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

Mardi
17 mars 2026
Séance de 10 heures 30

Compte rendu n° 4

SESSION ORDINAIRE DE 2025-2026

Présidence de
Mme Cyrielle Chatelain, rapporteure de la commission

ASSEMBLÉE NATIONALE

La séance est ouverte à dix heures trente-cinq.

Mme Cyrielle Chatelain, rapporteure, présidente. Je commence par excuser le président Philippe Latombe, qui ne pourra nous rejoindre qu'un peu plus tard dans la journée. Nous recevons ce matin M. Emmanuel Marcovitch, président de section à la première chambre de la Cour des comptes, et MM. Patrice Huiban et Laurent Zerah, conseillers référendaires.

Le 31 octobre dernier, la Cour des comptes a publié un rapport intitulé « Les enjeux de souveraineté des systèmes d'information civils de l'État », sur lequel vous avez tous les trois travaillé. En Europe, la France semble être plutôt force motrice dans la volonté de se libérer d'une trop grande dépendance aux technologies extra-européennes. La Cour souligne cependant que « l'ambition affichée par la France en matière de souveraineté numérique peine à être satisfaite ».

Je vous remercie de nous déclarer tout intérêt public ou privé de nature à influencer vos déclarations.

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.

(MM. Emmanuel Marcovitch, Patrice Huiban et Laurent Zerah prêtent successivement serment.)

M. Emmanuel Marcovitch, président de section à la première chambre de la Cour des comptes. Je vous remercie de nous avoir conviés pour évoquer le rapport que la Cour des comptes a publié en octobre dernier sur les enjeux de souveraineté des systèmes d'information civils de l'État, et qui examine à quel degré l'État maîtrise les technologies numériques qu'il utilise pour ses besoins propres, dans l'objectif de conserver une pleine autonomie de l'action publique. Nous avons examiné trois niveaux : les matériels, les logiciels et les données.

Ces enjeux sont particulièrement sensibles dans un contexte international marqué par la multiplication de cyberattaques, d'ingérences étrangères, de tensions géopolitiques et par la promulgation de lois extraterritoriales, notamment par les États-Unis, pays dont les opérateurs du numérique sont dominants en Europe et en particulier les opérateurs de cloud qu'on appelle *hyperscalers*. Je pense notamment au Cloud Act de 2018 qui permet à un juge américain, en cas d'enquête criminelle, d'exiger le transfert de données – relatives à des personnes ou à des entités – détenues par des fournisseurs de services situés aux États-Unis, même si ces données sont hébergées en dehors du territoire américain, sans avoir à passer par des procédures d'entraide judiciaire internationale.

En ce qui concerne les matériels, on constate que très peu d'industries sont présentes en Europe : qu'il s'agisse de la production de semi-conducteurs, d'équipements réseaux, d'ordinateurs ou de smartphones, tout se fait majoritairement aux États-Unis et en Asie. Il n'y a pas de souveraineté nationale ou européenne sur ce segment, mais l'un des rôles de l'Agence nationale de sécurité des systèmes d'information (Anssi), créée en 2009, est de veiller à ce que les matériels acquis par l'État soient fiables et sans risque sécuritaire. Il existe donc une protection. Par ailleurs, depuis 2015, le réseau interministériel de l'État (RIE), qui est opéré par la direction interministérielle du numérique (Dinum), garantit la résilience des communications gouvernementales, même en cas de défaillance majeure d'internet, pour un budget de l'ordre de 10 millions d'euros par an.

En ce qui concerne les logiciels, malgré la doctrine « cloud au centre » édictée par le gouvernement en 2021, la plupart des applications métier des administrations sont encore hébergées dans des centres informatiques ministériels ou interministériels dont l'État assure l'exploitation et la sécurité. En revanche, la question de la dépendance de l'État vis-à-vis des éditeurs de ces logiciels se pose. Recourir à des logiciels du marché permet de profiter de fonctionnalités déjà éprouvées, d'assurer une rapidité de déploiement, de maîtriser, au moins à court terme, le coût associé ; mais, malgré tous les garde-fous juridiques qui peuvent exister, la démarche crée une dépendance de fait vis-à-vis de l'éditeur, dès lors que les migrations de logiciels sont des projets longs et coûteux. La loi pour une République numérique du 7 octobre 2016 incitait à cet égard les administrations de l'État à utiliser des logiciels libres.

Sur ce volet, la Cour recommande à la Dinum d'intégrer à sa feuille de route une stratégie chiffrée de souveraineté numérique qui définisse notamment les modalités de développement et d'exploitation des applications informatiques de l'État.

Enfin, le niveau qui devient le plus sensible est celui de la protection des données des administrations, des entreprises et des citoyens. En effet, les infrastructures cloud exposent davantage les données que les hébergements sur site. L'Anssi a édicté à cette fin la qualification souveraine SecNumCloud, dont bénéficient à ce jour dix-sept fournisseurs de services. Depuis la révision de la doctrine en 2023, le recours à une telle offre souveraine n'est exigé pour les services de l'État que lorsque deux critères cumulatifs sont observés : d'une part, les données doivent relever de secrets protégés par la loi, d'autre part leur violation doit être susceptible d'engendrer une atteinte à l'ordre public, à la sécurité publique, à la santé, à la vie des personnes ou à la protection de la propriété intellectuelle. Malgré cette définition, il n'y a pas de doctrine interministérielle pour définir et distinguer les données qui relèvent de ce niveau de sensibilité. C'est pourquoi la Cour recommande à la Dinum et à l'Anssi de piloter un travail de cartographie de ces données avec l'ensemble des ministères.

Le choix fait en 2023 de limiter les cas de recours au service SecNumCloud à ces deux critères cumulatifs résulte d'un équilibre entre la revendication de souveraineté de la France et la logique suivie par l'Union européenne, puisque la Commission européenne promeut de son côté un cadre de confiance dans l'échange de données personnelles entre l'Union et les États-Unis, à travers des « décisions d'adéquation » contrôlées par la Cour de justice. Par ailleurs, malgré la demande de la France, le schéma de certification des fournisseurs de service de cloud (EUCS) en cours d'élaboration n'intégrera pas les questions de souveraineté et n'évoquera donc pas un niveau de sécurité de type SecNumCloud.

Pour favoriser le développement du cloud au sein de l'État, deux infrastructures – Nubo au ministère des finances et Pi au ministère de l'Intérieur – ont été ouvertes aux autres administrations. Ces deux clouds interministériels, qui ont mobilisé environ 55 millions d'euros en neuf ans, restent malheureusement peu utilisés. La Cour relève que la gamme des services offerts est limitée et que la tarification est inadaptée ; elle recommande donc une convergence des deux infrastructures sous l'égide de la Dinum. En marge de ces clouds interministériels, quelques administrations ont recours à une exploitation sur une infrastructure SecNumCloud commerciale, mais avec un surcoût par rapport à un hébergement traditionnel évalué entre 25 % et 45 %, sans compter le coût de migration pour des applications déjà existantes.

Qu'on parle de Pi, de Nubo ou des hébergeurs qualifiés SecNumCloud, ils n'ont pas la profondeur de service des *hyperscalers* américains. C'est la raison pour laquelle plusieurs ministères ont fait le choix de faire opérer une partie du système d'information des ressources humaines en mode cloud par une entreprise appartenant à un groupe américain – et donc de

s’affranchir du label SecNumCloud. C’est le cas du ministère de l’éducation nationale avec l’application Virtuo, application RH de gestion des personnels de l’éducation. Même si cette application gère des données d’une sensibilité particulière, le ministère estime qu’il n’y a pas lieu de recourir à une qualification souveraine car leur éventuelle divulgation n’entrerait pas dans un des critères de la circulaire de 2023, érigée au niveau législatif par la loi visant à sécuriser et à réguler l’espace numérique (Sren) de 2024.

Les données confidentielles des entreprises sont aussi des données sensibles dont la divulgation peut causer un trouble à l’ordre public ou à la protection de la propriété intellectuelle. C’est ainsi que le portail public chargé de la généralisation de la facturation électronique est hébergé dans un environnement souverain ; en revanche, tel n’était pas encore le cas de la plateforme d’achat public au moment de l’écriture du rapport – mais je crois que l’Agence pour l’informatique financière de l’État (AIFE), rattachée au ministère des finances, a entrepris des démarches dans ce sens.

La plateforme des données de santé, dite Health Data Hub, qui regroupe les données médicales pseudonymisées à des fins de recherche, a fait le choix au moment de sa création d’un hébergement par l’entreprise Microsoft, ce qui lui a permis de disposer d’un service opérationnel en quelques mois. Cependant, ce choix effectué au nom de la performance a, selon notre analyse, entravé son bon fonctionnement et son développement : une plateforme disposant de moins de fonctionnalités mais souveraine aurait probablement permis un déploiement moins heurté et un usage plus répandu, ce qui aurait rendu plus facile d’atteindre les objectifs recherchés.

Par ailleurs, notre rapport pointe les enjeux des services numériques opérés par des entreprises privées dans un champ public, qui ne relèvent donc pas des exigences portées par la circulaire de 2023 ou la loi Sren. C’est le cas dans le domaine de l’éducation de l’application Pronote, qu’utilisent la plupart des établissements d’enseignement secondaire, ou dans le domaine de la santé de l’application Doctolib, qui recueille des informations médicales très précises. Ces entreprises ne sont pas soumises à l’exigence de souveraineté, même si Docaposte, filiale du groupe La Poste qui édite Pronote, a fait le choix d’un hébergement qualifié SecNumCloud. En ce qui concerne les données de santé, la certification Hébergeur de données de santé (HDS), à laquelle Doctolib est soumise, apporte des garanties de sécurité et de traçabilité, mais n’intègre aucun critère de souveraineté. La dernière recommandation de la Cour est d’aligner la certification HDS sur les exigences de la qualification SecNumCloud en matière de protection vis-à-vis du droit extra-européen.

En conclusion de son rapport, le Cour estime que tant que l’Europe ne dispose pas d’opérateurs capables de rivaliser avec les *hyperscalers* américains, les administrations publiques devraient viser une performance de leurs systèmes d’information plus strictement adaptée à leurs besoins, en faisant le constat que 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. La recherche d’un degré trop élevé de performance à court terme peut en effet créer un double écueil : la mise en cause de la souveraineté sur les données et une dépendance vis-à-vis de la politique commerciale d’un éditeur dominant.

Mme Cyrielle Chatelain, rapporteure, présidente. Pouvez-vous développer la question de la dépendance de l’État vis-à-vis d’éditeurs. Avez-vous des informations sur le coût que cela représente : combien l’État dépense-t-il pour des éditeurs, notamment extra-européens ?

M. Emmanuel Marcovitch. Notre rapport ne visait pas à examiner de manière globale toutes les dépenses de l’État en matière de numérique – nous avons seulement pris quelques exemples, les services du premier ministre avec la Dinum, les ministères des finances, de

l'éducation nationale, de la santé. Toutefois, cette instruction a bel et bien fait ressortir des cas où une dépendance aux éditeurs génère ou pourrait générer des coûts manifestes. Nous citons notamment la situation du logiciel de virtualisation VMware, racheté par le groupe Broadcom, qui a décidé d'en changer la politique commerciale et d'imposer de nouvelles règles, ce qui a multiplié le prix des licences jusqu'à un facteur sept pour certains clients. Les administrations sont certes protégées par l'encadrement de leurs relations par des marchés pluriannuels, mais cela a néanmoins engendré un surcoût de 35 % pour l'AIFE. Les périodes de changement technologique où des éditeurs font basculer leurs offres vers le cloud sont souvent l'occasion d'un changement de politique commerciale, ce qui se traduit par plus de services mais aussi des surcoûts.

C'est aussi le cas, toujours pour l'AIFE, du logiciel Chorus, dont l'ancienne version fonctionnait sur le logiciel européen SAP. Un changement de version de ce dernier a obligé à une migration importante et l'AIFE a étudié la possibilité de changer d'éditeur. Des simulations de ce scénario ont fait apparaître un surcoût allant de 110 % à 160 %, ce qui représentait une charge supplémentaire de 64 millions d'euros. Ainsi, même si une administration peut juridiquement changer de prestataire, cela a un coût en termes de migration de données et de changement de fonctionnalités.

Mais nous n'avons pas étudié le coût pour l'ensemble des administrations de l'utilisation de logiciels d'éditeurs privés extra-européens.

Mme Cyrielle Chatelain, rapporteure, présidente. Le cas de VMware est lié au changement de grille tarifaire d'un acteur privé : avez-vous regardé s'il y avait d'autres acteurs sur le marché ? En général, la dépendance est-elle liée à un manque d'offre, à des habitudes, à des coûts de migration, à des marchés…?

M. Emmanuel Marcovitch. En règle générale, il n'y a pas d'éditeur monopolistique sur un domaine, mais certains sont dominants car leur offre fait référence. Nous citons l'exemple de l'utilisation statistique des données avec l'éditeur SAS, auquel ont recours les services statistiques de l'État, et qui ont aussi effectué des migrations. Ces dernières sont possibles mais elles rencontrent plusieurs freins : celui des compétences internes car il faut savoir gérer ces migrations, celui du changement des interfaces et du mode de travail des utilisateurs, et enfin un obstacle financier. En revanche, je ne crois pas avoir rencontré de situation où un éditeur serait incontournable.

Nous citons le cas de Microsoft Windows, système d'exploitation aujourd'hui largement dominant. Bien qu'il ne soit pas actuellement prévu de s'en passer complètement, d'autres systèmes existent et certaines administrations, comme la gendarmerie nationale, ont fait le choix de déployer un système d'exploitation libre. Ainsi, des alternatives existent, même à un système extrêmement répandu – cependant celles-ci ne sont pas simples à mettre en œuvre pour des questions de coût, de compétences et de changement d'habitudes des utilisateurs.

Mme Cyrielle Chatelain, rapporteure, présidente. Avez-vous pu comparer le coût de l'utilisation de Microsoft Windows et celui de logiciels libres ?

M. Emmanuel Marcovitch. Non, mais une enquête de la Cour, d'initiative citoyenne, sur les outils bureautiques et collaboratifs au sein de l'État est en cours. Elle porte sur les différents modèles utilisés par l'ensemble des ministères et permettra notamment une comparaison entre Microsoft Office Outlook, des outils libres et des outils cloud. Les résultats de cette enquête nous parviendront au deuxième semestre.

Mme Cyrielle Chatelain, rapporteure, présidente. Vous avez évoqué le cas de Pronote, qui est vu par de nombreux utilisateurs comme un outil de service public assez sécurisé et souverain. Pouvez-vous développer ?

M. Emmanuel Marcovitch. Cette situation particulière est liée à l'organisation du ministère de l'éducation nationale : ce sont les établissements scolaires qui choisissent leurs outils et non pas le ministère. Plusieurs éditeurs ont développé des outils destinés à assurer la communication avec les élèves et leurs parents, de même que le ministère de l'éducation lui-même. Il s'est trouvé que l'offre proposée par l'éditeur Index Éducation est celle qui a eu le plus de succès et à laquelle les chefs d'établissement ont recouru. Le logiciel développé par le ministère n'a été utilisé que par quelques dizaines d'établissements et a finalement été abandonné. Ainsi, là où l'on s'attendrait à trouver un outil géré par l'État, comme vous le dites, puisqu'il est intimement lié au service public de l'éducation, les établissements scolaires ont en fait recours à un outil développé par une entreprise privée.

La société Index Éducation a été rachetée par une filiale du groupe La Poste, Docaposte, qui a choisi pour l'outil Pronote un hébergement souverain SecNumCloud – mais elle a fait ce choix de sa propre initiative, en considérant que ces données qui portent sur des millions d'élèves sont très sensibles, sans y être légalement obligée.

Mme Cyrielle Chatelain, rapporteure, présidente. Le fait que l'offre du ministère de l'éducation nationale n'ait pas rencontré son public pose question. Avez-vous une idée du coût de cette offre, et des acteurs qui ont accompagné son développement – cela a-t-il été fait en lien avec des chefs d'établissement, des enseignants voire des associations de parents d'élèves ?

M. Emmanuel Marcovitch. Nous n'avons pas réalisé un audit en profondeur de ce projet ; il me semble qu'il s'agissait d'une extension du système d'information que le ministère avait développé par ailleurs pour ses propres besoins. Cette dimension ne faisant pas partie de son cœur de métier, le ministère a probablement limité ses investissements et a finalement fait le choix de se retirer.

M. Hervé Saulignac (SOC). S'agissant des deux clouds développés par les ministères de l'intérieur et des finances, désormais ouverts aux autres ministères, le rapport relève qu'ils sont peu utilisés et que leur coût est supérieur à celui du marché. Pouvez-vous confirmer que leur coût cumulé s'élève à 55 millions d'euros ? Avez-vous une explication sur le développement parallèle de ces deux clouds, qui répondent pourtant tous deux à des impératifs de sécurité extrêmement importants ?

M. Emmanuel Marcovitch. Oui, ce sont bien 55 millions d'euros qui ont été investis jusqu'à présent pour ces deux clouds ; cette somme est toutefois assez contenue au regard des investissements consentis par les opérateurs privés pour ce type de technologie.

Bien qu'ils possèdent des capacités d'hébergement internes, avec des data centers historiques et très importants, les deux ministères concernés ont basculé vers le cloud au moment où l'État a exigé la création d'infrastructures cloud publiques. Chacun a développé son initiative en parallèle, avec des différences : le cloud du ministère de l'intérieur gère des niveaux de sécurité supérieurs, ses données étant relatives à la sécurité de l'État – bien que les deux outils soient évidemment parfaitement sûrs en matière de cybersécurité. En s'ouvrant à l'interministériel, il s'agissait dans les deux cas de rationaliser l'usage des infrastructures tout en assurant la souveraineté des données et des applications hébergées.

En revanche, ces ministères n'ont pas suffisamment investi dans ces infrastructures : elles proposent aujourd'hui un niveau et une qualité de service inférieurs à celui du marché qualifié SecNumCloud et ne sont pas suffisamment attractives pour les administrations. Par ailleurs, la grille tarifaire est supérieure au coût réel de revient de ces structures. Cette tarification, inadaptée à la qualité des services proposés, devrait être revue afin d'être plus attractive.

Au total, peu d'administrations utilisent Pi et Nubo en dehors des deux ministères qui les ont développés, alors que ces outils maîtrisés par l'État sont, pour certaines applications particulièrement sensibles, des alternatives intéressantes à l'offre du marché. Nous préconisons ainsi un travail de convergence entre ces deux clouds interministériels, avec au moins des feuilles de route communes et un rapprochement des technologies. Quant à l'existence de deux infrastructures distinctes, elle peut se comprendre, pour des raisons de résilience, de redondance, tant que leur développement est coordonné.

Mme Isabelle Rauch (HOR). Au sujet de l'accompagnement au changement, vous avez parlé de difficultés liées au coût et aux compétences. Comment peut-on résoudre la contradiction – qui n'est peut-être qu'apparente – entre internalisation et externalisation des compétences, c'est-à-dire entre les exigences de souveraineté d'une part et du meilleur niveau de compétences d'autre part ? En ce qui concerne le changement d'habitudes, que préconisez-vous pour accompagner les usagers – puisque c'est bien ce changement qui est, au-delà du coût et des compétences, le facteur de succès ?

M. Emmanuel Marcovitch. Nous n'avons pas examiné dans ce rapport le travail entrepris sous l'égide de la Dinum afin de renforcer la filière RH numérique de l'État, notamment en alignant ses grilles salariales et de compétences, afin d'attirer des compétences également recherchées par le secteur privé.

Beaucoup de développements sont effectués par des sous-traitants, qu'il s'agisse de grandes sociétés ou bien de travailleurs indépendants. Cela pose la question de la capacité de l'État à maintenir une expertise dans la durée, à laquelle s'ajoutent des enjeux de confidentialité : tout cela doit être strictement encadré par des marchés et des règles juridiques et déontologiques. D'un autre côté, une internalisation complète impliquerait un recrutement massif de personnel très qualifié, ce qui n'est pas réaliste tant au regard des besoins que de la situation financière de l'État. L'Inspection générale des finances a produit un rapport en 2023 sur ce sujet.

La question du changement d'habitudes est un point sensible ; les outils bureautiques font partie du quotidien et leur modification peut créer des réticences de la part des utilisateurs. Cependant, ce changement peut avoir lieu sous l'effet d'impératifs liés à la souveraineté ou à la sécurité. Nous citons l'exemple – qui peut sembler anecdotique – des messageries instantanées au sein de l'État : des messageries du marché comme WhatsApp ou Telegram étaient utilisées dans l'administration et jusqu'au plus haut niveau, alors qu'elles n'étaient pas souveraines. L'État a réussi à imposer et à généraliser progressivement le recours à Tchap, application souveraine développée par la Dinum. Il a fallu attendre le temps que cette application atteigne la masse critique d'utilisateurs nécessaire à l'apparition d'un effet de réseau et qu'elle apporte des fonctionnalités nouvelles et utiles par rapport à ce qui existe sur le marché. Ce choix a dû être imposé par plusieurs circulaires du premier ministre.

On peut également citer le cas des applications de visioconférence, dont l'utilisation s'est généralisée avec l'essor du télétravail : des outils très différents étaient utilisés, comme Teams ou Zoom, dont beaucoup n'étaient pas souverains. Le premier ministre a imposé une généralisation de Visio, outil garanti par la Dinum, à l'ensemble des services de l'État.

Si un changement d'outil de visioconférence a des conséquences limitées, il faut prendre en compte les freins que peut constituer le changement d'un outil qui serait davantage au cœur du quotidien des agents. Certaines directions de systèmes d'information nous ont dit que des agents pouvaient se sentir malmenés par des outils qu'ils n'arrivent pas à maîtriser, ce qui peut représenter un obstacle à une politique des systèmes d'information ambitieuse.

Mme Cyrielle Chatelain, rapporteure, présidente. Avez-vous identifié des clauses contractuelles qui renchériraient le coût d'une migration, par exemple des pénalités financières imposées par des opérateurs extra-européens ?

D'autre part, M. Verdier, ancien ambassadeur pour le numérique et directeur général de la fondation Inria, nous a dit que les services comprenaient souvent beaucoup d'acheteurs et peu de développeurs : considérez-vous qu'on peut être un bon acheteur si l'on a peu de personnes capables de contrôler la qualité des outils numériques proposés par des opérateurs externes ?

M. Emmanuel Marcovitch. Je ne sais pas si cette répartition signifie nécessairement que les acheteurs ne seraient pas suffisamment formés. Un bon acheteur est capable de challenger le prestataire, dans le numérique comme dans tout autre domaine. Nous n'avons pas examiné ce sujet, mais le fait d'avoir peu de développeurs n'empêche pas forcément de bien exercer la fonction de maîtrise d'ouvrage – qui ne se confond pas avec celle de maîtrise d'œuvre.

En ce qui concerne les migrations, nous n'avons pas vu de marché où il existait des pénalités financières. Cependant, les éditeurs n'ont pas besoin de mettre de telles pénalités pour que la migration ait un coût important, et ce d'autant plus quand les données sont hébergées sur un cloud puisque dans ce modèle, l'éditeur maîtrise à la fois le logiciel et les données, ce qui complexifie encore les démarches. Ces coûts sont divers : coût interne, car il faut des compétences techniques pour opérer le passage d'un environnement à un autre ; coût d'usage, car tous les logiciels n'ont pas le même niveau de fonctionnalité ; parfois, le système existant est en lien avec d'autres applications, ce qui nécessite un redéveloppement en cas de changement d'éditeur. Le cas de Chorus a mis en évidence l'importance de ce coût de migration ; il y a une incitation à maintenir l'éditeur en place. Le frein à la migration est donc moins la clause juridique que ces données techniques et financières.

En 2019, la plateforme des données de santé a fait le choix de l'infrastructure Microsoft Azure parce qu'elle était à l'état de l'art et très rapidement déployable. Cette solution devait être temporaire, mais aucun changement n'est advenu depuis sept ans : les services se sont probablement rendu compte que l'action de migrer était très complexe ; une simple décision politico-administrative ne suffit pas.

Mme Cyrielle Chatelain, rapporteure, présidente. La recommandation n° 2 de votre rapport vise à l'élaboration d'une feuille de route de développement des outils par la Dinum, qui a déjà commencé – notamment avec LaSuite numérique, solution intéressante pour sortir des outils propriétaires. Quel doit être selon vous le rôle de l'État : prescripteur, utilisateur, développeur de projet ? Dans quelle mesure est-il plus intéressant de recourir aux outils développés par la Dinum plutôt qu'aux solutions de marché ?

M. Emmanuel Marcovitch. La recommandation était d'intégrer, à l'occasion de la révision de la feuille de route de la Dinum, une stratégie de souveraineté numérique qui définisse notamment les modalités de développement et d'exploitation des applications informatiques de l'État. Elle n'incitait pas à ce que les outils soient développés par la Dinum, mais pointait simplement le fait que la thématique de la souveraineté n'était pas suffisamment

traitée dans la feuille de route, notamment au sujet du développement et de l'exploitation des logiciels. Nous demandions donc un renforcement de la doctrine de l'État sur ce point, mais cela peut tout à fait passer par un recours à des solutions tierces.

Il y a une tension sur ce sujet : l'État n'a pas forcément vocation à proposer des solutions lorsqu'il en existe déjà sur le marché qui répondent aux besoins. La Dinum et les ministères avancent sur une ligne de crête : que choisissent-ils de faire eux-mêmes, de faire faire et d'acheter ? Ces trois possibilités ont chacune des avantages et des inconvénients. Produire soi-même son outil permet de répondre précisément aux besoins et d'en maîtriser toutes les fonctionnalités, mais cela peut poser un risque de dérapage financier et calendaire, que l'on a vu notamment sur de grands projets numériques dont certains ont duré des années plutôt que les quelques mois annoncés au départ et dont les coûts ont été multipliés par un facteur important. Cela est dû parfois aussi à l'expression par l'État d'exigences trop spécifiques, suivie d'une évolution des besoins, c'est-à-dire à un défaut de maîtrise d'ouvrage dans la conduite de ces projets. Plusieurs rapports de la Cour ont traité ce sujet par le passé.

Il n'y a donc pas un seul modèle à suivre, que ce soit celui du développement interne, du développement à façon ou de l'achat sur le marché ; notre recommandation était d'établir une doctrine générale sur la manière dont la souveraineté doit être traitée.

Mme Cyrielle Chatelain, rapporteure, présidente. Sur quel type de projet ces dérapages ont-ils lieu ? On sait qu'il est fréquent que des projets informatiques échouent, y compris dans le privé : voyez-vous une différence entre les développements en interne et en externe ? Est-ce lié au manque de compétences ?

M. Emmanuel Marcovitch. La plupart des grands projets numériques de l'État sont sous-traités : l'État établit un cahier des charges et gère la maîtrise d'ouvrage, mais il confie le projet à des prestataires extérieurs. Il ne me vient pas à l'esprit de grand projet numérique qui ait été totalement développé en interne, même s'il en existe sûrement. Vous évoquiez LaSuite numérique : la Dinum dispose de compétences internalisées, mais fonctionne avec des développeurs extérieurs.

Notre rapport sur la souveraineté n'a pas examiné ces grands projets numériques, bien que nous en évoquions certains qui ont été traités par d'autres rapports de la Cour ou des rapports d'inspection.

S'agissant des causes des dérapages, il s'agit le plus souvent d'un défaut de maîtrise d'ouvrage, que ce soit dans l'expression d'un besoin initial ou dans la stabilité des besoins dans le temps. Cela concerne plutôt des projets pour lesquels l'État a souhaité un développement à façon et passé un marché pour sous-traiter ce développement.

Mme Cyrielle Chatelain, rapporteure, présidente. Dans le domaine des logiciels, la transparence du code, la capacité à le comprendre et à contrôler l'adéquation de l'outil et de la commande font-elles partie des enjeux d'autonomie et d'indépendance ?

M. Emmanuel Marcovitch. Oui, cela y contribue. Il y a des compétences en la matière au sein de l'État : quand des projets numériques dévient, il est prévu dans le décret relatif à la Dinum que celle-ci mène des audits et intervienne sur les diverses facettes, fonctionnelles et techniques. Pouvoir soulever le capot est évidemment utile.

Mme Cyrielle Chatelain, rapporteure, présidente. Au-delà des compétences, savez-vous si les prestataires sont obligés par leur contrat à être transparents sur leur code ?

M. Emmanuel Marcovitch. Je ne sais pas ; l'Anssi peut probablement répondre à cette question car il est de son ressort de s'assurer de la sécurité de ce que les administrations achètent.

Quand on fait appel à des produits du marché, il est rare que les éditeurs ouvrent leur code ; en revanche, le code des logiciels libres est transparent et les administrations peuvent l'auditer.

Mme Cyrielle Chatelain, rapporteure, présidente. Ainsi, lorsque les administrations ont recours à des solutions « sur étagère », il n'est pas habituel de demander la transparence sur le code, qui est généralement propriétaire ?

M. Emmanuel Marcovitch. Je ne saurais pas vous dire.

Mme Cyrielle Chatelain, rapporteure, présidente. Vous avez évoqué le fait que les travaux sur la certification européenne pourraient être moins précis que ce que la France souhaite et pratique déjà sur les questions de souveraineté. Cela est-il susceptible de remettre en question le référentiel SecNumCloud ?

D'autre part, tout en restant dans le droit européen, est-il possible d'inclure des critères de souveraineté dans la stratégie d'achat public ?

M. Emmanuel Marcovitch. Il y a un chemin à trouver entre l'exigence française forte en matière de souveraineté et l'actuelle absence de consensus européen à ce sujet, notamment en ce qui concerne le marché intérieur. La France a inscrit dans la loi Sren des exigences de souveraineté, dans un périmètre encadré par la double condition que j'évoquais tout à l'heure. Le décret d'application de l'article 31 de la loi Sren a été transmis à la Commission européenne, qui n'a pas formulé d'objections et a donc laissé le travail réglementaire se poursuivre.

Les discussions sur le schéma de certification européen EUCS n'ont pas intégré la demande de la France d'y ajouter un niveau supérieur qui inclurait des questions de souveraineté, c'est-à-dire l'équivalent d'un SecNumCloud garantissant l'étanchéité à des lois extraterritoriales. Cette demande n'a pas été rejetée, mais la Commission européenne a considéré que tel n'était pas l'objet de ce schéma de certification et qu'il en serait question dans un futur règlement sur le développement de l'informatique en nuage et de l'IA. Ce report est aussi dû au fait que le sujet ne fait pas consensus : l'issue est donc incertaine.

Si l'Union européenne ne suivait pas les préconisations de la France, alors les cas d'immunité contre des lois extraterritoriales devraient se limiter à un périmètre circonscrit afin que cela ne revienne pas à exclure des marchés publics des entreprises installées dans d'autres États membres de l'Union européenne. C'est la position que la France a prise récemment avec la loi Sren, qui revient à circonscrire les exigences de souveraineté afin de ne pas trop empiéter sur le marché européen. Nous verrons ce qu'il advient : les discussions sur le futur règlement au sujet de l'informatique en nuage ne sont pas terminées.

Mme Cyrielle Chatelain, rapporteure, présidente. Un de ces États membres, l'Irlande, héberge un grand nombre d'entreprises américaines : cela signifie-t-il qu'on ne pourra pas exclure les branches d'Amazon ou de Google installées en Irlande ?

M. Emmanuel Marcovitch. Il ne s'agit pas que de l'Irlande : les *hyperscalers* américains installent des data centers partout en Europe, ce qu'ils font valoir dans leur communication comme un gage de souveraineté. Toutefois, dès lors qu'il s'agit d'entreprises américaines, elles sont susceptibles de subir des pressions du gouvernement et de la justice des États-Unis dans le cadre du Cloud Act ou du Foreign Intelligence Surveillance Act (Fisa), nous n'avons aucune garantie du respect de cette souveraineté. Ces entreprises sont très peu transparentes sur les sollicitations dont elles ont fait l'objet jusqu'à présent.

Si la France restait isolée sur ces questions, nous pourrions avoir des exigences très élevées en matière de cybersécurité, à l'instar de certaines normes allemandes ou espagnoles, mais il nous faudrait revoir à la baisse nos critères de souveraineté pour certains projets qui ne sont pas d'une sensibilité extrême.

C'est d'ailleurs l'attitude que le ministère de l'éducation a adoptée avec son système de gestion RH : en 2021, la doctrine « cloud au centre » était beaucoup plus large – elle exigeait un recours au SecNumCloud dès qu'il était question de données personnelles – puis, lorsqu'en 2023 la doctrine s'est resserrée autour du double critère, le ministère de l'éducation a argué que le deuxième critère n'était pas rempli, en considérant que la divulgation des informations ne créerait pas un trouble excessif à l'ordre public. Va-t-on devoir maintenir un périmètre restreint dans lequel nous pourrons imposer notre souveraineté, ou bien ce périmètre pourra-t-il s'élargir ? Le choix de l'Union européenne ne sera pas neutre de ce point de vue.

Mme Cyrielle Chatelain, rapporteure, présidente. Ce sujet est pris en compte au plus haut niveau de l'État, vous l'avez dit ; est-ce qu'il fait selon vous l'objet de choix et de décisions politiques, ou reste-t-il vu comme un sujet d'intendance ou de support ?

M. Emmanuel Marcovitch. En effet, ce sujet est dans le débat mais l'enjeu de souveraineté n'est pas encore complètement intégré dans les stratégies numériques des administrations. On peut identifier quatre domaines de contradiction ou d'incertitude. Tout d'abord, une gouvernance qui n'est pas assez affirmée – la feuille de route stratégique n'est pas suffisamment explicite, il n'existe pas de cartographie interministérielle des données sensibles. En deuxième lieu, on note une interférence entre les exigences de cybersécurité et de souveraineté – les administrations publiques choisissent les solutions les plus sûres en matière de cybersécurité mais celles-ci sont parfois extra-européennes. Une troisième tension existe entre performance technique et souveraineté, ce qui vaut pour le système de santé ou pour l'éducation nationale : une application non souveraine mais déjà déployée massivement à l'échelle mondiale et rapidement opérable peut être intéressante pour une administration publique. Enfin, la montée en puissance très lente des clouds interministériels Pi et Nubo ne favorise pas l'essor de cette architecture sécurisée et souveraine interne à l'État.

La volonté politique est donc affirmée mais il existe encore une grande marge de progrès sur ces différents axes. Aller plus loin ne nécessiterait probablement pas d'investissements lourds au regard des budgets numériques de l'État et de ce qui a été investi jusqu'ici dans les enjeux de souveraineté.

La séance s'achève à onze heures trente-cinq.

Membres présents ou excusés

Présents. – Mme Cyrielle Chatelain, M. Philippe Latombe, Mme Isabelle Rauch, M. Hervé Saulignac