs, les équipements de connexion et les matériels de soutien. Elle peut prendre la forme d'une simple salle d'armoires à serveurs ou d'un « centre de données ».

À partir des années 2000, les pratiques ont évolué, conduisant à délocaliser les centres de données et, concomitamment, à louer, souvent à plusieurs, les bâtiments eux-mêmes, puis les matériels qu'ils accueillent. Dans ce modèle, l'entité cliente accède à distance aux ressources et conserve la responsabilité de l'exploitation et des données, mais confie à un tiers la responsabilité de la maintenance et de la continuité de service.

L'utilisation du « *Cloud computing* » constitue une étape supplémentaire qui permet aux utilisateurs et aux entreprises de s'affranchir de la nécessité de gérer des serveurs physiques eux-mêmes, mais aussi d'exécuter des applications logicielles sur leurs propres équipements, notamment via les techniques de virtualisation (technologie permettant de créer et d'exécuter plusieurs représentations virtuelles d'un ordinateur sur une même machine physique). Dans ce cadre, l'entité cliente ne loue plus des serveurs physiques précisément identifiés, mais des serveurs virtuels qui peuvent être mis en place et supprimés en tant que de besoin, ainsi que d'autres prestations, le cas échéant, souvent facturées à l'usage.

Le tableau suivant présente l'évolution de l'informatique traditionnelle vers le modèle de l'informatique en nuage.

Tableau n° 6 : évolution des modèles d'informatique

	INFORMATIQUE TRADITIONNELLE			INFORMATIQUE EN NUAGE			
	SUR SITE *On-Premises*	**COLOCATION** *Colocation*	**HÉBERGEMENT** *Hosting*	**INFRASTRUCTURE EN TANT QUE SERVICE** *IaaS*	**PLATEFORME EN TANT QUE SERVICE** *PaaS*	**LOGICIEL EN TANT QUE SERVICE** *SaaS*	
VIRTUEL	Données	Données	Données	Données	Données	Données	**GESTION CONFIÉE À UN TIERS**
	Applications	Applications	Applications	Applications	Applications	Applications	
	Bases de données	Bases de données	Bases de données	Bases de données	Bases de données	Bases de données	
	Systèmes d'exploitation	Systèmes d'exploitation	Systèmes d'exploitation	Systèmes d'exploitation	Systèmes d'exploitation	Systèmes d'exploitation	
	Virtualisation	Virtualisation	Virtualisation	Virtualisation	Virtualisation	Virtualisation	
PHYSIQUE	Serveurs physiques	Serveurs physiques	Serveurs physiques	Serveurs physiques	Serveurs physiques	Serveurs physiques	
	Stockage	Stockage	Stockage	Stockage	Stockage	Stockage	
	Réseaux	Réseaux	Réseaux	Réseaux	Réseaux	Réseaux	
	Salles serveur, centres de données (data centers)	Centres de données (data centers)	Centres de données (data centers)	Centres de données (data centers)	Centres de données (data centers)	Centres de données (data centers)	

Source : Cour des comptes

Cette évolution s'est accompagnée d'un transfert de responsabilités au prestataire de *cloud*, transfert plus ou moins étendu selon la prestation choisie. L'accès à ces services s'effectue en effet selon trois principaux modèles :

- Infrastructure en tant que service (IaaS) ou hébergement distant des données : le prestataire fournit un environnement virtuel (les serveurs, le réseau, ainsi que les ressources de traitement et de calcul) mais le client utilise son propre système d'exploitation et ses logiciels. Cela permet d'obtenir un service de stockage susceptible d'évoluer en fonction des besoins ;
- Plateforme en tant que service (PaaS) : ce service fournit, en plus de l'hébergement des données, un système d'exploitation et des outils (*frameworks*) qui permettent aux équipes informatiques de l'entreprise cliente de développer leurs propres applications ; le fournisseur est responsable de l'environnement de développement, mais le client conserve la gestion de ses produits numériques ;
- Logiciel en tant que service (SaaS) : ce service représente la forme la plus aboutie de l'informatique en nuage, puisqu'il permet d'utiliser un logiciel directement dans le *cloud*. L'utilisateur final y accède à distance, depuis n'importe quel terminal, à l'aide d'une connexion Internet. Ce modèle s'oppose au mode de fonctionnement local (« on-premise ») où le client acquiert la licence d'un logiciel et l'installe sur son poste.

Par ailleurs, les différents types de *cloud* commerciaux se distinguent principalement par leur architecture, leur niveau de sécurité, leur coût et leur flexibilité.

Tableau n° 7 : comparaison des différents types de *cloud* commerciaux

Type	Propriété	Accès	Coût	Sécurité	Cas d'usage
Cloud public	Géré par des fournisseurs tiers (ex. : Amazon Web Services, Microsoft Azure)	Partagé entre plusieurs utilisateurs	Modèle de tarification basé sur l'utilisation, souvent moins onéreux	Niveau standard, adapté aux données non sensibles	Hébergement de sites web, développement d'applications, stockage de fichiers
Cloud privé	Exclusivement dédié à une seule organisation	Accès restreint aux utilisateurs autorisés	Généralement plus coûteux en raison de l'infrastructure dédiée	Sécurité renforcée, idéal pour les secteurs réglementés (santé, finance)	Gestion de données sensibles, applications critiques
Cloud hybride	Combine des éléments de *cloud* public et privé	Permet le déplacement des charges de travail entre les environnements	Optimisation des coûts en fonction des besoins, flexibilité accrue	Allie la sécurité du *cloud* privé avec l'agilité du *cloud* public	Entreprises ayant des besoins de scalabilité tout en maintenant certaines données en interne

Type	Propriété	Accès	Coût	Sécurité	Cas d'usage
Multicloud	Utilise plusieurs services *cloud* de différents fournisseurs	Permet une distribution des charges de travail entre plusieurs plateformes	Peut réduire les dépendances et optimiser les coûts en choisissant les meilleures offres	Dépend des stratégies de chaque fournisseur, mais offre une résilience accrue	Stratégies avancées de récupération après sinistre, optimisation des performances globales

Source : Cour des comptes

Annexe n° 2. Article 31 de la loi SREN

Article 31 de la loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (caractères en gras et soulignés par la Cour des comptes) :

I. - Lorsque les administrations de l'État, ses opérateurs dont la liste est annexée au projet de loi de finances ainsi que les groupements d'intérêt public comprenant les administrations ou les opérateurs mentionnés précédemment et dont la liste est fixée par décret en Conseil d'État ont recours à un service d'informatique en nuage fourni par un prestataire privé pour la mise en œuvre de systèmes ou d'applications informatiques, ils respectent les dispositions du présent article.

Si le système ou l'application informatique concerné traite de ***données d'une sensibilité particulière****, définies au II, qu'elles soient à caractère personnel ou non,* ***et si leur violation est susceptible d'engendrer une atteinte à l'ordre public, à la sécurité publique, à la santé ou à la vie des personnes ou à la protection de la propriété intellectuelle****, l'administration de l'État, ses opérateurs et les groupements mentionnés au présent I veillent à ce que le service d'informatique en nuage fourni par le prestataire privé mette en œuvre des* ***critères de sécurité et de protection des données garantissant notamment la protection des données traitées ou stockées contre tout accès par des autorités publiques d'États tiers*** *non autorisé par le droit de l'Union européenne ou d'un* ***État*** *membre.*

II. - ***Sont qualifiées de données d'une sensibilité particulière*** *au sens du I :*

1° Les données qui relèvent de secrets protégés par la loi*, notamment au titre des articles L. 311-5 et L. 311-6 du code des relations entre le public et l'administration ;*

2° *Les données nécessaires à l'accomplissement des* ***missions essentielles de l'État,*** *notamment* ***la sauvegarde de la sécurité nationale, le maintien de l'ordre public et la protection de la santé et de la vie des personnes.***

III. - Lorsque, à la date d'entrée en vigueur du présent article, l'administration de l'État, son opérateur ou le groupement mentionné au I a déjà engagé un projet nécessitant le recours à un service d'informatique en nuage, cette administration, cet opérateur ou ce groupement peut solliciter une dérogation au présent article.

IV. - Le I est applicable au groupement mentionné à l'article L. 1462-1 du code de la santé publique[108]*.*

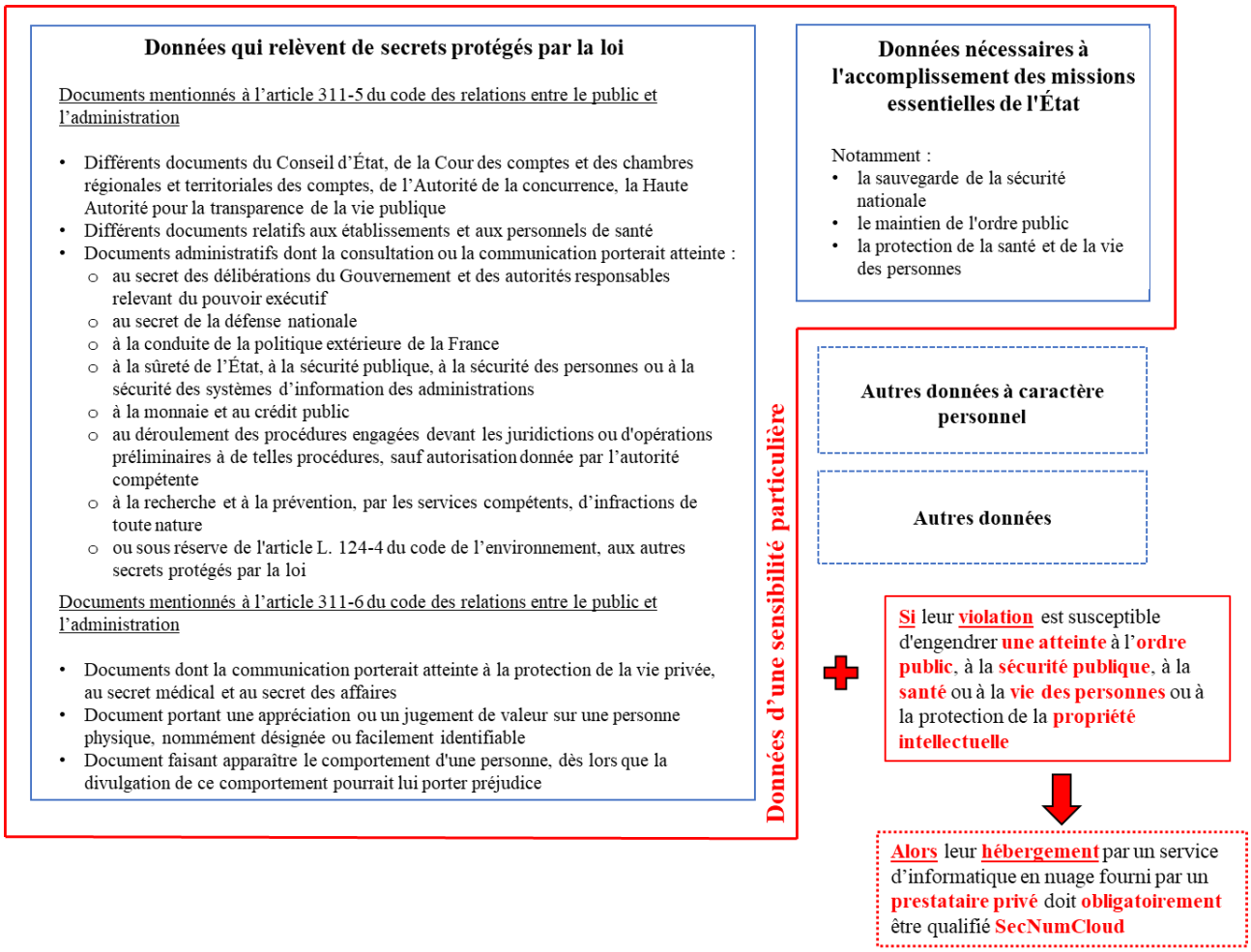
V. - Dans un délai de six mois à compter de la promulgation de la présente loi, un décret en Conseil d'État précise les modalités d'application du présent article, notamment les critères de sécurité et de protection, y compris en termes de détention du capital, des données mentionnés au I. Ce décret précise également les conditions dans lesquelles une dérogation motivée et rendue publique peut être accordée sous la responsabilité du ministre dont relève le projet déjà engagé et après validation par le Premier ministre, sans que cette dérogation puisse excéder dix-huit mois à compter de la date à laquelle une offre de services d'informatique en

[108] Plateforme des données de santé.

nuage acceptable est disponible en France, et fixe éventuellement les critères selon lesquels une telle offre peut être considérée comme acceptable.

VI. - Dans un délai de dix-huit mois à compter la promulgation de la présente loi, le Gouvernement remet au Parlement un rapport évaluant les moyens supplémentaires pouvant être pris afin de rehausser le niveau de la protection collective face aux risques et aux menaces que les législations extraterritoriales peuvent faire peser sur les données qualifiées d'une sensibilité particulière par le présent article ainsi que sur les données de santé à caractère personnel. Ce rapport évalue également l'opportunité et la faisabilité de soumettre les fournisseurs de services d'informatique en nuage établis en dehors de l'Union européenne à un audit de chiffrement certifié par l'Agence nationale de la sécurité des systèmes d'information.

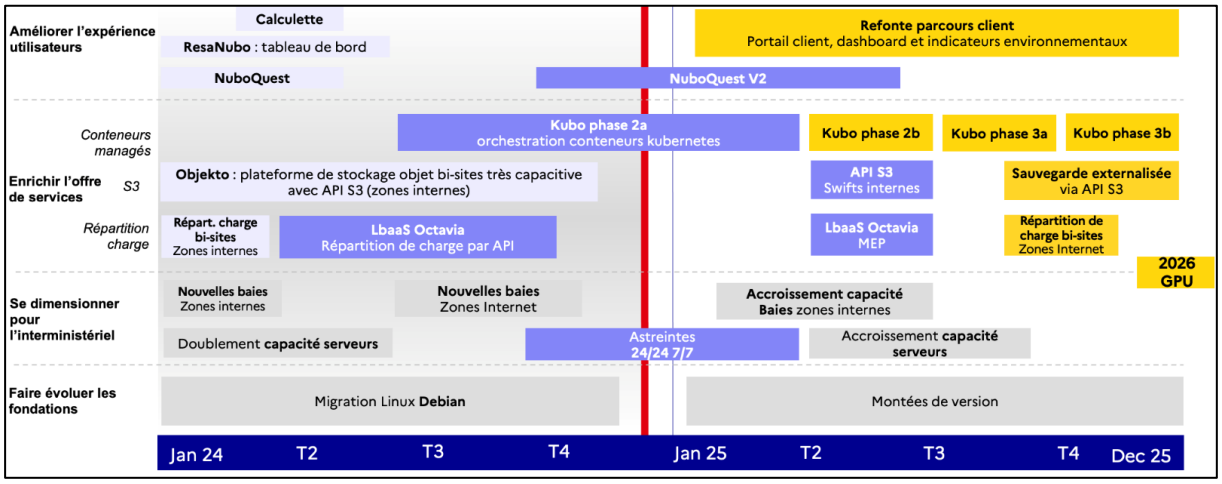
Graphique n° 4 : dispositions du I et du II de l'article 31 de la loi SREN



Source : Cour des comptes

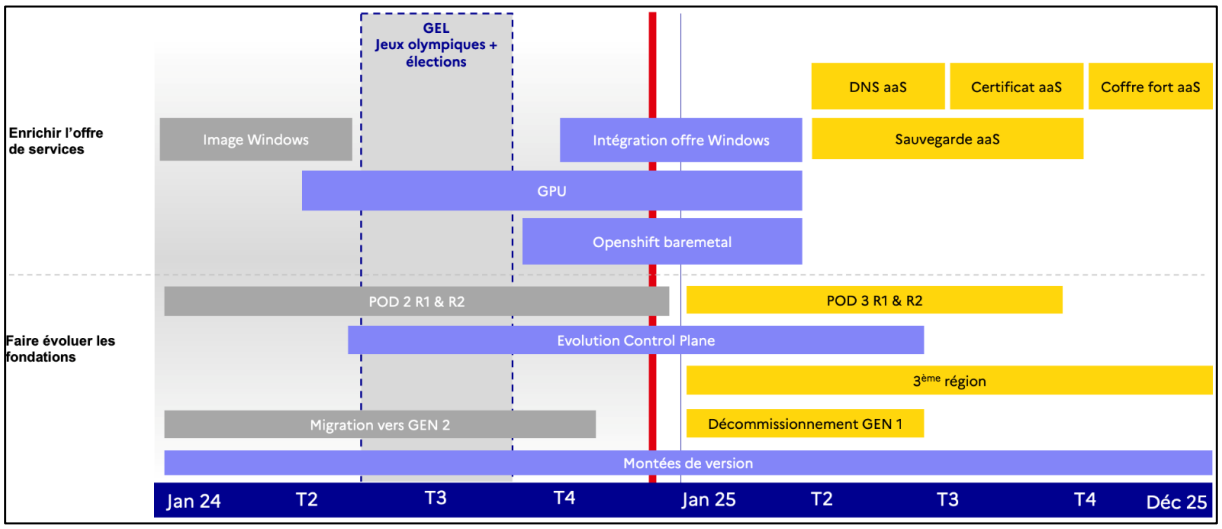
Annexe n° 3. Feuilles de route pour 2025 des *clouds* Nubo et Pi

Graphique n° 5 : feuille de route pour 2025 de Nubo



Source : DINUM

Graphique n° 6 : feuille de route pour 2025 de Pi



Source : DINUM

Annexe n° 4. Procédure d'accès au système national des données de santé

Par principe, toute personne ou structure, publique ou privée, à but lucratif ou non lucratif, peut accéder aux données du SNDS sur autorisation de la Cnil, en vue de réaliser un traitement de données présentant un intérêt public.

Pour des projets de recherche, les demandes sont à déposer auprès de la PDS. Elle est le point d'entrée unique des demandes d'autorisation d'accès au SNDS à des fins de recherche, étude ou évaluation, avec pour mission d'assurer un traitement des demandes conformément au cadre réglementaire et dans les délais définis par la loi.

La PDS assure également le secrétariat du comité éthique et scientifique pour les recherches, les études et les évaluations (Cesrees), un comité indépendant chargé d'examiner les demandes du point de vue méthodologique, afin de fournir un avis à la Cnil sur la cohérence entre la finalité de l'étude proposée, la méthodologie présentée et le périmètre des données auxquelles l'accès est demandé.

Pour certaines organisations chargées d'une mission de service public, une procédure spécifique d'accès au SNDS est prévue : ces organisations, listées par décret en conseil d'État pris après avis de la Cnil, peuvent pour accomplir leurs missions en accédant à certaines données de manière permanente. C'est par exemple le cas pour l'agence santé publique France, l'agence nationale de sécurité du médicament et des produits de santé, la Haute Autorité de santé, les chercheurs des CHU, des centres de lutte contre le cancer et de l'Inserm, l'agence de biomédecine ou encore les agences régionales de santé.

Annexe n° 5. Chronologie des textes et contentieux juridiques autour de l'hébergement des données de la plateforme des données de santé

Un collectif d'associations a contesté en justice un arrêté du 21 avril 2020 ayant confié à la PDS une mission consistant à croiser des données relatives à l'épidémie et requérant, après avis de la Cnil et publication d'un la mise en œuvre de procédures de pseudonymisation protéger les données personnelles, au motif d'un risque de transfert de données hors de l'UE.

Si le Conseil d'État a rejeté ce recours en référé le 19 juin 2020, la CJUE a, par son arrêt dit « Schrems II » du 16 juillet suivant, invalidé le régime de transfert de données entre l'UE et les États-Unis. L'arrêt de la CJUE a été rendu en considérant que la législation américaine (Section 702 Fisa, *Executive Order* 12 333 et *Cloud Act* adopté en 2018) permet l'accès, par les services de renseignements américains, aux données traitées par tout opérateur américain, qu'elles soient stockées aux États-Unis ou non (accessibles à distance ou durant leur transit vers leur territoire) : la Cour a jugé les garanties insuffisantes en termes d'exercice des droits des personnes et de sanctions possibles des atteintes par une autorité extérieure à l'UE.

Par une ordonnance du 13 octobre 2020 rendue dans le cadre d'un contentieux analogue, le Conseil d'État n'a pas relevé d'illégalité grave et manifeste justifiant la suspension immédiate du traitement des données par la PDS, a rappelé « l'absence de solution technique alternative satisfaisante » pour mener à bien les projets recourant à la plateforme.

Le ministre de la santé et le secrétaire d'État au numérique ont alors fait part de leur intention d'examiner des solutions alternatives recourant à un hébergeur de droit européen.

En février 2021, le conseil de la Cnam a rendu un avis réservé sur le projet de décret relatif au traitement de données à caractère personnel dénommé « système national des données de santé » en application de la loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé qui a créé la PDS. Le conseil soulignait que les conditions juridiques nécessaires ne semblaient pas réunies pour confier la base principale du SNDS à une entreprise non soumise exclusivement au droit européen pour la protection des données personnelles de santé. Dans l'attente d'un dispositif souverain soumis au RGPD, il a souhaité que la mise à disposition de la PDS des données soit limitée aux recherches, à la prévention, au traitement et à la prise en charge de la Covid 19.

L'association InterHop a saisi le Conseil d'État d'une demande d'annulation pour excès de pouvoir du décret précité. Cette requête a été rejetée avant la prise d'une nouvelle décision d'adéquation par la Commission européenne.

Comme elle l'a indiqué dans sa délibération n° 2020-106 du 29 octobre 2020, la Cnil *« s'inquiète […] de la duplication d'une base comportant, par nature, des données sensibles couvrant l'ensemble de la population. En effet, cette duplication implique de transférer régulièrement un grand volume de données entre la Cnam et la PDS, ainsi que de partager des identifiants pseudonymisés ; en outre, la Commission rappelle que la PDS ne dispose pas – contrairement à la Cnam – de ses propres centres de données et fait appel à un prestataire dans un centre de données mutualisé avec plusieurs clients. Elle rappelle que ces différentes opérations augmentent mécaniquement la surface d'attaque et les risques de violations sur ces données »*.

Cette doctrine de la Cnil est concordante avec l'approche retenue par les pouvoirs publics à propos des conditions d'accès aux données personnelles dans le contexte du recours

à l'informatique en nuage (*cloud computing*). C'est ainsi que les circulaires du Premier ministre du 5 juillet 2021 arrêtant la doctrine d'utilisation de l'informatique en nuage par l'État (« Cloud au centre ») et celle du 31 mai 2023 actualisant cette doctrine imposent une qualification SecNumCloud (ou une qualification européenne d'un niveau au moins équivalent) immunisée contre toute réglementation extracommunautaire en cas de recours à une offre de *cloud* commerciale pour le maniement de données d'une sensibilité particulière telles que les données personnelles.

Le 10 juillet 2023 et après que le président des États-Unis a adopté un décret présidentiel destiné à renforcer les garanties concernant la collecte et l'utilisation des données personnelles par les services de renseignement américains, la Commission européenne a adopté une décision d'adéquation constatant que les États-Unis assurent un niveau de protection substantiellement équivalent à celui de l'UE, ouvrant la possibilité, sous certaines conditions, de transférer des données personnelles vers ce pays, sans exigences supplémentaires.

Néanmoins, la doctrine de la Cnil, reflétant celle du Comité européen de protection des données (CEPD), identifie comme facteur de risque, outre les transferts de données à proprement parler, la situation dans laquelle les juridictions ou les autorités exécutives (notamment des services de renseignement) étrangères peuvent se faire communiquer des données, même si elles sont hébergées sur le territoire de l'UE : cette dernière situation se présente notamment lorsque le prestataire est une filiale d'un groupe américain.

Annexe n° 6. Liste des sigles

AIFE ..... Agence pour l'informatique financière de l'État
Anssi ..... Agence nationale de la sécurité des systèmes d'information
API ..... Application Programming Interface
AWS ..... Amazon Web Services
CASD ..... Centre d'accès sécurisé aux données
Cinum ..... Comité interministériel du numérique
CJUE ..... Cour de justice de l'Union européenne
Cnam ..... Caisse nationale de l'assurance maladie
Cnil ..... Commission nationale de l'informatique et des libertés
Cosinum ..... Comité d'orientation stratégique interministériel du numérique
CSP ..... *Cloud Service Provider*
DAE ..... Direction des achats de l'État
Daj ..... Direction des affaires juridiques
DGFiP ..... Direction générale des finances publiques
DNS ..... Délégation au numérique en santé
DNUM ..... Direction du numérique
Dinum ..... Direction interministérielle du numérique
ETP ..... Équivalent temps plein
EUCS ..... *European Union Cybersecurity Certification Scheme for Cloud Services*
Fisa ..... *Foreign Intelligence Surveillance Act*
FSSI ..... Fonctionnaire de sécurité des systèmes d'information
Gafam ..... Google (Alphabet), Apple, Facebook (Meta), Amazon et Microsoft
GPU ..... *Graphics Processing Unit*
HDS ..... Hébergeur de données de santé
IA ..... Intelligence artificielle
Iaas ..... *Infrastructure-as-a-service*
INDS ..... Institut national des données de santé
Inserm ..... Institut national de la santé et de la recherche médicale
MEN ..... Ministère de l'éducation nationale
Micaf ..... Mission interministérielle de lutte contre la fraude
MINT ..... Ministère de l'intérieur
Odice ..... Ordinateurs commandés par l'État

OMC..... Organisation mondiale du commerce

Paas..... *Platform-as-a-service*

PDS..... Plateforme des données de santé

Piste ..... Plateforme d'intermédiation des services pour la transformation de l'État

PME..... Petites et moyennes entreprises

PMSI..... Programme de médicalisation des systèmes d'information

PSSIE ..... Politique de sécurité des systèmes d'information de l'État.

Renater ..... Réseau national de télécommunications pour la technologie, l'enseignement et la recherche

RGPD ..... Règlement général sur la protection des données

RGS ..... Référentiel général de sécurité

RIE ..... Réseau interministériel de l'État

Saas..... *Software-as-a-service*

SI ..... Système d'information.

SICE ..... Système d'information et de communication de l'État

SIRH..... Système d'information de gestion des ressources humaines

SGDSN..... Secrétariat général pour la défense et la sécurité nationale

SNDS..... Système national des données de santé

SNIIRAM ..... Système national d'information inter-régimes de l'assurance maladie

SREN..... Sécuriser et réguler l'espace numérique.

UE..... Union européenne

Ugap ..... Union des groupements d'achats publics