ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Compte rendu

Commission d'enquête sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France

Jeudi
7 mai 2026
Séance de 9 heures

Compte rendu n° 39

SESSION ORDINAIRE DE 2025-2026

Présidence de
M. Aurélien Taché,
secrétaire de la commission

ASSEMBLÉE NATIONALE

La séance est ouverte à neuf heures cinq.

M. Aurélien Taché, président. Notre commission se préoccupe de la question de la souveraineté numérique et, en particulier, des risques que les solutions numériques proposées par des États étrangers peuvent faire peser sur notre souveraineté. Elle a déjà auditionné des directions des systèmes d'information (DSI) d'autres administrations et nous souhaitions poursuivre ces échanges avec la DGFIP, qui gère le système d'information fiscal avec un cloud souverain propriétaire, Nubo, ainsi qu'avec la gendarmerie, qui se situe également au cœur des missions de l'État et a développé une culture numérique indépendante en s'appuyant sur le logiciel libre. Cette approche ne se retrouve pas dans d'autres ministères en charge de la sécurité, je pense par exemple aux accords qui peuvent interroger, comme celui de la direction générale de la sécurité intérieure (DGSI) avec Palantir.

Pourriez-vous tout d'abord nous présenter les spécificités des systèmes d'information (SI) que vous gérez au regard des enjeux de souveraineté et de vulnérabilités technologiques ?

Je vous remercie de nous déclarer tout intérêt public ou privé susceptible d'influencer vos déclarations. Je vous rappelle également que l'article 6 de l'ordonnance du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires impose aux personnes auditionnées par une commission d'enquête de prêter serment de dire la vérité, toute la vérité, rien que la vérité. Je vous invite donc à lever la main droite et à dire « Je le jure ».

(M. Tomasz Blanc et le général de corps d'armée Marc Boget prêtent serment.)

M. Tomasz Blanc, chef du service des systèmes d'information de la direction générale des finances publiques (DGFIP). En matière numérique, la souveraineté constitue effectivement un enjeu stratégique majeur. Historiquement dominé par des acteurs américains, ce domaine a longtemps imposé un arbitrage entre performance et souveraineté, ce dernier critère s'étant largement imposé ces dernières années. Le système d'information de la DGFIP, fort de 795 applications, sert 95 000 agents ainsi que l'ensemble des usagers et entreprises. En interface avec toutes les administrations pour les questions financières, notre direction se distingue par une imbrication totale entre le numérique et des métiers, mais également par la manipulation de données d'une grande sensibilité, plaçant la sécurité au cœur de nos priorités.

Compte tenu de l'ancienneté de notre système, des dépendances extra-européennes subsistent, que nous nous efforçons de maîtriser et de réduire. Nos principales dépendances concernent les infrastructures matérielles, avec IBM et Oracle, quasi exclusivement produites en Asie et aux États-Unis à défaut de solutions européennes complètes. Nous activons toutefois les leviers de la concurrence dans l'acquisition des matériels et des marchés afin de maîtriser au mieux ces dépendances. S'agissant d'IBM, notre dépendance est héritée des années quatre-vingt, à l'image des serveurs IBM Z, qui supportent encore nos applications historiques de calcul de l'impôt ou d'échanges bancaires. Bien que fiables et performants, ces systèmes sont coûteux (4,5 millions d'euros en 2025) et en sortir s'avère complexe. La migration d'applications écrites en Cobol (*Common Business-Oriented Language*) vers des logiciels libres exige en effet des projets longs et des tests rigoureux, comme l'illustre la refonte progressive de la paie des fonctionnaires d'État. Cette complexité structurelle limite d'ailleurs notre capacité de négociation contractuelle. Quant à Oracle, sur lequel s'appuient encore de nombreuses applications, notre dépendance date du début de l'ère web, époque où cet éditeur

s’imposait pour la fiabilité des bases de données. Oracle, qui représente 8,5 millions d’euros annuels, équipe notamment la déclaration en ligne des revenus et la comptabilité locale. Là encore, la richesse fonctionnelle de ces outils rend leur remplacement long et onéreux.

Si ces dépendances sont avérées, elles diminuent donc au fil du temps. À noter que notre exposition aux Gafam reste limitée, puisque seul le système d’exploitation des postes de travail dépend de Microsoft. Nous n’utilisons ni la suite Office ni Active Directory et, grâce à nos choix technologiques dans le cloud, nous avons su éviter toute nouvelle dépendance envers les *hyperscalers* américains.

S’agissant des leviers que nous employons pour progresser en souveraineté, ils sont au nombre de quatre : le recours au logiciel libre, l’appui sur nos forces internes pour la maitrise et la fabrication de nos systèmes d’information, la standardisation de la fabrication et, enfin, une réflexion stratégique sur le long terme.

Le logiciel libre constitue le pilier central de cette démarche. Depuis les années 2000, l’émergence de solutions matures (telles que Linux pour les systèmes d’exploitation ou PostgreSQL pour les bases de données) offre des performances comparables aux produits propriétaires. Pour pallier l’absence de support éditeur, nous avons structuré dès 2005 un marché de support devenu interministériel s’appuyant sur des entreprises françaises spécialisées. Cette approche nous garantit une expertise de haut niveau et une correction réactive des bogues, pour un coût nettement inférieur aux licences classiques. Les résultats concrets valident ce choix puisque depuis 2010, la priorité est systématiquement donnée au logiciel libre pour tout nouveau projet. C’est le cas du prélèvement à la source, dont la brique de collecte des revenus est intégralement libre. Cette stratégie a permis de réduire notre parc Oracle et de limiter l’influence de Microsoft, en privilégiant LibreOffice et Samba. Pour ce dernier outil, un investissement de 1,5 million d’euros dans l’amélioration du code source nous a évité des millions d’euros de redevances annuelles. Cependant, le libre impose une rigueur interne accrue car s’il favorise l’écosystème économique français, il offre parfois une ergonomie ou des fonctions collaboratives moins abouties que des suites comme Office 365. Cela exige un effort constant de pédagogie auprès de nos agents et une discipline technique pour ne pas s’égarer dans un écosystème trop foisonnant.

Le deuxième levier réside dans la maîtrise de nos forces internes pour le SI. Avec un corps de 5 000 informaticiens, nous limitons l’externalisation pour protéger le caractère stratégique de nos missions. Chaque projet est ainsi piloté par une équipe noyau de la DGFIP qui assure la conception et l’architecture, ne déléguant que l’exécution technique sous une surveillance étroite. Cette philosophie a guidé notre transition vers le cloud. Face aux risques posés par les lois extraterritoriales américaines, nous avons refusé les offres des grands acteurs étrangers pour développer Nubo, notre cloud interne interministériel. Conçu à partir de logiciels libres et exploité par nos propres agents, Nubo héberge aujourd’hui 25 % de notre SI. Bien que moins riche en fonctionnalités que les solutions des *hyperscalers* américains, il garantit la sécurité absolue du secret fiscal et nous force à une sobriété technologique bienvenue, en nous concentrant sur les besoins essentiels.

Le troisième levier est la standardisation de la fabrication applicative. En imposant des normes strictes, nous facilitons la réversibilité technique, c’est-à-dire notre capacité à quitter un prestataire si un risque émerge. Cette discipline est essentielle puisqu’en évitant d’utiliser les fonctions trop spécifiques des produits propriétaires, comme les optimisations exclusives d’Oracle, nous reprenons l’ascendant lors des négociations commerciales. Cette méthode nous

a déjà permis de sortir presque totalement d'Oracle sur le périmètre de la fiscalité des entreprises.

Enfin, le dernier levier est celui de la constance stratégique sur le long terme. La souveraineté numérique ne se décrète pas, elle se construit sur des décennies. Notre bascule vers le libre a été amorcée il y a vingt ans. Déconstruire des dépendances héritées de systèmes quarantenaires, tout en intégrant chaque année les évolutions des lois de finances, impose une stratégie immuable. La réussite de ce chantier dépendra de notre capacité à maintenir cette priorité et à poursuivre la montée en compétence technique de nos équipes sur le très long terme.

M. le général de corps d'armée Marc Boget, directeur de l'agence du numérique des forces de sécurité intérieure (Anfsi). Mon propos liminaire portera sur ce qui constitue, à mes yeux, une urgence absolue : la souveraineté numérique comme pilier de nos forces de sécurité intérieure.

L'Anfsi, qui assure la direction des systèmes d'information pour la police et la gendarmerie nationales, s'appuie sur 530 agents en administration centrale, renforcés par 100 développeurs et environ 200 personnels dédiés à l'exploitation de 5 000 serveurs répartis sur nos *data centers* de Rosny-sous-Bois et de Nogent-sur-Marne. À mon sens, la souveraineté numérique ne se négocie pas mais s'impose comme une nécessité vitale pour protéger notre démocratie. Sans la maîtrise de nos outils, l'indépendance de l'action publique, principe compris depuis longtemps par la gendarmerie, ne peut subsister. Cette souveraineté est devenue la condition *sine qua non* de la continuité de l'État et de la protection de nos libertés individuelles, comme l'illustrent trois enjeux majeurs.

Le premier est le risque d'extraterritorialité : le Cloud Act américain nous rappelle que confier nos données à des tiers revient à accepter que les justices étrangères puissent s'immiscer dans nos dossiers judiciaires et nos fichiers de police. Sans souveraineté technique et physique sur nos serveurs, le secret de nos enquêtes est directement menacé par des intérêts divergeant des nôtres.

Le deuxième enjeu concerne la fragilité de la chaîne d'approvisionnement logiciel. Moins nous maîtrisons cette chaîne, plus nous nous exposons à des défaillances critiques. L'incident CrowdStrike de 2024, où une mise à jour défectueuse a paralysé 8,5 millions d'ordinateurs, démontre qu'un tel accident constituerait, pour la police et la gendarmerie, une rupture grave de la protection des populations. C'est pour parer à cette vulnérabilité que le choix du logiciel libre et la maîtrise interne du code source sont vitaux.

La troisième illustration réside dans l'usage du numérique comme arme dans les conflits hybrides. L'exemple de l'Ukraine montre que des coupe-circuits logiciels peuvent servir d'outils de coercition. Au début du conflit, l'attaque contre le réseau Viasat, par l'introduction d'un virus dans les modems, a paralysé une partie des armées ukrainiennes et neutralisé des milliers d'éoliennes en Allemagne. Sans autonomie totale sur ses systèmes de commandement, la France s'expose à un risque de neutralisation à distance en cas de tensions géopolitiques majeures. Être souverain, c'est garantir que seul l'État français conserve le contrôle de l'interrupteur de ses propres SI.

La gendarmerie nationale a été précurseur en opérant, dès le début des années 2000, un virage stratégique vers Linux pour ses serveurs et ses postes de travail. Ce choix du logiciel libre visait à rompre avec les dépendances aux éditeurs étrangers pour garantir l'intégrité de nos systèmes et redevenir maîtres de notre destin numérique et financier. Aujourd'hui, nous ne

possédons plus aucun serveur Windows et seuls 1 054 postes sur 80 000 conservent ce système pour des besoins de niche très spécifiques. De la même façon, nous achevons notre sortie d'Oracle au profit de bases de données libres comme PostgreSQL. Nous nous intégrons en outre activement aux communautés open source selon un modèle d'accord gagnant-gagnant où nos développements profitent également à tous.

Ce système repose sur une intégration forte entre les outils techniques et le modèle humain de la gendarmerie puisque, depuis 30 ans, nous cultivons une filière d'experts qui alternent entre-temps de missions de terrain et spécialisation technique. Cette polyvalence permet à nos officiers et sous-officiers de concevoir des outils parfaitement adaptés aux réalités opérationnelles. Pour anticiper les besoins futurs, nous formons chaque année nos cadres dans de grandes écoles. À titre d'exemple, j'ai envoyé des officiers se former sur le quantique dès 2023 pour préparer l'horizon 2030.

L'internalisation de ces compétences garantit la maîtrise permanente de nos systèmes critiques. Mon premier principe est de ne jamais déléguer le pilotage de nos outils et si nous recourons ponctuellement à des prestataires extérieurs français, c'est toujours sous la direction d'un noyau dur interne. Je dois être capable, à tout moment, de changer d'industriel sans fragiliser l'institution. Mon second principe concerne la conservation des données dans des *data centers* souverains. Comme un trésor que l'on protège, nos données sensibles ne sortent jamais de nos centres car même un SecNumCloud ne peut offrir les garanties de sécurité que procure une exploitation directe par des gendarmes au sein de nos propres casernes. Actuellement, nous exploitons deux *data centers* et construisons une troisième région pour le cloud Pi, le second cloud interministériel avec Nubo.

Face à des vulnérabilités mondiales de plus en plus fréquentes et rapidement exploitées, détenir tous les leviers de contrôle est une nécessité absolue. Ce modèle d'autonomie exige toutefois des ressources humaines conséquentes. La nouvelle grille salariale de la direction interministérielle du numérique (Dinum) est, à cet égard, un progrès majeur pour recruter rapidement dans un secteur privé très concurrentiel.

En conclusion, je tiens à souligner que ce combat exige une vigilance de chaque instant. Nous concentrons nos efforts sur la modularité de nos systèmes d'information afin de pouvoir remplacer n'importe quel composant sans en fragiliser l'ensemble, tout en définissant un cadre de cohérence technique pour standardiser nos développements. Il faut toutefois reconnaître que certains volets, tels que les routeurs, le matériel, les processeurs ou certains logiciels dont l'offre open source manque encore de maturité, ne sont pas totalement couverts. Dans ces cas précis, je m'efforce de mitiger le risque en diversifiant les solutions pour ne jamais dépendre d'un acteur unique. À ce titre, nous participons activement aux travaux collaboratifs menés avec les autres ministères, la Dinum et l'écosystème européen, notamment à travers le programme Impact. Ma priorité absolue demeure d'éviter toute impasse technologique, et j'ai la chance de bénéficier de la confiance de mes deux directeurs généraux, qui s'inscrivent pleinement dans cette dynamique et m'octroient les moyens humains et financiers nécessaires à cette ambition.

M. Aurélien Taché, président. Vous avez tous deux abordé la question des lois américaines à portée extraterritoriale, notamment le Cloud Act, et souligné la menace qu'elles représentent pour notre souveraineté. Il est rassurant d'apprendre que des institutions aussi éminentes que la DGFIP et la gendarmerie nationale sont propriétaires de leur propre cloud. Mon général, vous avez d'ailleurs précisé que, même pour vos données sensibles hébergées, vous privilégiez systématiquement des solutions non américaines.

Ma première interrogation porte sur le traitement des données dites non sensibles : le recours à des prestataires américains est-il envisageable pour ce type d'informations et, le cas échéant, selon quels critères distinguez-vous les données sensibles de celles qui ne le sont pas ?

Ma seconde question vise à comparer vos deux modèles, dont le haut niveau d'intégration prouve qu'il est possible de s'affranchir des grands fournisseurs de cloud, aux solutions bénéficiant du visa SecNumCloud. Ces dernières, parfois moins intégrées, ne risquent-elles pas de fragiliser notre souveraineté ?

M. le général de corps d'armée Marc Boget. La règle que j'applique est simple : dès qu'une donnée est sensible, ce que je détermine grâce au repère infaillible que constitue la déclaration de tous mes SI auprès de la Commission nationale de l'informatique et des libertés (Cnil), souvent accompagnée d'un décret en Conseil d'État, elle demeure strictement au sein de nos infrastructures. Pour les données non sensibles, notamment celles destinées à être ouvertes à nos concitoyens, j'utilise actuellement une solution imparfaite consistant à les héberger à l'extérieur. Pour protéger mes données sensibles, j'ai instauré un barrage interdisant toute intrusion dans mon système interne depuis l'extérieur. Toutefois, ce dispositif devient inopérant lorsqu'il s'agit d'interagir avec les usagers, ces derniers n'ayant pas de droit d'accès. J'utilise donc un point applicatif externe, hébergé chez un prestataire rigoureusement sélectionné, où je viens recueillir les données pour les rapatrier. Ce processus repose sur une coupure protocolaire permanente, évitant ainsi tout lien direct avec mes systèmes internes.

Concernant les nouvelles applications en cours de développement, qui s'appuient sur le cloud public pour la partie *front*, nous expérimentons différentes options, notamment des solutions bénéficiant du visa SecNumCloud proposées par certains hébergeurs du nord de la France, afin d'arrêter le choix le plus éclairé possible.

Si je ne confie pas de données sensibles à un cloud qualifié SecNumCloud, c'est pour une raison bien précise. Bien que ce label de l'Agence nationale de la sécurité des systèmes d'information (Anssi) résulte d'un travail remarquable pour se prémunir du Cloud Act américain, il m'ôte la maîtrise des opérateurs exploitant les serveurs. Un environnement SecNumCloud est en effet géré par des salariés du secteur privé dont je ne peux surveiller l'activité en permanence. Or face au coût mondial de la cybercriminalité, estimé à plus de 10 500 milliards de dollars en 2025, la réalité de la corruption ne peut être ignorée. Une telle menace exige que les agents soient soit étroitement contrôlés, soit totalement insensibles à la pression économique. Dès lors que les serveurs ne sont pas hébergés et administrés par des gendarmes, je ne peux plus garantir ni surveiller l'intégrité des opérations, ce qui justifie mon refus d'y déposer la moindre donnée sensible.

M. Tomasz Blanc. En pratique, la quasi-totalité de nos données, même non sensibles, est hébergée en interne dans nos propres centres de données. Le recours aux Gafam demeure tout à fait exceptionnel et ne concerne que des données publiques, comme c'est le cas pour l'exploitation de photos aériennes au sein de notre SI.

Comme je l'ai précédemment souligné, la standardisation constitue un enjeu majeur, car multiplier les filières d'hébergement et de fabrication engendre des coûts importants. Notre SI traitant très majoritairement des données sensibles, qu'elles soient fiscales ou personnelles, tant pour les particuliers que pour les professionnels, nous ne souhaitons pas développer de filière spécifique pour les rares applications qui n'en contiendraient pas. Nous privilégions une standardisation massive en maintenant ces applications sur les architectures et les filières utilisées pour le reste de nos activités.

S’agissant de la comparaison entre nos infrastructures internes et les solutions SecNumCloud, je précise que ce label s’adresse prioritairement aux offres commerciales. Néanmoins, lors des procédures d’homologation de notre cloud Nubo, nous intégrons les règles de sécurité technique de ce référentiel, auxquelles nous ajoutons les exigences de la politique de sécurité des systèmes d’information de l’État (PSSI-E). En matière de sécurité, le cloud Nubo se situe donc au même niveau, sinon au-delà, des offres SecNumCloud. Comme l’évoquait le général Boget, la différence réside dans le fait que nos infrastructures sont exploitées par des agents de la DGFIP, contrôleurs ou inspecteurs des finances publiques. Nous assurons ainsi une maîtrise de bout en bout, de l’intégration du logiciel à l’exploitation par nos agents, jusqu’à l’hébergement au cœur de nos propres centres de données.

Mme Cyrielle Chatelain, rapporteure de la commission d’enquête sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l’indépendance de la France. Mes premières interrogations concernent la gestion des compétences et l’évolution de vos effectifs. Pourriez-vous nous préciser si vos équipes s’étoffent ou si elles se maintiennent à un niveau constant, et dans quelle mesure cette dynamique a transformé votre politique de recrutement ? Certains témoignages suggèrent que l’usage du logiciel libre valorise des savoir-faire spécifiques : cela a-t-il orienté vos critères d’embauche ou privilégiez-vous plutôt la formation interne des agents recrutés ? Par ailleurs, vous avez mentionné l’importance de l’indépendance à travers la notion de taux d’externalisation. Disposez-vous de seuils d’alerte précis vous permettant de qualifier une situation d’acceptable, de préoccupante ou de critique pour la sécurité de vos services ?

Ma seconde question porte sur la transition des solutions propriétaires vers le logiciel libre, un processus que vous avez décrit comme long et onéreux. Pourriez-vous nous éclairer sur les délais et les coûts engendrés, en vous appuyant sur un ou deux cas concrets ? La gendarmerie nationale nous offrant l’opportunité d’une analyse sur le temps long, estimez-vous, avec le recul nécessaire, que les investissements consentis sont aujourd’hui rentabilisés ?

M. le général de corps d’armée Marc Boget. Sur les recrutements, la gendarmerie investit dans ce domaine depuis 1987, date de création de la sous-direction des télécommunications et de l’informatique. Notre politique en la matière n’a donc pas été bouleversée, car elle intègre cette dimension de longue date. Nous avons toujours privilégié un pluralisme de profils : anciens sous-officiers, officiers issus des grandes écoles militaires ou recrutés sur titres après une expérience dans le privé, et diplômés de niveau bac+5 par voie de concours universitaire. Cette adaptation permanente me permet, en tant que responsable de filière, d’anticiper les besoins en volumes et en compétences à un horizon de trois ans.

Un aspect fondamental de notre stratégie d’internalisation réside dans le refus d’une filière exclusivement numérique. Un ingénieur ne rejoindra pas la gendarmerie pour y exercer les mêmes missions que dans le secteur privé, où les rémunérations sont plus attractives. Ce qui motive ces personnels et garantit leur fidélité, c’est la perspective d’une carrière alternant des fonctions techniques et opérationnelles. Ce modèle, qui offre à la fois du sens et une visibilité sur la trajectoire professionnelle, est notre meilleur rempart contre la rotation des effectifs, alors même que ces profils sont très courtisés par le marché.

Quant au passage au logiciel libre, initié il y a vingt ans, la transition fut conduite avec une rigueur toute militaire, peut-être un peu brusque, mais elle s’est accomplie en trois ans sans heurts majeurs. Aujourd’hui, l’exercice est bien plus aisé puisque l’environnement Linux et la suite LibreOffice sont devenus si conviviaux que même les recrues formées aux outils Microsoft s’y adaptent sans difficulté.

Enfin, sur le plan financier, nous avons évalué les économies générées par cette stratégie, qu'il s'agisse des postes de travail ou de nos smartphones professionnels, équipés d'un système d'exploitation souverain. Ce choix technique nous protège d'ailleurs efficacement : les téléphones des directeurs généraux de la gendarmerie et de la police nationales ont ainsi été préservés de l'infiltration par le logiciel Pegasus. Depuis 2004, ces dépenses évitées s'élèvent précisément à 534 millions d'euros. Dans un contexte de budgets contraints, c'est un argument de poids.

M. Tomasz Blanc. Les effectifs de la DGFIP comptent 5 000 informaticiens. Le nombre total d'agents de la direction a significativement diminué depuis 2008, passant de 130 000 à 95 000, et l'outil numérique a largement contribué à cette réduction. Toutefois, depuis la mise en œuvre du prélèvement à la source, la DGFIP a adopté une véritable stratégie de priorisation du numérique et, depuis 2020, nous avons stabilisé puis renforcé nos moyens, alors même que le reste de la direction subissait encore des suppressions d'emplois. Ce choix affirmé démontre que le numérique est devenu un levier stratégique pour nos métiers financiers. En matière de pilotage, le taux d'externalisation moyen de la DGFIP s'établit à 40 %. Bien que ce chiffre soit conforme aux normes de la Dinum, qui fixent le seuil de risque au-delà de 60 %, certains de nos projets dépassent localement cette limite. Concernant le recrutement, si le concours spécialisé demeure notre voie d'accès privilégiée, l'importance des départs à la retraite nous conduit, depuis 2020, à solliciter davantage de contractuels. Cela a permis de diversifier nos profils tout en capitalisant sur l'attractivité de nos missions, sur notre culture du logiciel libre et sur la maîtrise de nos projets, des arguments forts face à la concurrence du secteur privé.

Bien que nous n'ayons pas réalisé d'étude sur les coûts évités grâce au logiciel libre, l'exemple de LibreOffice est révélateur puisque son coût annuel est quasi nul là où une suite propriétaire reviendrait à environ 10 millions d'euros par an. Pour un usage courant, nos enquêtes annuelles de satisfaction révèlent que les agents jugent ces deux solutions équivalentes. Si nous nous autorisons l'achat ponctuel de licences Microsoft pour des besoins d'expertise spécifiques, la généralisation de LibreOffice garantit notre résilience puisqu'en cas de défaillance du fournisseur privé, la continuité de service serait assurée pour tous.

Le déploiement d'outils libres exige toutefois une conduite du changement rigoureuse. LibreOffice est désormais parfaitement intégré depuis 2015 grâce à un effort soutenu de pédagogie, et nous étudions maintenant la possibilité de basculer vers des systèmes Linux. Malgré les progrès des distributions libres, l'écart avec Windows persiste et un tel déploiement nécessitera donc une préparation minutieuse pour vaincre les résistances prévisibles.

Mme Cyrielle Chatelain, rapporteure. Pour le déploiement sur Linux, avez-vous une idée du calendrier et de la manière dont vous vous préparez à l'accompagnement ?

Ma deuxième question porte sur les marchés publics. Vous avez mentionné le développement de marchés de support dédiés aux logiciels libres ainsi que l'intégration d'exigences spécifiques dans vos cahiers des charges. Or il ressort de nos auditions que le code de la commande publique ne permet pas systématiquement de privilégier des solutions françaises ou européennes. Pourriez-vous nous préciser les critères de vigilance que vous retenez pour sélectionner les prestataires les plus fiables et les mieux protégés contre les lois extraterritoriales ? Par ailleurs, comment s'articule votre collaboration avec les plateformes d'achat de l'État ? Observez-vous une évolution de ces marchés vers une meilleure prise en compte de vos besoins ?

M. Tomasz Blanc. Sur la question de Linux, je précise qu'avant d'engager la conduite du changement, nous devons valider plusieurs préalables techniques. Sur un parc comptant entre 110 000 et 115 000 postes de travail, le défi ne réside pas tant dans l'installation de Linux que dans notre capacité à administrer l'ensemble de la flotte. Il est impératif de pouvoir diffuser rapidement des correctifs de sécurité et de déployer des logiciels à distance sans intervention physique. Actuellement, notre environnement Windows bénéficie d'une automatisation très poussée et nous devons nous assurer de disposer d'outils équivalents offrant le même niveau de performance, car nous ne pouvons nous permettre aucune régression de la productivité de notre support utilisateur. L'étude que nous menons cette année porte précisément sur ce point critique afin d'obtenir les garanties nécessaires avant toute décision.

S'agissant de la commande publique, force est de constater qu'elle a été conçue pour prévenir les risques de corruption et garantir l'efficacité de la dépense, plutôt que pour répondre aux enjeux de souveraineté. Si elle remplit efficacement ses objectifs initiaux, elle s'avère moins adaptée aux impératifs de souveraineté. Par conception, la DGFIP privilégie le logiciel libre et, tout comme la gendarmerie, nous assurons la maîtrise interne de nos projets grâce à nos propres équipes. Nous achetons ainsi principalement de la prestation de services qui, en France, provient majoritairement d'entreprises nationales ou de succursales locales. La difficulté réelle apparaît lors de l'achat de logiciels sur étagère : imposer des exigences de souveraineté dans ce cadre contractuel semble bien plus complexe, même si cette question mériterait l'expertise de spécialistes du droit de la commande publique.

M. le général de corps d'armée Marc Boget. À l'instar des services de Bercy, nous privilégions généralement la prestation d'expertise aux achats de produits sur étagère. Toutefois, lorsqu'un tel achat s'avère nécessaire, la situation est en effet complexe. Si le code des marchés publics n'est pas réputé pour sa souplesse, il nous permet néanmoins de mettre en avant certains critères auxquels nous sommes particulièrement vigilants, tels que la normalisation, le respect des standards, la réversibilité ou, lorsque cela est envisageable, l'audit du code source. En somme, nous nous efforçons d'intégrer un maximum d'exigences pour conserver une maîtrise optimale sur nos acquisitions.

Je précise que mon agence n'est pas directement responsable de la passation des marchés, cette mission incombant au service de l'achat, de l'innovation et de la logistique du ministère de l'intérieur (Sailmi). Mes équipes se chargent de la rédaction des cahiers des clauses techniques particulières (CCTP), et nous militons systématiquement pour que le critère technique bénéficie de la pondération la plus élevée possible. Un arbitrage est souvent nécessaire entre l'acheteur, dont l'objectif est d'accorder une importance prédominante au prix, et le technicien, qui souhaite privilégier la valeur technique pour garantir le bon fonctionnement du service. Afin de trouver ce compromis tout en gardant la main sur les orientations technologiques, nous exigeons systématiquement des garanties de réversibilité et de conformité aux normes impératives d'ouverture, ce qui permet d'écarter les solutions propriétaires. La sélection s'opère ensuite sur la base de la valeur technique lors de l'examen des offres. À cet égard, nous avons la chance de pouvoir compter en France sur des entreprises d'un très haut niveau, qui n'ont rien à envier à leurs concurrents américains.

M. Aurélien Taché, président. Vous avez tous deux parfaitement exposé les vertus des logiciels libres, qui sont à la fois moins onéreux, pratiques et simples d'utilisation. Vous avez également précisé que la gendarmerie utilise sur ses terminaux mobiles des systèmes d'exploitation indépendants, ce qui vous a préservés de l'espionnage par le logiciel Pegasus. Dès lors, pour quelles raisons les autres services de l'État ne franchissent-ils pas le pas ?

Je souhaite par ailleurs revenir sur le cas de la DGSI, car son partenariat avec Palantir, ainsi que l'utilisation de ce logiciel pour le traitement des données, sont particulièrement préoccupants. Cette entreprise, qui poursuit un agenda géopolitique, vient en effet de publier une sorte de « manifeste techno-fasciste ». Comment une telle situation a-t-elle pu s'instaurer ? Comment pouvons-nous en sortir et convaincre les autres administrations d'adopter vos solutions sans plus tarder ?

Ma dernière question porte sur l'intelligence artificielle. J'imagine que vous observerez la même prudence en évitant le recours à des logiciels tels que Claude, dont les liens avec certains acteurs technologiques posent question, ou d'autres outils de même nature. Il serait très éclairant de connaître votre position sur ce sujet.

M. le général de corps d'armée Marc Boget. S'agissant de l'intelligence artificielle, nous avons déjà déployé un modèle s'appuyant sur une plateforme souveraine. J'ai la chance de compter, parmi mes effectifs d'officiers de gendarmerie, des *data scientists* de haut niveau, grâce auxquels nous disposons d'une plateforme accessible aux policiers et aux gendarmes. Les données y sont totalement maîtrisées en interne et ne sont jamais externalisées vers des services tiers, ce qui constitue pour moi une exigence absolue. Notre infrastructure actuelle, qui utilise une IA développée en interne baptisée l'Agent, va prochainement migrer vers le modèle Génial du ministère des armées. Ce dernier a accompli un travail remarquable en développant une solution basée sur l'open source et un modèle communautaire, parfaitement adaptée aux besoins des forces de sécurité intérieure.

Quant à savoir pourquoi les autres administrations ne franchissent pas le pas vers Linux, je pense qu'il ne faut pas sous-estimer l'ampleur du défi que représente la conduite du changement. Un acteur comme Microsoft déploie une stratégie de lobbying extrêmement efficace dès le milieu scolaire, et cette approche n'a rien d'anodin puisqu'une personne formée exclusivement sur ces outils dès son plus jeune âge cherchera naturellement à les retrouver dans sa vie professionnelle. Cette habitude ancrée constitue un frein majeur au changement pour de nombreuses organisations. Nous observons toutefois une évolution notable à l'échelle internationale puisque de grandes municipalités, notamment en Allemagne, ainsi que des entreprises d'envergure, opèrent désormais une transition vers Linux. La Dinum vient par ailleurs de publier une distribution Linux dédiée au poste de travail, ce qui prouve que les lignes bougent, même si le processus est lent.

Sur le sujet de Palantir, je ne suis ni compétent ni en possession des informations nécessaires pour m'exprimer. Nous touchons là au domaine du renseignement et seule la DGSI pourrait vous répondre. Ce que je peux toutefois vous confirmer, c'est que les équipes techniques de la DSI sont constituées de personnes particulièrement intelligentes et responsables, dotées d'un haut niveau d'expertise, qui agissent rarement sans raison.

M. Tomasz Blanc. Sur la question de savoir pourquoi les autres administrations ne franchissent pas encore ce pas, je serais plus nuancé. L'ensemble des services de l'État que je côtoie a désormais engagé une démarche en faveur du logiciel libre, même si les rythmes et les contraintes diffèrent. Le modèle de la gendarmerie, où le poste de travail lui-même fonctionne sous Linux, représente un stade avancé qui exige d'avoir préalablement éliminé toute dépendance aux logiciels propriétaires. À la DGFIP, une telle généralisation était inenvisageable il y a dix ans, car certains de nos outils n'étaient compatibles qu'avec Windows. Depuis, ces logiciels ont été modernisés ou remplacés, ce qui nous permet aujourd'hui d'étudier sérieusement cette transition.

Ces transformations s'inscrivent nécessairement dans le temps long, car faire évoluer tout un système d'information pour gagner en souveraineté, notamment par le levier du logiciel libre, requiert environ une décennie. L'enjeu majeur, lors de chaque révolution technologique, est d'éviter de créer de nouvelles dépendances. L'intelligence artificielle en est l'exemple type : si l'apparition de ChatGPT a suscité un fort engouement, il faut garder le recul nécessaire pour comprendre que, sous l'angle de la souveraineté, le recours à un tel outil est exclu.

À la DGFIP, nous appliquons à l'IA le modèle de maîtrise interne que j'ai exposé. Nous nous appuyons sur nos propres *data scientists* et ingénieurs pour exploiter des modèles de langage libres sur nos propres puces GPU, hébergées dans nos centres de données. Cette infrastructure garantit que les données ne sortent jamais de nos murs et offre la flexibilité nécessaire pour changer de modèle aisément. Cette plateforme centralisée alimente déjà plusieurs cas d'usage, dont le plus visible est le nouveau moteur de recherche du site impots.gouv.fr, qui utilise l'IA pour améliorer la pertinence des résultats.

Je ne m'interdis pas, à l'avenir, d'intégrer des modèles de langage propriétaires tels que Mistral, à la condition impérative qu'ils soient suffisamment standardisés pour s'insérer dans notre architecture. Cela nous permettrait de bénéficier d'éventuels gains de performance tout en conservant la faculté de basculer à nouveau vers des modèles libres si la politique commerciale de l'éditeur ou les risques pour notre souveraineté l'exigeaient. Enfin, nous allons également étudier de près le modèle Génial du ministère des armées afin de déterminer s'il peut nous aider à accélérer nos propres travaux.

Mme Cyrielle Chatelain, rapporteure. Je souhaiterais désormais évoquer la question du *kill switch*, particulièrement pertinente pour des solutions hybrides comme celles développées par S3NS. Vous avez souligné en début d'audition qu'une faille est désormais exploitée dans un délai très court. Le risque lié au *kill switch* réside dans l'interruption brutale des mises à jour technologiques : le service ne s'arrête pas instantanément, mais les vulnérabilités ne sont plus corrigées. Compte tenu de la rapidité avec laquelle ces failles sont aujourd'hui exploitées, comment évaluez-vous le danger que représente cette absence de maintenance pour des solutions hybrides dont nous n'avons pas la pleine maîtrise technique ? Selon vous, combien de temps une telle solution peut-elle encore fonctionner de manière sécurisée une fois privée de ses mises à jour ?

M. le général de corps d'armée Marc Boget. Ces éléments nourriront la réflexion que j'ai engagée car il s'agit, très clairement, d'un sujet majeur. Pour S3NS, cet enjeu est central : le principe repose sur la détention des clés de chiffrement par un tiers, et non par le fournisseur de cloud, afin d'interdire à ce dernier tout accès physique aux données. Si cette garantie est appréciable, elle n'élude pas le risque qu'un arrêt des mises à jour de sécurité par Google ne rende le système rapidement obsolète et vulnérable. Avec 35 000 vulnérabilités découvertes cette année, rien ne laisse présager une baisse de cette menace à l'avenir. La capacité à parer ces failles constituera donc un point de vigilance essentiel de mon étude, pour lequel S3NS devra apporter des garanties incontestables.

M. Tomasz Blanc. Sur la question du *kill switch*, je n'ai pas encore approfondi le sujet, car la DGFIP n'envisage pas de recourir à ces solutions à brève échéance mais, pour l'instant, je reste dubitatif et n'ai pas trouvé d'arguments convaincants.

Mme Cyrielle Chatelain, rapporteure. Existe-t-il aujourd'hui une volonté de généraliser l'usage de Nubo et de Pi, qui sont des clouds interministériels ou, en tout cas, d'offrir la possibilité à d'autres ministères d'utiliser ces solutions ?

M. Tomasz Blanc. Ces solutions sont d'ores et déjà accessibles à l'échelon interministériel : le ministère de la culture s'appuie ainsi sur Nubo pour un service d'archivage, tout comme la Dinum qui l'utilise pour la solution ProConnect dédiée à l'authentification des agents et des professionnels. Une importante marge de progression subsiste toutefois dans leur adoption généralisée.

Il faut en effet mesurer l'effort considérable que représente, pour une organisation, le passage d'un mode de développement classique vers une architecture cloud. À la DGFIP, en tant que concepteurs de Nubo, nous avons bénéficié d'une impulsion stratégique déterminante de notre direction générale, assortie d'objectifs chiffrés. Cette dynamique a permis de basculer environ un quart de nos SI, nous donnant aujourd'hui une vision claire de la transformation profonde des pratiques nécessaires pour tirer pleinement profit des avantages du cloud.

Par ailleurs, si Nubo et Pi coexistent, nous ne travaillons pas de manière isolée, et nos collaborations actuelles visent à garantir une interopérabilité entre ces deux environnements. Bien que nos solutions techniques diffèrent légèrement, cette capacité de migration de l'un vers l'autre constitue un levier majeur de résilience, nous permettant de réagir efficacement en cas de défaillance de l'un des systèmes.

M. Aurélien Taché, président. Vous avez insisté sur la nécessité de la conduite du changement et sur l'investissement que cela implique pour que nos administrations soient le plus souveraines possible. J'espère que votre exemple inspirera le maximum de ministères, de communes et de grandes entreprises françaises.

La séance s'achève à dix heures trente.

Membres présents ou excusés

Présents. – Mme Cyrielle Chatelain, M. Aurélien Taché

Excusés. – M. Philippe Latombe, Mme Isabelle Rauch