Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

COMMISSION SUPERIEURE DU NUMERIQUE ET DES POSTES

AVIS N°2023-06

DU 12 SEPTEMBRE 2023

SUR LA SOUVERAINETE NUMERIQUE

AVIS N°2023-06 DU 12 SEPTEMBRE 2023
SUR LA SOUVERAINETE NUMERIQUE

Les membres de la Commission Supérieure du Numérique et des Postes (CSNP) ont confié à Madame Anne LE HÉNANFF, députée du Morbihan, la mission de formuler un certain nombre de recommandations afin de renforcer notre souveraineté numérique.

Le groupe de travail sur la souveraineté numérique s'est efforcé, tout au long des auditions qu'il a menées, d'identifier et de définir des mesures concrètes et réalistes pour assurer et renforcer l'indépendance de la France et de l'Europe en matière de souveraineté numérique, s'appuyant sur une industrie nationale et européenne de premier rang.

Les membres du groupe de travail ont porté une attention toute particulière aux quatre points suivants :

- La définition de la souveraineté numérique,
- Les conditions de mise en œuvre de notre souveraineté numérique,
- Les leviers des marchés publics et de l'émergence des *clouds* de confiance pour garantir une souveraineté numérique,
- La mise en œuvre de la qualification SecNumCloud au sein de l'Etat et des collectivités territoriales.

Au terme de ses travaux, le groupe de travail formule les 10 recommandations suivantes :

Recommandation 1: Les données sensibles détenues et gérées par les administrations et établissements des collectivités territoriales, les établissements de santé et les universités, sont identifiées. Lorsque cette cartographie aura été réalisée, la CSNP estime que ces données pourraient se conformer aux exigences posées par la circulaire du 31 mai 2023 sur « le cloud au centre ».

Recommandation 2: L'extension du rôle des préfets afin qu'ils s'assurent que les données sensibles des collectivités territoriales et de leurs établissements soient bien hébergées dans un cloud souverain. A cet effet nous proposons qu'un volet numérique soit intégré au plan communal de sauvegarde numérique (PCS numérique). Ces nouvelles attributions seront accompagnées d'un renforcement de leurs moyens, lequel s'inscrira en cohérence avec la mise en œuvre des textes européens (Directive NIS2, Data Act), notamment en termes de calendrier.

Recommandation 3: L'accompagnement des plus petites collectivités, des établissements de santé et des universités qui ne disposent pas des moyens financiers et humains suffisants pour la mise en conformité avec la législation sur l'hébergement des données.

Recommandation 4 : Le code des marchés publics intègre davantage la nécessité de souscrire à des solutions numériques souveraines et est simplifié pour ne pas dissuader les nouveaux acteurs du numérique de répondre à des appels d'offre jugés trop complexes, mais au contraire les y encourager.

Recommandation 5 : Le CSF Numérique de confiance formule des propositions concrètes afin de trouver des solutions souveraines intégrées qui permettraient de répondre aux attentes des acheteurs publics.

Recommandation 6 : Les autorités françaises portent avec force et vigueur, auprès de la Commission européenne et des autres Etats membres, l'adoption d'un « Buy European Tech Act » et d'un « Small Business Act » dans les meilleurs délais.

Recommandation 7 : Le chef de l'Etat et son Gouvernement présentent, en début de quinquennat, une feuille de route sur la stratégie politique garantissant la souveraineté industrielle et numérique de la France. Un suivi de la mise en œuvre de la feuille de route pourra être présenté devant la représentation nationale chaque année à l'occasion de l'examen du projet de loi de finances ou dans le cadre des débats annuels du Printemps de l'évaluation.

Recommandation 8 : Le Gouvernement s'engage à inscrire, dans chaque projet de loi de finances, une ligne budgétaire consacrée à la souveraineté numérique et à sa mise en œuvre ainsi qu'un document budgétaire retraçant l'effort de l'Etat en la matière (« jaune budgétaire »). Une meilleure lisibilité du financement au pilotage et au soutien apporté au numérique au niveau territorial nous apparait essentiel.

Recommandation 9 : La création d'un Conseil de défense de la stratégie numérique, auprès du Président de la République.

Recommandation 10 : Les enjeux et dossiers relatifs à la souveraineté numérique sont directement rattachés aux attributions du Premier ministre et suivis par ses services.

AVIS N°2023-06 DU 12 SEPTEMBRE 2023
SUR LA SOUVERAINETE NUMERIQUE

En France, l'expression "souveraineté numérique" et la nécessité de repenser la souveraineté des États dans un monde où les outils et la puissance numérique sont concentrés aux mains de quelques acteurs et de quelques pays ont été consacrées et abordées par Bernard BENHAMOU et Laurent SORBIER dans leur ouvrage *Souveraineté et réseaux numériques* en 2006.

Par ailleurs, plusieurs rapports parlementaires ont déjà abordé la définition de la souveraineté numérique ces dernières années. Parmi les récents et les plus complets sur ce sujet, on citera le rapport de nos collègues Philippe LATOMBE et Jean-Luc WARSMANN « *Bâtir et promouvoir une souveraineté numérique nationale et européenne* », paru en juin 2021.

Dans ce contexte, les travaux du groupe de travail se sont concentrés sur une définition opérationnelle de la souveraineté numérique sur laquelle pourrait s'appuyer les décisions politiques et les actions à engager pour la mettre en œuvre :

- La souveraineté est un principe défini et garanti par la charte des Nations Unies qui dispose que chaque État est souverain sur son territoire.

- La notion de souveraineté numérique se retrouve dans de nombreux domaines mais elle s'apprécie tout particulièrement dans les domaines militaire et économique. En effet, face à un monde en constante évolution, répondre aux enjeux géopolitiques, stratégiques, d'indépendance, financiers et économiques est nécessaire à une nation souveraine.

- La souveraineté numérique est la capacité pour un État de conserver un accès autonome à son espace numérique et aux services numériques liés à l'exercice de sa souveraineté, en sécurisant son autonomie et l'accès aux contenus qu'il a définis comme stratégiques, ainsi que les données qu'il juge stratégiques et/ou sensibles.

Cette définition suppose une souveraineté d'ordre technologique et une souveraineté sur les données.

S'agissant de la souveraineté technologique, il convient de rappeler que le numérique comporte différentes couches technologiques et que, pour être totalement souverain, un État devrait en maîtriser la totalité. Cependant, aujourd'hui, aucun pays ne dispose d'une autonomie totale sur l'ensemble de la chaîne de valeurs (terres rares, microprocesseurs, intégrateurs, câbles sous-marins internet etc.).

Concernant la souveraineté des données, il est essentiel de comprendre que ces données publiques ou privées ont une incidence directe sur les États et peuvent avoir un impact financier, géopolitique, soulevant alors des enjeux démocratiques. Les données, à défaut d'un accord express de la part de l'utilisateur ou du client, doivent rester sa propriété. Le règlement général sur la protection des données (RGPD), entré en application le 25 mai 2018 et qui encadre le traitement des données de manière égalitaire sur l'ensemble du territoire de l'Union européenne va en ce sens, mais la pratique montre que ce texte européen majeur ne garantit pas à lui seul ce principe.

Les données à caractère personnel sont donc couvertes par le RGPD, mais ce n'est pas le cas des données non personnelles car elles ne font pas l'objet d'une protection garantie par les Etats, ou alors dans une moindre mesure. Ainsi, les données non personnelles mais stratégiques et sensibles des collectivités locales, des hôpitaux, etc.. ne sont protégées par aucun dispositif réglementaire.

Partant de cette définition et de ces constats, les membres de la Commission Supérieure du Numérique et des Postes considèrent que c'est au plus haut niveau de l'État, et sous le contrôle du Parlement, qu'il faut arbitrer sur le périmètre et les moyens à engager pour garantir une véritable souveraineté numérique.

I. Pas de souveraineté numérique sans maîtrise de nos données

Les données sont au cœur de la souveraineté numérique, même s'il n'en existe pas de définition légale. Toutefois, certaines catégorie de données ont été plus ou moins clairement définies afin de permettre aux textes législatifs, règlementaires et normatifs d'y faire référence.

Ainsi, l'article 4 du RGPD considère que par « données à caractère personnel » on entend *« toute information se rapportant à une personne physique identifiée ou identifiable, […] »*. La définition de la donnée sensible est plus difficile à déterminer, mais, si on se réfère à la Commission Nationale de l'Informatique et des Libertés (CNIL), les données sensibles *« sont des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique. »*

Si la donnée est partiellement ou totalement hébergée chez des opérateurs étrangers peut-on alors considérer que nous sommes en situation de garantir une situation de souveraineté numérique ?

Aujourd'hui, trois géants américains détiennent 65% du marché du cloud mondial[1] : Amazon Web Services (AWS) à hauteur de 32%, Microsoft Azure à hauteur de 23% et Google Cloud pour 10%.

Aussi, il est indispensable que les acteurs du secteur public comme privé prennent conscience de l'importance de protéger leurs données ainsi que celles de leurs usagers. Cependant, on constate encore un manque de connaissance de ces enjeux de protection, de confidentialité et de sécurité de la donnée chez certaines administrations et entreprises publiques ou privées.

Si les données publiques et privées doivent être protégées, les données sensibles doivent l'être encore plus. Il est impératif que nos données sensibles soient hébergées dans des espaces sécurisés, dont l'accès et le contrôle sont placés sous l'autorité de notre pays.

L'une des solutions les plus concrètes serait que les entreprises publiques comme les entreprises privées, ainsi que les administrations s'assurent que leurs données sensibles soient hébergées chez un fournisseur de cloud non soumis à des législations extraterritoriales, et de préférence dans des clouds français ou européens.

La notion de cloud souverain peut être discutée. Cependant, si l'on se base sur les enjeux portés par les stratégies et politiques mises en œuvre, on entend par cloud souverain un cloud de confiance, transparent, non soumis à des législations extraterritoriales, et dont des certifications garantissent son niveau de confiance.

En 2016, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a élaboré le référentiel SecNumCloud visant à permettre la qualification de prestataires de cloud avec pour objectif de certifier le niveau de confiance d'un hébergeur.

[1] Etude de Synergy Research Group pour le 1er trimestre 2023 https://www.srgresearch.com/articles

Cette qualification repose sur un certain nombre de critères et est valable pour une durée de 3 ans renouvelable, conditionnée par le respect des engagements du prestataire durant toute la durée de la qualification. Elle vise notamment à orienter les autorités administratives, les entreprises privées et les opérateurs d'importance vitale vers des solutions de cloud de confiance, mais également à rassurer les clients en recherche de solutions sécurisées pour héberger leurs données sensibles.

Avec l'adoption de la doctrine « cloud au centre » en mai 2021, le Gouvernement a fait du cloud un prérequis pour tout nouveau projet numérique au sein de l'État, l'hébergement pouvant se faire soit sur un cloud interne, soit sur un cloud externe qualifié par l'ANSSI comme un cloud de confiance. L'objectif étant d'accélérer la transformation numérique au bénéfice des usagers et dans le strict respect de la cybersécurité et de la protection des données des citoyens et des entreprises.

Le paragraphe [R9] de la circulaire du 5 juillet 2021[2] précise que *« si le système ou l'application informatique manipule des données d'une sensibilité particulière, qu'elles relèvent notamment des données personnelles des citoyens français, des données économiques relatives aux entreprises françaises, ou d'applications métiers relatives aux agents publics de l'État : l'offre de cloud commercial retenue devra impérativement respecter la qualification SecNumCloud (ou une qualification européenne d'un niveau au moins équivalent) et être immunisée contre toute réglementation extracommunautaire. »*

Recemment, la circulaire du 31 mai 2023[3] est venue préciser la précédente circulaire et notamment le périmètre des données relevant d'une sensibilité particulière, à savoir « *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 (par exemple, les secrets liés aux délibérations du Gouvernement et des autorités relevant du pouvoir exécutif, à la défense nationale, à conduite de la politique extérieure de la France, à la sûreté de l'Etat, aux procédures engagées devant les juridictions ou encore le secret de la vie privée, le secret médical, le secret des affaires qui comprend le secret des procédés, des informations économiques et financières et des stratégies commerciales ou industrielles) »* 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. »*

Ainsi, cette circulaire impose l'utilisation d'un hébergeur de confiance pour l'ensemble des données sensibles préalablement citées mais exclue *de facto* les données non considérées comme sensibles.

Cette circulaire ne concerne donc que l'utilisation de l'informatique en nuage par l'État (« cloud au centre») bien que les collectivités territoriales soient amenées à gérer quotidiennement des données personnelles telles que l'état civil, les affaires scolaires, les données médicales, ou des données sur la sécurité des personnes, et devraient, selon la CSNP être concernées par l'obligation d'un hébergement sur un cloud respectant la qualification SecNumCloud.

La Commission recommande à l'ensemble des administrations, des collectivités territoriales, des établissements de santé et des universités (recherche) d'avoir recours à des hébergeurs de confiance pour les données sensibles ou nécessitant une protection particulière dont elles disposent,

[2] Circulaire n° 6282-SG du 5 juillet 2021 relative à la doctrine d'utilisation de l'informatique en nuage par l'État https://www.legifrance.gouv.fr/circulaire/id/45205

[3] Actualisation de la doctrine d'utilisation de l'informatique en nuage par l'État (« cloud au centre») https://www.legifrance.gouv.fr/circulaire/id/45446?origin=list

une fois ces dernières identifiées comme telles. L'hébergement mais également le traitement des données doit être garanti.

Les membres de la CSNP estiment également essentiel l'accompagnement des petites collectivités et des établissements publics qui ne disposeraient pas des moyens humains et financiers nécessaires pour se conformer à cette doctrine. Par ailleurs, les offres labélisées sont généralement plus coûteuses, ce qui peut constituer un frein pour ces acteurs.

Les membres de la CSNP proposent donc que les missions des préfets soient renforcées pour accompagner et veiller à la mise en œuvre de la sécurisation des données sensibles et à caractère personnel des collectivités locales, notamment au regard du RGPD, mais également des établissements publics de santé et des universités. Avec des moyens renforcés, les préfets s'assureront du bon déroulement des migrations des données concernées vers des clouds de confiance. Dans l'éventualité où le recours à ces opérateurs cloud représenterait un surcoût conséquent pour ces acteurs, il est nécessaire que l'Etat le prenne en compte en prévoyant un accompagnement humain et/ou financier.

Recommandations :

Recommandation 1: Les données sensibles détenues et gérées par les administrations et établissements des collectivités territoriales, les établissements de santé et les universités, sont identifiées. Lorsque cette cartographie aura été réalisée, la CSNP estime que ces données pourraient se conformer aux exigences posées par la circulaire du 31 mai 2023 sur « le cloud au centre ».

Recommandation 2: L'extension du rôle des préfets afin qu'ils s'assurent que les données sensibles des collectivités territoriales et de leurs établissements soient bien hébergées dans un cloud souverain. A cet effet nous proposons qu'un volet numérique soit intégré au plan communal de sauvegarde numérique (PCS numérique). Ces nouvelles attributions seront accompagnées d'un renforcement de leurs moyens, lequel s'inscrira en cohérence avec la mise en œuvre des textes européens (Directive NIS2, Data Act), notamment en termes de calendrier.

Recommandation 3: L'accompagnement des plus petites collectivités, des établissements de santé et des universités qui ne disposent pas des moyens financiers et humains suffisants pour la mise en conformité avec la législation sur l'hébergement des données.

II. La Commande publique : un levier essentiel pour renforcer l'écosystème français et européen du numérique

Les membres de la Commission Supérieure ne sont pas favorables à une politique de protectionnisme absolue qui n'aurait que très peu d'intérêt et serait vraisemblablement contreproductive, pour les acheteurs publics.

En revanche, les membres de la Commission Supérieure estiment que La France et les États européens seraient très naïfs de penser que la commande publique ne doit pas jouer toute sa part à l'élaboration d'une offre numérique européenne et souveraine.

Sachant que nous considérons que, pour être efficace, une politique de souveraineté doit articuler de manière cohérente les trois leviers suivants : le réglementaire, la commande publique et l'investissement public.

- **Au niveau européen**

Alors qu'aux Etats-Unis, des réglementations liées à la commande publique (« Buy American Act » et « Small Business Act ») ont permis de favoriser et donc de financer les entreprises américaines stratégiques sur leur marché intérieur, le principe d'un « Small Business Act » ou d'un « Buy European Act » qui réserverait une partie des marchés publics à des offres européennes, notamment sur les marchés sensibles et essentiels, est discuté depuis plusieurs années sans que ces projets aboutissent.

Il est primordial que ces propositions se concrétisent sans tarder au niveau européen.

Les membres de la Commission Supérieure pensent que la souveraineté française et européenne, notamment en matière de cloud, pourrait se traduire et se concrétiser par le recours, dans le cadre de la commande publique, à une solution française ou européenne dès lors que des données sensibles et/ou à caractère personnel seraient concernées. Cette mise en œuvre se ferait en cohérence avec les directives européennes.

Le recours à une solution française ou européenne dans le cadre de la commande publique s'appuie sur l'actuelle politique du Gouvernement qui vise à ce que les opérateurs français et européens montent en compétence et se développent afin de proposer des solutions souveraines qui répondent à la demande.

Les membres de la Commission supérieure souhaitent que la France porte un message fort en ce sens auprès de l'Union européenne.

- **Au niveau français**

Les membres de la Commission Supérieure du Numérique et des Postes ont accueilli très favorablement le lancement d'un comité stratégique de filière (CSF) Numérique de confiance en septembre 2022 et attendent avec intérêt les propositions concrètes de ce comité, notamment sur le volet « marchés publics ».

La prise de conscience des élus sur les fragilités liées à des solutions ne garantissant pas une véritable souveraineté numérique et présentant une faible sécurisation des données est encore partielle. Pourtant, les collectivités locales et les établissements publics sont demandeurs de règles claires à appliquer dans leurs achats de services numériques.

Il nous semble que le moment est venu de proposer et d'adopter des règles de commande publique qui établissent une priorité pour des solutions souveraines, par voie règlementaire et législative.

Les offres françaises et européennes existent, mais il convient d'adapter les règles des marchés publics afin que :

- les acheteurs soient incités à acquérir des solutions souveraines intégrées,

- les entreprises françaises et européennes, notamment les TPE/PME, ne soient pas dissuadées de répondre à des appels d'offres complexes qui, *in fine*, n'intègrent pas les solutions françaises ou européennes.

Recommandations :

Recommandation 4 : Le code des marchés publics intègre davantage la nécessité de souscrire à des solutions numériques souveraines et est simplifié pour ne pas dissuader les nouveaux acteurs du numérique de répondre à des appels d'offre jugés trop complexes, mais au contraire les y encourager.

Recommandation 5 : Le CSF Numérique de confiance formule des propositions concrètes afin de trouver des solutions souveraines intégrées qui permettraient de répondre aux attentes des acheteurs publics.

Recommandation 6 : Les autorités françaises portent avec force et vigueur, auprès de la Commission européenne et des autres Etats membres, l'adoption d'un « Buy European Tech Act » et d'un « Small Business Act » dans les meilleurs délais.

III. Souveraineté numérique : la nécessité d'un portage politique au plus haut niveau

- **Des champions du numérique internationaux portés par des choix stratégiques et politiques**

Les Etats- Unis ont massivement investi dans les technologies avancées dès les années 1960 en créant la Defense Advanced Research Projects Agency (DARPA). Ces investissements se sont notamment concrétisés dans les domaines de l'aérospatiale, des biotechnologies et des technologies numériques. Portés par une volonté politique forte, ces investissements massifs ont permis l'émergence d'écosystèmes dans la Tech mais surtout des grands acteurs du numérique que nous connaissons aujourd'hui.

Dès les années 1990, la Chine a pris conscience de la révolution que constituaient les télécommunications et le numérique. A cette époque, le Gouvernement chinois a adopté une circulaire affirmant la priorité des cours d'informatique dans les établissements scolaires et universitaires. Cette décision, qui émanait directement du Gouvernement central, a abouti à l'émergence de nombreux chercheurs et ingénieurs dotés d'excellentes compétences en informatique lesquels ont contribué à l'autonomie numérique que la Chine a su déployer sur quasiment l'ensemble de la chaine de valeurs ainsi qu'à sa vitalité dans l'innovation.

La Corée du Sud et Israël illustrent également l'importance de la volonté stratégique et politique pour faire émerger une industrie numérique de pointe.

- **Le positionnement de la France**

La France a porté de véritables ambitions souveraines dans le domaine de l'aérospatiale et de l'énergie. Dans le domaine de l'informatique et du numérique, force est de constater que la France a perdu la bataille du numérique pour le grand public au profit des GAFAM même si les technologies spécialisées de grands groupes comme Atos, Dassault systems, Thales, sont reconnus au niveau international.

Pour ne pas dépendre de solutions non souveraines, le ministère des Armées a anticipé les risques opérationnels en développant ses propres solutions avec des acteurs de confiance.

Face à ce constat, les causes relevées par les membres de la Commission sont de deux ordres : industrielles et stratégiques.

Alors que la France dispose d'écoles et de centres de recherche dont sont issus les grands noms de la Tech, employés notamment dans les Big Tech américaines, à l'instar de Yann LE CUN, responsable de la recherche en Intelligence artificielle chez Meta, les autorités françaises ont sous-investi pendant des décennies dans ces domaines. Elles ont également démontré un manque de volontarisme dans la conduite d'une véritable politique en matière de souveraineté numérique.

Or, nous constatons, d'une part, que la France et l'Europe ne disposent pas de véritables stratégies industrielles, avec une vision sur l'ensemble de la chaine de valeur et, d'autre part, qu'il est évident que nous devons renforcer notre stratégie de protection des données.

Il est urgent d'adopter une stratégie de souveraineté avec une vision française et européenne, de long terme et transverse pour soutenir la souveraineté numérique de la France et de l'Europe qui doit pouvoir s'appuyer sur une puissance de création, de licornes, de chercheurs et d'ingénieurs.

Il ne s'agit pas, bien entendu, de tenter de mettre en place à notre échelle ce que les Big Techs américaines et chinoises ont réussi à faire au cours de ces dernières années, mais il serait irresponsable de ne pas anticiper les risques que font peser ces monopoles sur nos démocraties.

- **Une véritable souveraineté ne se fera pas sans une stratégie nationale et un vrai portage politique.**

La souveraineté numérique doit être portée au plus haut niveau politique. Aux Etats-Unis, par exemple, la définition de la stratégie de développement d'Internet est directement rattachée au président.

En France, la souveraineté numérique est placée, depuis 2022, sous la responsabilité du ministère de l'Economie, des Finances et de la Souveraineté industrielle et numérique alors que la sécurité numérique est assurée par l'ANSSI.

Dans la continuité du discours de la Sorbonne de juin 2017, où le Président de la République s'était engagé « pour une Europe souveraine, unie, démocratique » le Gouvernement a mis en place une politique axée sur la souveraineté numérique qui s'est notamment illustrée lors de la présidence française du Conseil de l'Union européenne au semestre 2022. Le Gouvernement français se veut dès lors résolument ferme face à la question de la souveraineté numérique et la place des GAFAM au sein de l'écosystème numérique européen.

Afin de concrétiser le réveil technologique européen nécessaire, le ministre de l'Économie, des Finances et de la Souveraineté industrielle et numérique a insisté sur le besoin de maîtriser les innovations, la souveraineté technologique et politique à laquelle la France et l'Europe « aspire entre la Chine et les Etats-Unis ». Par ailleurs, la mise en œuvre de la stratégie nationale pour le Cloud et la souveraineté numérique annoncée à Strasbourg le 12 septembre 2022, , portée par M. Jean-Noël BARROT, ministre délégué chargé du numérique, marque un renforcement et une continuité de la volonté française.

L'examen du projet de loi visant à sécuriser et réguler l'espace numérique et qui comprend l'interopérabilité et la portabilité des services de cloud permettra notamment de renforcer notre souveraineté numérique face au monopole et aux pratiques de concurrence déloyale des fournisseurs.

Aussi, pour la majorité des membres de la Commission supérieure, la politique de souveraineté numérique pourrait être définie au plus haut niveau de l'État, à savoir par le président de la République et le Premier ministre.

S'agissant d'un domaine aussi stratégique, il est essentiel que la politique de la France intègre toutes les dimensions de ces enjeux alors qu'aujourd'hui on constate que les sujets du numérique ne sont pas transverses, mais « en silo » au sein de chaque ministère, ce que la CSNP regrette. En effet, un tel fonctionnement ne permet pas d'avoir une politique de grande ampleur et uniforme selon les secteurs, allant parfois jusqu'à la mise en œuvre de mesures en inadéquation les unes par rapport aux autres.

La Commission Supérieure du Numérique et des Postes a débattu du niveau le plus approprié pour renforcer ce portage politique. La majorité des membres de la CSNP estime que la création d'un Conseil de défense de la stratégie numérique présidé par le président de la République ainsi que la formulation d'une stratégie politique en début de quinquennat permettrait de renforcer la lisibilité de la politique française en matière de souveraineté numérique.

La mise en œuvre de cette politique par les différents ministères serait pilotée et contrôlée par les services du Premier ministre et trouverait sa traduction législative et budgétaire dans le cadre des lois de finances. Elle pourrait également donner lieu chaque année à un contrôle parlementaire lors du Printemps de l'évaluation.

Madame Sophia Chikirou s'est montrée réservée à l'égard d'un rattachement d'un Conseil stratégique à la Présidence de la république et privilégie un portage par le Conseil économique, social et environnemental. Mme Sophia Chikirou a voté contre l'adoption du présent avis.

Recommandations :

Recommandation 7 : Le chef de l'Etat et son Gouvernement présentent, en début de quinquennat, une feuille de route sur la stratégie politique garantissant la souveraineté industrielle et numérique de la France. Un suivi de la mise en œuvre de la feuille de route pourra être présenté devant la représentation nationale chaque année à l'occasion de l'examen du projet de loi de finances ou dans le cadre des débats annuels du Printemps de l'évaluation.

Recommandation 8 : Le Gouvernement s'engage à inscrire, dans chaque projet de loi de finances, une ligne budgétaire consacrée à la souveraineté numérique et à sa mise en œuvre ainsi qu'un document budgétaire retraçant l'effort de l'Etat en la matière (« jaune budgétaire »). Une meilleure lisibilité du financement au pilotage et au soutien apporté au numérique au niveau territorial nous apparait essentiel.

Recommandation 9 : La création d'un Conseil de défense de la stratégie numérique, auprès du Président de la République.

Recommandation 10 : Les enjeux et dossiers relatifs à la souveraineté numérique sont directement rattachés aux attributions du Premier ministre et suivis par ses services.

PERSONNES AUDITIONNEES

GDI. Aymeric BONNEMAISON, Commandant de la Cyberdéfense – Ministère des Armées

M. Marc DARMON, Directeur général adjoint en charge des systèmes d'information et de communication sécurisés – Thalès

M. Jean-Noël de GALZAIN, Président – Hexatrust

M. Michel PAULIN, Directeur général – OVH Cloud

Pr. Kavé SALAMATIAN, Professeur spécialisé sur les enjeux géopolitiques – Université de Savoie

M. Vincent TEJEDOR, Directeur général du numérique - Ministère des Armées

M. Olivier VALLET, Directeur général – Docaposte

M. Henri VERDIER, Ambassadeur pour le numérique – Ministère de l'Europe et des Affaires étrangères

M. Mathieu WEILL, Directeur du numérique – Ministère de l'Intérieur