CSNPE

COMMISSION SUPÉRIEURE DU NUMÉRIQUE ET DES POSTES

RAPPORT D'ACTIVITÉ 2024

SOMMAIRE

Damien MICHALLET,
Sénateur de l'Isère
Président de la Commission Supérieure
du Numérique et des Postes

ÉDITORIAL DU PRÉSIDENT

En 2024, l'activité de la Commission Supérieure du Numérique et des Postes a reflété plus que jamais les préoccupations de nos concitoyens dans le domaine des télécommunications, du numérique et des services postaux.

En effet, l'année 2024 a été particulièrement dynamique pour la CSNP, marquée par des contributions significatives aux débats nationaux et européens sur des sujets cruciaux tels que la cybersécurité, l'intelligence artificielle, le déploiement des réseaux de télécommunications ou encore l'inclusion numérique.

Dans le cadre de la transposition de la directive NIS 2, la CSNP a été saisie par l'ANSSI sur la transposition de ce texte majeur qui vise à renforcer le niveau de cybersécurité de notre pays. Nous avons rendu un avis et un rapport en vue de sa mise en conformité en droit français. Cette directive impose des exigences strictes aux entités concernées, et nous sommes vigilants à ce qu'il n'y ait pas de surtransposition.

Sur l'impact potentiel de l'intelligence artificielle sur le marché du travail et la société, nous avons plaidé pour un débat public approfondi et une évaluation rigoureuse de l'impact de l'IA dans la société. En effet, nous avons souligné l'importance d'une approche centrée sur l'humain, respectueuse des droits fondamentaux, et avons appelé à une régulation transparente pour encadrer le déploiement de l'IA dans divers secteurs.

La CSNP a souhaité faire entendre ses préoccupations quant aux réductions budgétaires prévues dans le cadre de la politique d'inclusion numérique dans le projet de loi de finances 2025. En novembre 2024, nous avons alerté sur la diminution significative des fonds alloués au dispositif des conseillers numériques, passant de 62 millions d'euros en 2024 à 27 millions en 2025. Nous avons souligné l'importance cruciale de maintenir un financement adéquat pour assurer l'accès de tous les citoyens aux outils numériques, particulièrement les populations vulnérables.

L'accessibilité aux services numériques passe aussi par une couverture, en réseau optique et mobile, homogène sur l'ensemble du territoire. Nous avons saisi le gouvernement et avons demandé des engagements fermes sur la mise en œuvre du Plan France Très Haut Débit afin qu'il arrive à son terme et qu'une réflexion soit engagée pour la suite du Plan, notamment en termes de pérennité et d'entretien des réseaux.

Dans le cadre des obligations qui lui sont conférées par la loi, la CSNP a évalué et contrôlé les missions de service public confiées au Groupe La Poste, notamment celles de Service Universel Postal et d'aménagement du territoire. A ce titre, nous appelons le gouvernement à compenser les missions de service public au plus près des coûts réels. Les services de La Poste sont indispensables pour contribuer à la cohésion sociale et pour garantir un développement équilibré dans tous les territoires.

En 2024, la Commission a rendu 9 avis et a organisé plus de 90 auditions, qui ont contribué à éclairer le Parlement et le Gouvernement sur les enjeux du numérique ainsi que les activités postales.

Enfin, en dépit des discussions entourant la possible suppression de la CSNP dans le cadre du projet de loi de simplification de la vie économique, la Commission demeure résolue à poursuivre sa mission en 2025. Nous continuerons à concentrer nos efforts sur des thématiques telles que la fin des technologies 2G et 3G, la fermeture du réseau cuivre, la 5G industrielle, le service universel des télécommunications, les ingérences étrangères et les réseaux sociaux, la transition écologique des infrastructures numériques et le déploiement des réseaux.

Nous nous engageons à continuer de fournir des analyses et des recommandations éclairées pour accompagner les transformations numériques et postales au service de l'intérêt général.

Damien Michallet

COMPOSITION ET MOUVEMENTS AU SEIN DE LA CSNP EN 2024

L'article L125 du Code des postes et des télécommunications précise que la Commission supérieure du numérique et des postes comprend sept députés et sept sénateurs ainsi que trois personnalités qualifiées dans les secteurs des postes et des communications électroniques, désignées par les ministres chargés des postes et des communications électroniques parmi six personnalités proposées par le Président de la Commission. Elle est présidée alternativement par un député et un sénateur élu en son sein pour une durée de trois ans. L'écart entre le nombre de femmes et d'hommes, membres de la Commission, ne peut être supérieur à un.

A l'issue des élections sénatoriales de septembre 2023, les mandats de sénatrice de Mmes Toine BOURRAT et Martine FILLEUL ont pris fin mais celles-ci ont continué de siéger au sein de la Commission jusqu'à la désignation de leurs successeurs comme le prévoit le règlement intérieur de la CSNP.

Le Président du Sénat a nommé, le 19 février 2024, les sept sénateurs au sein de la Commission supérieure :

M. Bernard DELCROS, Mme Patricia DEMAS, Mme Audrey LINKENHELD, M. Damien MICHALLET, M. Christian REDON-SARRAZY, M. Jean-Yves ROUX, Mme Denise SAINT-PÉ.

A la suite de la séance d'installation du 27 février 2024, les membres de la Commission supérieure ont élu M. Damien MICHALLET, Président de la CSNP, ainsi qu'un nouveau bureau :

- Mme Mireille CLAPOT, Députée de la Drôme, première vice-présidente ;
- M. Xavier BATUT, Député de la Seine-Maritime, deuxième vice-président ;
- M. Christian REDON-SARRAZY, Sénateur de la Haute-Vienne, secrétaire.

A l'issue des élections législatives de juin et juillet 2024, les mandats de député de Mme Mireille CLAPOT et M. Xavier BATUT ont pris fin mais ceux-ci ont continué de siéger au sein de la Commission jusqu'à la désignation de leurs successeurs comme le prévoit le règlement intérieur de la CSNP.

La Présidente de l'Assemblée nationale a désigné Mme Mireille Clapot au collège de l'ARCEP le 15 octobre 2024, ce qui a entrainé la fin de ses fonctions au sein de la CSNP.

La Présidente de l'Assemblée nationale a nommé, le 3 décembre 2024, sept députés au sein de la Commission : Mme Lisa BELLUCO, Mme Anne Le HENNANF, fM. Aurélien LOPEZ-LIGUORI, M. Jacques OBERTI, Mme Marie POCHON, M. Stéphane TRAVERT, M. Stéphane VOJETTA.

Les personnalités qualifiées désignées en juillet et septembre 2022 par le Ministre de l'Économie, des Finances et de la Souveraineté industrielle et numérique sont : M. Henri d'AGRAIN, Mme Jeanne BRETECHER, M. Patrick GUILLEMOT.

A la suite de la séance d'installation du 14 janvier 2025, les membres de la Commission supérieure ont réélu M. Damien MICHALLET, Président de la CSNP, ainsi qu'un nouveau bureau :

- M. Jacques OBERTI, Député de la Haute-Garonne a été élu premier vice-président
- Mme Anne LE HENANFF, Députée du Morbihan a été élue deuxième vice-présidente
- M. Christian REDON-SARRAZY, Sénateur de la Haute-Vienne, a été réélu secrétaire

MEMBRES

DÉPUTÉS :

Mme Lisa BELLUCO (Ecologiste et Social), Députée de la Vienne ; Secrétaire de la Commission du développement durable et de l'aménagement du territoire ; Membre de la CSNP depuis le 3 décembre 2024.

Mme Anne Le HENANFF (Horizons), Députée du Morbihan ; Membre de la commission de la défense nationale et des forces armées ; Deuxième vice-Présidente de la Commission supérieure du numérique et des postes; Présidente du groupe d'amitié France-Vietnam ; Vice-Présidente du groupe d'amitié France-Estonie ; Ancienne Conseillère régionale de Bretagne; Membre de la CSNP depuis le 22 octobre 2022.

M. Aurélien LOPEZ-LIGUORI (Rassemblement National), Député de l'Hérault ; Membre de la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République ; Vice-Président du groupe d'amitié France-Argentine ; Vice-Président du groupe d'amitié France-Estonie; Membre de la CSNP depuis le 22 octobre 2022.

M. Jacques OBERTI (Socialistes et apparentés), Député de Haute-Garonne ; Membre de la Commission des finances, de l'économie générale et du contrôle budgétaire; Premier vice-Président de la Commission supérieure du numérique et des postes; Membre de la CSNP depuis le 3 décembre 2024.

Mme Marie POCHON (Ecologiste et Social), Députée de la Drôme ; Membre de la Commission du développement durable et de l'aménagement du territoire; Membre de la CSNP depuis le 3 décembre 2024.

M. Stéphane TRAVERT (Ensemble pour la République), Député de La Manche ; Membre de la Commission des affaires économiques ; Ancien Ministre de l'Agriculture et de l'Alimentation ; Ancien Conseiller régional de Basse-Normandie ; Ancien Conseiller régional de Normandie; Membre de la CSNP depuis le 22 octobre 2022.

M. Stéphane VOJETTA (Ensemble pour la République), Député des Français de l'Etranger : Membre de la Commission des affaires économiques; Membre de la CSNP depuis le 3 décembre 2024.

M. Xavier BATUT (Horizons), Ancien Député de Seine-Maritime (2017-2024); Ancien vice-Président de la CSNP du 27 février 2024 au 3 décembre 2024; Ancien Secrétaire de la CSNP du 10 novembre 2022 au 27 février 2024; Ancien Membre de la Commission de la défense nationale et des forces armées; Membre de la CSNP jusqu'au 3 décembre 2024.

Mme Sophia CHIKIROU (La France Insoumise), Députée de Paris ; Membre de la Commission des affaires étrangères; Membre de la CSNP jusqu'au 3 décembre 2024.

Mme Mireille CLAPOT (Apparentée Renaissance), Ancienne Députée de la Drôme (2017-2024) ; Ancienne Présidente de la CSNP du 11 février 2021 au 27 février 2024 ; Ancienne vice-Présidente de la Commission des Affaires étrangères; Membre de la CSNP jusqu'au 15 octobre 2024.

Mme Angélique RANC (Rassemblement National), Députée de l'Aube ; Membre de la Commission des affaires sociales; Membre de la CSNP jusqu'au 3 décembre 2024.

Sénateurs :

M. Bernard DELCROS (Union Centriste), Sénateur du Cantal ; Membre de la Commission des finances ; Président de la délégation sénatoriale aux collectivités territoriales et à la décentralisation. Membre de la CSNP depuis le 21 septembre 2018.

Mme. Patricia DEMAS (Les Républicains), Sénatrice des Alpes-Maritimes ; Membre de la Commission des affaires sociales ; Membre de la délégation sénatoriale à la prospective; Membre de la CSNP depuis le 19 février 2024.

Mme. Audrey LINKENHELD (Socialiste, Ecologiste et Républicain), Sénatrice du Nord ; Membre de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale ; Membre de la Commission des affaires européennes; Membre de la CSNP depuis le 19 février 2024.

M. Damien MICHALLET (Les Républicains), Sénateur de l'Isère ; Président de la Commission Supérieure du Numérique et des Postes depuis le 27 février 2024 ; Membre de la Commission de l'aménagement du territoire et du développement durable ; Membre de la délégation sénatoriale aux entreprises; Membre de la CSNP depuis le 19 février 2024.

M. Christian REDON-SARRAZY (Socialiste, Écologiste et Républicain), Sénateur de la Haute-Vienne ; Secrétaire de la CSNP depuis le 27 février 2024 ; Membre de la commission des affaires économiques ; Membre de la délégation sénatoriale à la prospective; Membre de la CSNP depuis le 28 juillet 2021.

M. Jean-Yves ROUX (Rassemblement Démocratique et Social Européen), Sénateur des Alpes de Haute-Provence ; Vice-Président de la commission de l'aménagement du territoire et du développement durable ; Membre de la délégation sénatoriale aux collectivités territoriales et à la décentralisation; Membre de la CSNP depuis le 19 février 2024.

Mme Denise SAINT-PÉ (Union Centriste), Sénatrice des Pyrénées-Atlantiques ; Membre de la Commission de l'aménagement du territoire et du développement durable ; Ancienne Conseillère régionale de Nouvelle Aquitaine, Ancienne Vice-Présidente du Conseil général des Pyrénées-Atlantiques; Membre de la CSNP depuis le 21 septembre 2018.

PERSONNALITÉS QUALIFIÉES :

M. Henri d'AGRAIN, Délégué général du CIGREF.

Mme Jeanne BRETECHER, Présidente de Social Good Accelerator et Directrice conseil chez Jungle Coop/Coopaname

M. Patrick GUILLEMOT, Ancien Directeur Exécutif Appui et Soutien de la branche Grand Public et Numérique du Groupe La Poste – en retraite du groupe La Poste

SECRÉTARIAT GÉNÉRAL :

Mme Valérie MONTANÉ, Secrétaire générale.

M. Marc SIFFERT SIRVENT, Secrétaire général adjoint.

COMPOSITION DE LA CSNP JUSQU'AU 3 DECEMBRE 2024

Xavier BATUT
Député de Seine-Maritime

Sophia CHIKIROU
Députée de Paris

Mireille CLAPOT
Députée de la Drôme

Anne LE HENANFF
Député du Morbihan

Aurélien LOPEZ-LIGUORI
Député de l'Hérault

Angélique RANC
Député de l'Aube

Stéphane TRAVERT
Député de la Manche

Bernard DELCROS
Sénateur du Cantal

Patricia DEMAS
Sénatrice des Alpes-Maritimes

Audrey LINKENHELD
Sénatrice du Nord

Damien MICHALLET
Sénateur de l'Isère

Christian REDON-SARRAZY
Sénateur de la Haute-Vienne

Jean-Yves ROUX
Sénateur des Alpes de Haute-Provence

Denise SAINT-PÉ
Sénatrice des Pyrénées-Atlantiques

Henri D'AGRAIN
CIGREF

Jeanne BRETECHER
Présidente Social Good Accelerator

Patrick GUILLEMOT
Groupe La Poste

COMPOSITION DE LA CSNP AU 3 DECEMBRE 2024

Lisa BELLUCO
Députée de la Vienne

Anne LE HENANFF
Députée du Morbihan

Aurélien LOPEZ-LIGUORI
Député de l'Hérault

Jacques OBERTI
Député de la Haute-Garonne

Marie POCHON
Députée de la Drôme

Stéphane TRAVERT
Député de la Manche

Stéphane VOJETTA
Député établis hors de France

Bernard DELCROS
Sénateur du Cantal

Patricia DEMAS
Sénatrice des Alpes-Maritimes

Audrey LINKENHELD
Sénatrice du Nord

Damien MICHALLET
Sénateur de l'Isère

Christian REDON-SARRAZY
Sénateur de la Haute-Vienne

Jean-Yves ROUX
Sénateur des Alpes de Haute-Provence

Denise SAINT-PÉ
Sénatrice des Pyrénées-Atlantiques

Henri D'AGRAIN
CIGREF

Jeanne BRETECHER
Présidente Social Good Accelerator

Patrick GUILLEMOT
Groupe La Poste

LES MISSIONS DE LA CSNP

La Commission Supérieure du Numérique et des Postes (CSNP) est issue de la Commission Supérieure du Service Public des Postes et des Télécommunications (CSSPPT) créée par la loi n° 90-568 du 2 juillet 1990, relative à l'organisation du service public des postes et télécommunications.

La loi n°2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle a confirmé ses missions, en élargissant son domaine d'intervention aux communications électroniques.

Avec le vote de la Loi pour une République Numérique, en 2016, la Commission Supérieure du Service Public des Postes et des Communications Electroniques (CSSPPCE) devient la Commission Supérieure du Numérique et des Postes (CSNP). Ce changement de nom apporte à la Commission Supérieure une plus grande lisibilité de ses travaux dans un secteur où Numérique et Postes sont plus que jamais complémentaires.

L'article L125 du Code des postes et des télécommunications précise que la Commission supérieure du numérique et des postes veille à l'évolution équilibrée des secteurs des postes et des communications électroniques et étudie les questions relatives à la neutralité de l'internet.

Elle émet, à cette fin, un avis sur les projets de modification de la législation applicable à ces secteurs, sur les projets de cahier des charges de La Poste et des opérateurs chargés du service universel des communications électroniques et les projets de contrats de plan de La Poste.

Elle est consultée par les ministres chargés des postes et des communications électroniques lors de la préparation des directives communautaires relatives à ces secteurs.

Elle peut être consultée par l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse et par les commissions permanentes de l'Assemblée nationale et du Sénat sur les questions relevant de sa compétence.

Elle peut saisir l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse sur des questions concernant la compétence de cette autorité en matière de contrôle et de sanction du respect, par les opérateurs, des obligations de service public et de service universel qui leur sont applicables.

Elle peut suggérer les modifications de nature législative et réglementaire que lui paraît appeler l'évolution technologique, économique et sociale des activités postales et de communications électroniques.

Elle adresse des recommandations au Gouvernement pour l'exercice d'une concurrence loyale dans les activités postales et de communications électroniques.

Elle peut recueillir toutes les informations utiles à l'accomplissement de ses missions et notamment demander aux ministres chargés des postes et des communications électroniques de faire procéder à toute étude ou investigation concernant La Poste et les opérateurs chargés du service universel des communications électroniques.

Concrètement, quelles sont les méthodes de travail de la Commission supérieure du numérique et des postes ?

L'activité de la Commission supérieure est rythmée par les auditions organisées en séance plénière ou en groupe de travail.

Plusieurs groupes de travail ont été mis en place sur les sujets suivants :

- Intelligence artificielle
- les conséquences des coupes budgétaires sur le Plan France Très Haut Débit au regard des enjeux de déploiement de résilience et de la fermeture du réseau cuivre
- Transposition de la directive NIS 2
- Missions de services publics de la Poste
- Les enjeux politiques et économiques du schéma European Union Cybersecurity Certification Scheme for Cloud Services (EUCS)
- Inclusion numérique, médiation et citoyenneté numérique

Ces groupes de travail sont chacun pilotés par des membres de la Commission supérieure.

En quelques chiffres, l'activité de la CSNP en 2024 :

- 9 avis rendus,
- 9 séances plénières,
- 98 auditions et réunions en groupes de travail,
- 14 participations et interventions lors de colloques et salons thématiques.

Parce que les sujets traités par la Commission supérieure peuvent être extrêmement techniques, les membres de la commission supérieure associent à leurs auditions et à leurs travaux un groupe d'experts associés aux profils différents : M. Henri d'AGRAIN, Délégué général du CIGREF, Mme Jeanne BRETECHER, Présidente de Social Good Accelerator et Directrice conseil chez Jungle Coop/Coopaname et M. Patrick GUILLEMOT, ancien directeur exécutif Appui et soutien de la banche Grand Public et numérique du Groupe La Poste.

Ces personnalités qualifiées participent aux auditions et contribuent à l'élaboration des avis notamment les plus techniques.

Les domaines d'intervention

Sécurité numérique

Souveraineté numérique

Télécommunications

LA POSTE GROUPE

Missions de services publics de la Poste

Inclusion numérique, médiation et citoyenneté numérique

Intelligence artificielle

Numérique responsable et communs numériques

Sujets sociétaux et réglementaires.

L'activité de la CSNP en quelques chiffres

9 avis rendus

9 séances plénières

98 auditions et réunions en groupes de travail

14 participations et interventions lors de colloques et salons thématiques

LES MOYENS DE LA CNSP

L'article L125 du code des postes et des télécommunications électroniques précise que les moyens nécessaires au fonctionnement de la commission supérieure du numérique et des postes et à l'accomplissement de ses missions sont inscrits au budget des ministères chargés des postes et des communications électroniques.

Le plafond de crédit (frais de mission et frais de représentation) fixé au titre de l'année 2024 s'est élevé à 15 800 euros.

Le montant total des crédits de fonctionnement consommés se sont élevés à 11 220 euros en 2024 contre 18 213 euros en 2023 (Source : Ministère de l'économie, des finances et de la souveraineté industrielle et numérique).

Cette diminution de la consommation des crédits s'explique principalement par la baisse des frais de missions effectuées par la CSNP.

Les frais de représentation ont représenté 3 156 euros en 2024 contre 3 278 euros en 2023 (plafond des frais de représentations fixé à 3 500 euros par le Secrétariat général du Minefi en 2024).

Les frais de mission ont représenté 5 173 euros en 2024 contre 7 370 euros en 2023 (plafond des frais de missions fixé à 9 394 euros par le Secrétariat général du Minefi en 2024).

Conformément au décret n°2001-478 du 30 mai 2001, l'indemnisation des personnalités qualifiées a représenté une enveloppe annuelle de 16 453,80 euros en 2024.

Au 31 décembre 2024, les effectifs de la CSNP étaient composés de deux emplois temps plein (une secrétaire générale et un secrétaire général adjoint).

Les personnels du Secrétariat général de la CSNP sont mis à disposition par le Ministère de l'Economie, des Finances et de la Souveraineté industrielle et numérique.

LES PRIORITÉS DE LA CSNP

Pour mieux encadrer l'usage de l'intelligence artificielle

Entretien avec Mme Mireille CLAPOT, Ancienne Députée de la Drôme et ancienne Présidente de la CSNP

© Mireille CLAPOT, Assemblée nationale

Pourquoi est-il crucial d'encadrer le développement de l'intelligence artificielle aujourd'hui ?

Avec mes collègues de la CSNP, nous avons souhaité nous saisir de ce sujet car nous considérons que le développement de l'IA, et plus particulièrement de l'IA générative, représente un saut technologique majeur avec des implications profondes pour nos sociétés et démocraties. Bien que les opportunités soient immenses, il existe également des risques, notamment en termes de protection des libertés fondamentales, de souveraineté numérique et d'impact environnemental. Une régulation adaptée est essentielle pour équilibrer la protection des droits individuels et la promotion de l'innovation. Cet équilibre permettra de tirer parti des avantages de l'IA tout en minimisant ses effets négatifs, tels que les biais ou les abus d'utilisation.

Quels sont les principaux défis liés à une régulation européenne de l'IA ?

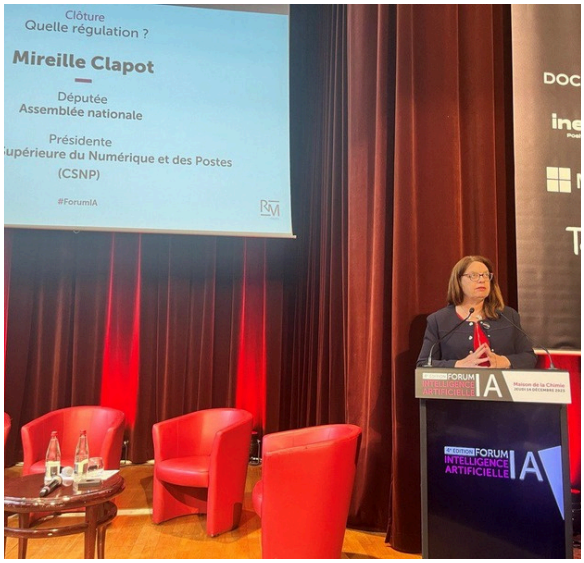
L'un des principaux défis est de trouver un compromis entre deux visions opposées : une régulation très stricte pour protéger les droits individuels et une approche plus permissive pour stimuler l'innovation. Le règlement européen sur l'IA, connu sous le nom d'IA Act, vise à établir un cadre équilibré en classant les usages de l'IA selon leur niveau de risque, allant des applications interdites aux applications à haut risque. Cependant, il reste des enjeux, comme l'articulation entre régulations nation-ales et européennes et l'adaptation des règles règles aux évolutions rapides de la technologie. Une flexibilité réglementaire est donc nécessaire pour éviter de freiner la recherche et l'innovation.

Quelles recommandations sont proposées pour stimuler le développement d'une IA européenne ?

L'avis met en avant plusieurs recommandations, comme l'accélération de l'accès aux jeux de données, le renforcement des financements pour la recherche et le soutien aux startups innovantes. Par exemple, il est crucial de faciliter la collecte et le partage de données, tout en respectant les normes de confidentialité. De plus, des initiatives telles que la revalorisation des salaires des chercheurs français et le développement de centres européens de supercalculateurs sont préconisées. Ces actions visent à rattraper le retard sur les géants technologiques américains et chinois tout en assurant une souveraineté numérique européenne.

Comment l'avis aborde-t-il les impacts sociaux et environnementaux de l'IA ?

L'IA a des répercussions sociales profondes, notamment sur l'emploi et les compétences, avec un potentiel de création et de destruction d'emplois. L'avis insiste sur l'importance de la formation continue et de la reconversion pour anticiper ces transformations. Sur le plan environnemental, l'IA offre des opportunités, comme l'optimisation des ressources, mais engendre également des défis, tels que la consommation d'énergie et d'eau des centres de données, et la consommation de terres rares. L'avis recommande la création d'un consortium dédié à l'IA frugale et le développement d'un référentiel international pour mesurer l'impact carbone de l'IA.



Quelle est votre vision concernant l'utilisation de l'IA dans les services publics ?

L'avis encourage l'intégration progressive de l'IA dans les services publics pour améliorer leur efficacité et simplifier les démarches administratives. Toutefois, il souligne la nécessité de maintenir un contrôle humain sur les décisions administratives et d'assurer une transparence totale vis-à-vis des citoyens. Par exemple, les initiatives en cours, comme l'utilisation d'IA générative pour répondre aux usagers, montrent des résultats prometteurs. Mais l'avis rappelle l'importance de former les agents publics et de veiller à éviter les biais dans les systèmes d'IA utilisés.

➡ **Avis n°2024-01 du 17 janvier 2024** « Pour mieux encadrer l'usage de l'intelligence artificielle »

Les conséquences des coupes budgétaires sur le Plan France Très Haut Débit au regard des enjeux de déploiement, de résilience et de la fermeture du réseau cuivre

Entretien avec M. Xavier BATUT, Ancien député de Seine-Maritime et vice-Président de la CSNP

© Xavier BATUT Assemblée nationale

Quels sont les principaux impacts des coupes budgétaires sur le Plan France Très Haut Débit ?

Les coupes budgétaires annoncées début 2024, totalisaient 155 millions d'euros, représentent une menace pour l'achèvement du plan prévu pour fin 2025. Pour rappel, afin d'atteindre cet objectif, le plan mobilise, au total, un investissement de plus de 35 milliards d'euros partagé entre les opérateurs privés à hauteur de 22,4 milliards €, les collectivités territoriales à hauteur de 8,84 milliards €, l'Etat à hauteur de 3,5 milliards € et l'Europe à hauteur de 0,55 milliards €. Si les investissements massifs des opérateurs privés, des collectivités territoriales et de l'Etat sont à saluer, il n'en demeure pas moins qu'il reste encore beaucoup à faire et le plus difficile reste à venir. En effet, la complétude des déploiements ne pourra être atteinte si le financement des raccordements complexes, en domaine public et privé, n'est pas rapidement mis en œuvre, en trouvant une source de financement à la hauteur des enjeux. Aussi, bien que les ajustements financiers annoncés pour 2024 aient été présentés comme n'ayant pas d'impact immédiat, ils risquent toutefois d'impacter les phases critiques du projet, notamment les raccordements complexes en zones rurales ou privatives. Ainsi, sans réintégration de ces financements dans le prochain budget 2025, la transition vers le « 100 % raccordés » pourrait être retardée, aggravant encore les inégalités numériques. Ces restrictions budgétaires arrivent à un moment où la fermeture progressive du réseau cuivre impose des investissements supplémentaires pour garantir une transition réussie.

Pourquoi le financement des raccordements complexes est-il essentiel ?

Les raccordements complexes concernent des zones où les coûts d'installation sont élevés, souvent en raison de l'éloignement ou de la dispersion des habitations. Ces déploiements, estimées à environ 440 000 foyers, ont nécessité des moyens financiers importants. Le coût moyen d'un raccordement complexe varie entre 2 000 et 3 000 euros, bien au-delà des coûts standards. Si ces besoins ne sont pas financés, des foyers, notamment en milieu rural, risquent d'être laissés de côté. Une enveloppe budgétaire spécifique est recommandée pour accompagner ces raccordements et éviter que des ménages modestes ne soient exclus de l'accès au Très Haut Débit. Pour apporter une réponse à ce problème des raccordements complexes dans le domaine privatif, le gouvernement a inscrit dans le projet de loi de finances pour 2025, 16,1 millions d'euros pour soutenir le lancement d'un dispositif expérimental de soutien au financement des raccordements complexes en domaine privé, tel que nous le recommandions dans notre avis d'octobre 2023.

Quels mécanismes sont proposés pour assurer l'équité entre les zones rurales et urbaines ?

La Commission préconise de renforcer le mécanisme de péréquation pour compenser les surcoûts dans les zones rurales, où les infrastructures existantes, souvent inadaptées, nécessitent des travaux supplémentaires. Le fonds d'aménagement numérique des territoires (FANT), créé en 2009 mais jamais utilisé, pourrait être activé pour financer ces ajustements. De plus, il est crucial que l'ARCEP et les pouvoirs publics surveillent les ajustements tarifaires pour éviter que les opérateurs ne répercutent ces coûts sur les consommateurs en zone rurale, aggravant ainsi la fracture numérique.

Comment les coupes budgétaires pourraient impacter la résilience et la sécurité des réseaux ?

La résilience des réseaux, essentielle face aux aléas climatiques et aux actes de malveillance, nécessite des investissements continus. Les récents actes de vandalisme, avec 550 incidents recensés entre novembre 2023 et février 2024, illustrent la fragilité des infrastructures. L'entretien et la sécurisation des réseaux, comme l'enfouissement des lignes ou la prévention des sabotages, nécessiteront une évaluation approfondie des coûts et un renforcement des sanctions pénales. Sans ces mesures, les réseaux risquent de devenir vulnérables, mettant en péril leur durabilité et leur efficacité.

➡ **Avis n°2024-04 du 6 juin 2024** sur les conséquences des coupes budgétaires sur le Plan France Très Haut Débit au regard des enjeux de déploiement de résilience et de la fermeture du réseau cuivre.

Quelle est la position de la Commission sur la fermeture du réseau cuivre ?

La Commission soutient la fermeture progressive du réseau cuivre, prévue pour 2030, à condition que la fibre soit intégralement déployée dans les zones concernées. Cependant, des obstacles, comme le refus de certaines copropriétés ou l'absence de données précises sur les locaux raccordés, compliquent cette transition. La Commission recommande que Orange améliore la qualité de sa base de données en cuivre pour faciliter la planification et propose que les coûts des raccordements optiques soient supportés par les demandeurs en cas de refus initial proposé par l'opérateur d'infrastructure. Cette approche vise à garantir une transition ordonnée et équitable pour tous les usagers.

Sur les enjeux politiques et économiques du schéma européen de certification de sécurité des services Cloud

Entretien avec M Henri d'Agrain, Membre de la CSNP, Délégué général du CIGREF

© HENRI D'AGRAIN

Pourquoi le schéma européen de certification des services cloud (EUCS) est-il essentiel pour la souveraineté numérique de l'Europe ?

L'EUCS vise à garantir un haut niveau de sécurité, de confidentialité et de conformité pour les services cloud utilisés en Europe. Il est crucial dans le contexte d'une dépendance croissante envers les opérateurs étrangers, principalement américains. L'intégration d'un niveau de certification "High+" dans ce schéma permettra de protéger les données sensibles contre des législations non européennes à portée extraterritoriale, telles que la section 702 du FISA aux États-Unis. En renforçant la souveraineté numérique, l'Europe pourrait ainsi réduire les risques de surveillance économique et renforcer son industrie locale des services cloud, indispensables pour sa compétitivité et sa sécurité.

Quels sont les principaux risques identifiés si le niveau High+ de l'EUCS n'est pas adopté ?

L'absence du niveau High+ exposerait les données sensibles des entreprises et administrations européennes face aux risques d'ingérences étrangères. De plus, cela affaiblirait la compétitivité des acteurs européens face aux géants du cloud américain et chinois, renforçant ainsi leur domination. Par ailleurs, l'impossibilité de garantir une protection robuste des données stratégiques pourrait dissuader de nombreux organismes d'externaliser leurs projets sensibles. Enfin, cela compromet l'autonomie technologique de l'Union européenne, la rendant vulnérable aux pressions géopolitiques mais aussi créé un désavantage économique face aux grands acteurs extra-européens.

Quelles critiques ont été formulées contre le niveau High+ par les opposants internationaux et européens ?

Aux États-Unis, des associations professionnelles ont dénoncé le niveau High+ comme un moyen de désavantager les entreprises américaines au profit des alternatives locales, compromettant les intérêts économiques et sécuritaires américains. Sur le plan européen, certains États membres craignent des tensions avec les États-Unis ou des restrictions sur leurs exportations. De plus, certains acteurs économiques, fortement liés au marché américain, redoutent des représailles commerciales. Ces critiques montrent une divergence entre les intérêts stratégiques européens et les dépendances économiques individuelles.

Quelles recommandations clés la Commission supérieure du numérique et des postes formule-t-elle sur l'EUCS ?

La CSNP recommande de maintenir le niveau High+ dans le schéma EUCS pour garantir l'immunité contre les législations extraterritoriales. Elle appelle le gouvernement à clarifier sa position et à inciter les États membres de l'UE opposés à ce niveau à justifier leur position. La CSNP propose également une analyse approfondie des conséquences économiques et géopolitiques liées à l'absence de ce niveau. Enfin, elle demande une évaluation des risques associés à l'adoption du High+ dans le cadre des accords internationaux, tout en insistant sur la nécessité d'un schéma renforçant l'autonomie technologique européenne.

➡ **Avis n°2024-05 du 4 septembre 2024** sur les enjeux politiques et économiques du schéma EUCS

La mission d'aménagement du territoire confiée au Groupe La Poste et la méthode d'évaluation du Service Universel Postal

Entretien avec M Stéphane TRAVERT, député de la Manche, Membre de la CSNP et Président de l'Observatoire national de la présence postale (ONPP)

© Stéphane TRAVERT, Assemblée nationale

Pourquoi la méthode d'évaluation du coût net du service universel postal est-elle un enjeu central pour La Poste et l'État ?

La méthode d'évaluation du coût net du service universel postal est essentielle pour garantir une juste compensation des missions de service public confiées à La Poste. Depuis 2018, le service universel postal est déficitaire en raison de la baisse importante des volumes de courrier, ayant perdu plus de 6 milliards d'euros de recettes en dix ans. En 2022, le déficit s'élevait à 703 millions d'euros. L'État a le devoir de compenser ce déficit pour maintenir la qualité et la pérennité de ce service essentiel. Après avoir été saisie les 4 mars 2024, la Commission supérieure du numérique et des postes a été une nouvelle fois saisie le 31 mai 2024, puis le 19 juillet 2024 par la Direction générale des entreprises en vue de rendre un avis sur le projet de décret relatif à la méthode d'évaluation du coût net lié aux obligations de service universel postal, pris en application de l'article L. 2-2 du Code des postes et des communications électroniques (CPCE).

La CSNP dans son avis rappelle que le projet de décret introduit des critères spécifiques pour évaluer la "charge financière inéquitable" et indique que ces critères suscitent des inquiétudes quant à leurs compatibilités avec une compensation équitable.

Quels sont les principaux points de désaccord soulevés par la Commission supérieure sur le projet de décret relatif au service universel postal ?

La Commission critique plusieurs aspects du projet de décret, notamment l'introduction de critères comme le seuil de 1 % du chiffre d'affaires pour caractériser une charge financière inéquitable. Nous estimons que cette approche est restrictive et pourrait limiter les compensations nécessaires. De plus, nous notons que certains critères s'inspirent de pays européens où le cadre est très différent, ce qui pourrait constituer une surtransposition des directives européennes. Enfin, nous insistons sur le fait que la notion de charge financière inéquitable devrait être reconnue dès qu'une perte non compensée survient.

Vous avez rendu un autre avis concernant la mission d'aménagement du territoire confiée au Groupe La Poste. Pouvez-vous rappeler comment est évalué le coût net de la mission d'aménagement du territoire, et quels défis sont identifiés pour 2023 ?

Le coût net de la mission d'aménagement du territoire est évalué en modélisant trois réseaux théoriques : le réseau commercial, le réseau d'accessibilité et le réseau complémentaire. En 2023, ce coût est estimé à 322 millions d'euros par l'Arcep, mais l'État n'a compensé que 164 millions d'euros via le fonds postal de péréquation. Les principaux défis incluent la baisse constante de l'activité dans les points de contact et l'augmentation des charges en raison de l'inflation. Ces facteurs mettent en péril la qualité et la disponibilité du service, tout en fragilisant économiquement La Poste.

Quels sont les points positifs relevés par la Commission dans la gestion des missions de La Poste ?

La Commission note avec satisfaction la convergence entre les évaluations du coût net fournies par La Poste et l'Arcep, témoignant d'une méthodologie solide et d'une transparence accrue. Elle salue également les efforts de transformation et d'adaptation de La Poste face à la baisse de fréquentation, notamment par le développement de formes de présence innovantes comme la mutualisation des services. Ces initiatives sont perçues comme prometteuses pour maintenir un service de qualité tout en optimisant les ressources.

Quelles recommandations principales la Commission formule-t-elle pour garantir l'équilibre des missions de service public de La Poste ?

La Commission recommande une juste et complète compensation des coûts réels liés aux missions de service public. Elle appelle l'État à respecter ses engagements financiers, notamment via une dotation annuelle de 174 millions d'euros au fonds national de péréquation territoriale. Elle préconise également l'intégration d'indicateurs de qualité reflétant la satisfaction des utilisateurs. Enfin, elle encourage La Poste à poursuivre sa transformation, tout en veillant à préserver la présence et l'efficacité des services sur l'ensemble du territoire.

➡ **Avis n°2024-06 du 26 juillet 2024** sur le décret relatif à la méthode d'évaluation du Service Universel Postal

➡ **Avis n°2024-09 du 11 décembre 2024** sur le cout net de la mission d'aménagement du territoire confiée au Groupe La Poste en 2023

Les enjeux de la transposition de la Directive NIS (Network & Information Security) 2 en France

Entretien avec Mme Anne LE HENANFF, Vice Présidente de la CSNP, Députée du Morbihan

© Anne LE HENANFF

Pourquoi la directive NIS 2 en France est-elle jugée essentielle par la CSNP ?

La directive NIS 2 marque un véritable tournant et représente un levier important pour renforcer la cybersécurité en Europe. Son importance est particulièrement reconnue en France car elle élargit son champ d'application de 600 entités sous NIS 1 à environ 15 000, incluant des entreprises et des collectivités locales. Ce changement d'échelle vise à harmoniser les normes de sécurité numérique et à protéger les secteurs critiques comme la santé, l'énergie et d'autres secteurs essentiels. Nous estimons que cette transposition est essentielle pour relever collectivement le niveau de résilience face à la hausse des cyberattaques. En renforçant les obligations de sécurité, elle contribue à protéger les données sensibles et à sécuriser les infrastructures critiques.

Quels sont les principaux défis identifiés pour les entités concernées par NIS 2 ?

L'extension du périmètre de la directive NIS 2 pose plusieurs défis. Tout d'abord, de nombreuses entreprises et collectivités locales ne disposent pas actuellement des moyens humains, techniques et financiers suffisants pour répondre aux nouvelles obligations. Le manque de sensibilisation et d'accompagnement aggrave ce problème, notamment pour les petites structures. Ensuite, les exigences de notification rapide des incidents et de mise en conformité, avec des délais perçus comme contraints, peuvent inquiéter. Enfin, les entités doivent également gérer la complexité de leurs relations avec les sous-traitants, notamment pour garantir leur conformité. Ces défis soulignent l'importance d'un accompagnement technique et financier adapté.

Quels outils ou mesures la CSNP recommande-t-elle pour faciliter la mise en œuvre de la directive NIS 2 ?

La Commission propose plusieurs recommandations pour soutenir les entités concernées. Une campagne nationale de communication est préconisée pour informer sur les nouvelles obligations et sensibiliser aux enjeux de cybersécurité. Elle suggère également la création d'un guichet unique pour simplifier la déclaration des incidents, et l'uniformisation des formulaires pour réduire la charge administrative. Par ailleurs, la mise en place d'un système de labellisation NIS 2 pourrait encourager les entités qui se sont conformées à la directive à valoriser leurs efforts. La CSNP insiste également sur le rôle renforcé de l'ANSSI pour accompagner les petites structures dans leur transition.

Pourquoi le délai de mise en conformité fixé au 31 décembre 2027 est-il recommandé ?

La CSNP recommande un délai de mise en conformité jusqu'au 31 décembre 2027 afin de permettre aux entreprises et collectivités d'acquérir les moyens nécessaires, de disposer d'un temps d'adaptation et d'investir dans des solutions techniques adaptées. L'expérience avec la directive NIS 1 a montré que des délais trop courts peuvent freiner l'efficacité de la mise en œuvre. En introduisant un calendrier progressif avec des étapes intermédiaires, les entités auront le temps de s'adapter aux exigences tout en maintenant leurs activités essentielles.

© Jennifer CHRETIEN © Vincent STRUBEL

Quelles sont les principales préoccupations liées aux interactions entre NIS 2 et d'autres régulations, comme le règlement DORA (Digital Operational Resilience Act) ?

Un point de vigilance soulevé concerne les risques de double régulation pour certains secteurs, comme les assurances, soumis à la fois à NIS 2 et au règlement DORA, qui entrera en vigueur en janvier 2025. La CSNP souligne qu'un chevauchement entre ces deux cadres législatifs pourraient entraîner une insécurité juridique et des coûts supplémentaires pour les entreprises françaises, les désavantageant face à leurs concurrents européens. Elle recommande de clarifier les limites respectives de NIS 2 et DORA pour éviter les redondances et de privilégier une approche harmonisée à l'échelle européenne afin de renforcer la compétitivité.

➡ **Avis n°2024-07 du 3 octobre 2024** sur les enjeux de la transposition de la directive NIS 2 en France

Pour une politique nationale d'inclusion numérique adaptée aux besoins de nos concitoyens

Entretien avec M. Christian REDON-SARRAZY, Sénateur de la Haute-Vienne, Secrétaire de la CSNP

© Christian REDON-SARRAZY, Sénat

Pourquoi une politique nationale d'inclusion numérique est-elle essentielle en France ?

La CSNP a souhaité créer un groupe de travail dont j'étais le pilote avec Jeanne BRETECHER, personnalité qualifiée, afin de se saisir du sujet de l'inclusion numérique en France, suite au projet de loi de finances 2025 qui laissait peser de vives inquiétudes avec une baisse drastique des crédits allouées à cette politique. En effet, environ 25 % des Français rencontrent des difficultés pour utiliser pleinement les outils numériques, selon le Baromètre du numérique présenté par le Crédoc. Ce chiffre révèle une fracture numérique qui empêche l'accès équitable aux services, publics et marchands, essentiels dans notre société de plus en plus digitalisée. Les démarches administratives dématérialisées, souvent complexes, aggravent le non-recours aux droits sociaux, comme le RSA ou le minimum vieillesse. Une politique d'inclusion numérique permet d'assurer l'égalité des droits, de maintenir des points de contact physiques et téléphoniques, et de simplifier les interfaces numériques pour répondre aux besoins de tous, et en particulier pour les populations précaires et en situation d'handicap. Au regard de ces constats, il nous a paru primordial de traiter ce sujet essentiel d'égalité face aux droits.

Quels sont les impacts des coupes budgétaires sur le dispositif d'inclusion numérique ?

La réduction des crédits dédiés au programme « Numérique Ensemble » de 62 millions à 27 millions d'euros met en péril des initiatives clés, comme le déploiement des conseillers numériques. Ces derniers ont accompagné plus de 2 millions de citoyens, mais leur nombre pourrait diminuer drastiquement, affectant particulièrement les zones rurales et les publics précaires. Cette coupe budgétaire anéantirait quatre ans d'investissements de l'État et compromettrait les objectifs fixés, tels que l'accompagnement de 8 millions de personnes d'ici 2027. Les acteurs locaux, déjà sous pression budgétaire, ne pourront compenser cette baisse, mettant en danger la continuité des efforts en matière d'inclusion numérique.

© Mission locale rurale à Aixe-sur-Vienne

Quels sont les principaux axes d'amélioration proposés pour renforcer l'inclusion numérique ?

La CSNP propose effectivement plusieurs recommandations, notamment de garantir des alternatives aux démarches dématérialisées, comme des points de contact physiques et téléphoniques. Egalement, la Commission propose de simplifier les procédures administratives et de rendre les interfaces numériques accessibles, notamment aux personnes en situation de handicap. Elle recommande également de rétablir le financement à hauteur de 62 millions d'euros et de créer un fonds national d'inclusion numérique pour agréger des financements publics, privés et européens. Enfin, le développement de la formation des conseillers numériques, notamment pour accompagner des publics spécifiques comme les personnes handicapées, est essentiel pour pérenniser les avancés.

Comment le dispositif des conseillers numériques contribue-t-il à réduire la fracture numérique ?

Les conseillers numériques jouent un rôle central dans l'accompagnement des publics éloignés du numérique. Ils ont permis à 97% des bénéficiaires de progresser dans leur utilisation des outils numériques et à 83 % d'entre eux de se sentir plus à l'aise. Ce dispositif, qui couvre aujourd'hui 98% des accompagnements réalisés, est essentiel pour atteindre les objectifs de la feuille de route "Numérique Ensemble". Leur capacité à se déplacer et à offrir des formations adaptées, individuellement ou collectivement, fait d'eux un maillon clé de l'inclusion numérique. Cependant, leur précarisation et les réductions budgétaires compromettent la pérennité de ce service indispensable.

Quels mécanismes financiers pourraient soutenir une politique durable d'inclusion numérique ?

La CSNP préconise plusieurs mesures pour assurer un financement durable. Elle suggère la création d'un fonds national d'inclusion numérique piloté par la Banque des Territoires pour mobiliser des fonds publics et privés, ainsi que des contributions européennes. Une taxe "numériseur-payeur", ciblant les grandes entreprises du numérique, pourrait être instaurée pour redistribuer une partie des gains économiques réalisés grâce à la digitalisation. Par ailleurs, flécher les recettes des sanctions pour non-conformité en matière d'accessibilité numérique vers des projets d'inclusion est une autre piste envisagée. Ces mécanismes permettront de répondre aux besoins croissants d'un public vulnérable, tout en renforçant la cohésion sociale.

➡ **Avis n°2024-08 du 28 novembre 2024** « Pour une politique nationale d'inclusion numérique adaptée aux besoins de nos concitoyens »

AGENDA 2024

JANVIER

17 janvier
- Publication de l'avis « Pour mieux encadrer l'usage de l'intelligence artificielle ».

23 janvier
- Participation au Cybercercle : La cyberdéfense dans l'armée de Terre.

25 janvier
- Participation au colloque "L'intelligence artificielle en 2050" Espace Diderot.

30 janvier
- Participation à l'ONPP.

31 janvier
- Publication du Rapport annuel 2023.
- Réunion de travail avec le groupe Altitude.

FÉVRIER

1 février
- Participation à l'instance de concertation réseaux fixes - MINEFI.

7 février - 9 février
- Participation au Salon international sur l'intelligence artificielle à Cannes.

19 février
- Réunion de travail sur le colloque "2040, l'ambition des réseaux durables".

20 février
- Réunion de travail avec la Direction générale des entreprises.

22 février
- Réunion de travail avec Infranum.

27 février
- Séance d'installation des nouveaux membres élus du Bureau de la CSNP.

28 février
- Présidence de la matinale du Cybercercle : "Economie numérique et politiques publiques".

MARS

6 mars
- Participation de M. Xavier BATUT, Vice-président de la CSNP, à la table ronde « Imaginons l'évolution des réseaux pour les territoires de demain 2024 : l'ambition des réseaux durables » organisée par Infranum.

7 mars
- Réunion de travail avec Infranum.

12 mars
- Participation à la 11ème édition du Baromètre de la confiance des Français dans le numérique.

13 mars
- Petit-déjeuner organisé par la CSNP visant à partager les recommandations de l'avis n°2024-01 « Pour mieux encadrer l'usage de l'IA », avec la participation de Mme Amélie de MONTCHALIN, représentante permanente de la France auprès de l'OCDE.

14 mars
- Réunion de travail avec le groupe Orange.
- Réunion de travail avec la DGE sur le Service universel postal.

19 mars
- Audition de M. Vincent STRUBEL, Directeur général de l'ANSSI.

20 mars
- Participation au Cybercercle.
- Audition de Mme Laure de LA RAUDIERE, Présidente de l'ARCEP.
- Audition de M. Zacharia ALAHYANE, directeur de la mission France Très Haut Débit à l'ANCT.

21 mars
- Participation à l'instance de concertation réseaux mobiles - MINEFI.
- Audition de Maître Alexandra ITEANU.

25 mars
- Audition de M. Gabriel GOUDY, Directeur général de Nouvelle Aquitaine THD.

26 mars
- Audition de Mme Marina FERRARI, Secrétaire d'État chargée du numérique.

27 mars
- Intervention de Mme. Mireille CLAPOT, Députée de la Drôme et vice-présidente de la CSNP, au Forum International de la Cybersécurité (FIC).

28 mars
- Audition de M. Patrick CHAIZE, sénateur, vice-président de la FNCCR.

AVRIL

2 avril
- Réunion de bureau de la CSNP
- Audition des associations représentant les collectivités locales (ADF, AMF, AVICCA, FNCCR, INTERCO, Régions de France, France urbaine).

3 avril
- Audition de Renaissance numérique.
- Participation de la CSNP à la réunion de l'ONPP.

4 avril
- Audition des représentants d'ADN OUEST, du CIGREF, du CDSE et du CYBERCERCLE.
- Audition de la Fédération française des télécoms.
- Audition de M. Philippe LE GRAND, président d'INFRANUM.

9 avril
- Audition de M. Philippe WAHL, Président du Groupe la Poste.

10 avril
- Participation à une matinée dédiée à la cybersécurité au CyberCampus.
- Petit-déjeuner débat autour des priorités du secteur des télécoms

15 avril
- Publication de l'avis relatif au projet de décret sur la méthode d'évaluation de la mission du SUP.

24 avril
- Participation et propos introductifs de M. Xavier BATUT, vice-président de la CSNP, au colloque « Infrastructures numériques : Former aujourd'hui pour préparer demain » organisé par le Cercle CREDO et Objectif Fibre.
- Audition conjointe de l'AFNIC, l'AFNUM, la FFT, le FIEEC, France Digitale, Hexatrust, et NUMEUM.
- Audition de M. Vincent TRELY, Président de l'Association pour la sécurité des SI des professions de santé (APSSIS) et de M. Jean-Sylvain CHAVANNE, RSSI du CHRU de Brest.

25 avril
- Audition du groupe Altitude.
- Audition du groupe Orange.
- Participation à l'instance de concertation réseaux fixes - MINEFI.

MAI

14 mai
- Audition conjointe de représentants de la CPME et du MEDEF.

15 mai
- Audition du Président de la CSNP au Sénat sur la loi simplification.
- Audition de France Assureurs.

16 mai
- Participation au Cybercercle : Échanges autour de NIS 2.

17 mai
- Participation à la présentation du référentiel écoconception de services numériques.

21 mai
- Audition des Clouders extra-européens (Microsoft, Google Cloud, AWS, Huawei).
- Audition de M. Antoine Jourdan, Sous-directeur des communications électroniques et des postes – DGE.

22 mai
- Audition des cabinets de conseils EY, Onepoint, Wavestone.
- Publication de l'avis relatif au titre II du projet de loi relatif à la résilience des activités d'importance vitale, à la protection des infrastructures critiques, à la cybersécurité et à la résilience opérationnelle numérique du secteur financier.

23 mai
- Délégation de la CSNP au salon Vivatech.

28 mai
- Participation au Trip de l'Avicca.

29 mai
- Audition des éditeurs de logiciels Arpege, Berger-Levrault, Egerie.

30 mai
- Audition des clouders UE (OVH, Docaposte, Outscale, Scaleway, Cloud Temple).

JUIN

4 juin
- Audition de Mme. Laure de La Raudière, Présidente de l'ARCEP.

6 juin
- Publication de l'avis sur les conséquences des coupes budgétaires sur le Plan France Très Haut Débit, au regard des enjeux de déploiement, de résilience et de la fermeture du réseau cuivre.
- Présidence et participation aux Assises du très haut débit et des Infrastructures du Numérique 2024.
- Participation à l'instance de concertation réseaux mobiles - MINEFI.

12 juin
- Réunion de l'observatoire national de la présence postale (ONPP) au Mémorial de Caen.

13 juin
- Visite de la plateforme industrielle de La Poste à Colombelles (14).
- Visite de la La Poste Agence Communale intégrée dans un tiers lieu avec France Services de Merville-Franceville (14).
- Réunion entre les membres de l'ONPP et l'ensemble des Présidents de CDPPT de Normandie.

20 juin
- Participation au Cybercercle : Intelligence économique des acteurs de la Défense à l'heure du numérique : de la résilience à l'offensif.
- Participation à une conférence sur l'IA : quels enjeux pour les territoires numériques et les télécommunications ? Maison de l'Alsace.

21 juin
- Réunion de travail avec La Poste.

JUILLET

2 juillet
- Participation à la 5ème édition du baromètre « la fibre en entreprise ».

3 juillet
- Réunion de travail avec la DGE sur le Service Universel Postal.

12 juillet
- Réunion de travail avec le Centre pour la Cybersécurité belge, autorité nationale en charge de la cybersécurité en Belgique.

24 juillet
- Séance plénière, examen du projet d'avis sur le projet de décret transmis par la DGE sur la compensation du Service Universel Postal.

26 juillet
- Publication de l'avis sur le projet de décret relatif à la méthode d'évaluation utilisée pour le calcul du cout net de la mission de Service Universel Postal.

ÂOUT

28 août
- Séance plénière - Examen d'un projet d'avis sur les enjeux politiques et économiques du le schéma européen de certification de sécurité des services Cloud dit EUCS.

Les enjeux de la transposition de la directive NIS 2 en France

SEPTEMBRE

4 septembre
- Publication de l'avis sur les enjeux politiques et économiques du schéma européen de certification de sécurité des services Cloud

5 septembre
- 10ème édition des Universités d'été de la Cybersécurité et du Cloud de Confiance

11 septembre au 13 septembre
- Déplacement de la CSNP à Copenhague dans le cadre de l'ONPP.

18 septembre
- Séance plénière : examen d'un projet d'avis sur les enjeux de la transposition de la directive NIS 2 en France.
- Réunion de travail avec Infranum.

20 septembre
- Réunion de travail avec la CPME Ile de France.

26 septembre
- Participation à la réunion de rentrée de l'ARCEP.

OCTOBRE

3 Octobre
- Publication de l'avis sur les enjeux de la transposition de la directive NIS 2 en France.
- Table ronde de présentation de l'avis sur les enjeux de la transposition de la Directive NIS 2 en France

8 Octobre
- Réunion de travail avec la DGE.

10 octobre
- Participation à l'instance de concertation réseaux fixes - MINEFI.

14 octobre
- Audition de M. Laurent ROJEY, Directeur général délégué Numérique de l'ANCT, et Mme Léa GISLAIS, Co-Directrice Programme Société numérique de l'ANCT.

15 Octobre au 16 octobre
- Université d'Infranum à Strasbourg.

18 octobre
- Participation à l'instance de concertation réseaux mobiles - MINEFI.

21 octobre
- Audition de M. Christophe GENTER, M. François BLOUVAC, Mme Emmanuelle BORRELLY, Mme Sacha DESMARIS et Mme Julie STEIN de la Banque des territoires.

23 octobre
- Participation à la réunion de l'ONPP et des CDPPT.

24 octobre
- Réunion de travail avec l'ANCT.

28 octobre
- Audition de M. Michel SAUVADE, Co-Président de la commission numérique de l'AMF, et Mme Céline COLUCCI, Déléguée générale d'Interconnectés.

29 octobre
- Audition de M. Jan BÜSCHER, Directeur général de la Mednum, et Mme Mélusine BLONDEL, Co-Directrice générale de la Mednum.

30 octobre
- Participation au Cybercercle : IA & cybersécurité pour la Défense.
- Audition de Mme Isabelle LHERBIER, Directrice des relations opérateurs publics et privés et de Mme Rebecca PERES, Déléguée aux affaires territoriales et parlementaires du Groupe La Poste.

NOVEMBRE

6 novembre au 7 novembre
- Mission de la CSNP en Haute-Vienne.
- Rencontre avec des représentantes du Conseil départemental de la Haute-Vienne
- Rencontre avec les représentants de la mission locale rurale de Limoges à Aixe-sur-Vienne
- Rencontre avec Mme Anne-Sophie MARCON, Sous-Préfète en charge du numérique
- Rencontre avec les représentants de la Mairie de Rilhac-Rancon
- Rencontre avec les représentants de FACIL'ITI.

8 novembre
- Audition des représentants d'association actives dans le domaine de l'inclusion numérique.

13 novembre
- Séance plénière : Audition de Mme Clara CHAPPAZ, Secrétaire d'État chargée de l'Intelligence artificielle et du Numérique.

14 novembre
- Participation au rendez-vous de la fibre du Cercle Credo.

21 novembre
- Réunion de travail avec l'ARCEP.

26 novembre
- Séance plénière : examen d'un projet d'avis sur l'inclusion numérique.

27 novembre
- Participation du Président Damien Michallet à la table ronde organisée par l'AVICCA sur la Cybersécurité.

28 novembre
- Publication de l'avis : « Pour une politique nationale d'inclusion numérique adaptée aux besoins de nos concitoyens »
- Audition de Nicolas Routier, Directeur général adjoint du groupe La Poste en charge du service public et de la régulation dans le cadre de l'évaluation du coût net de la mission d'aménagement du territoire de La Poste.

DÉCEMBRE

3 décembre
- Désignation des sept nouveaux députés, membres de la Commission supérieure du numérique et des postes.

10 décembre
- Participation à la présentation des résultats du Baromètre de la Fibre en Entreprise COVAGE INFRANUM 2024.

11 décembre
- Publication de l'avis sur le cout net de la mission d'aménagement du territoire confiée au Groupe La Poste en 2023.

12 décembre
- Présidence et participation aux 6èmes Assises de la Cohésion Numérique et Territoriale.

16 décembre
- Participation à l'instance de concertation réseaux mobiles - MINEFI.
- Participation à la réunion de l'ONPP.

Avis rendus en 2024

Avis rendus en 2024

- **Avis n°2024-01 du 17 janvier 2024** « Pour mieux encadrer l'usage de l'intelligence artificielle »
- **Avis n°2024-02 du 15 avril 2024** relatif au projet de décret sur la méthode d'évaluation de la mission du SUP
- **Avis n°2024-03 du 21 mai 2024** relatif au titre II du projet de loi relatif à la résilience des activités d'importance vitale, à la protection des infrastructures critiques, à la cybersécurité et à la résilience opérationnelle numérique du secteur financier
- **Avis n°2024-04 du 6 juin 2024** sur les conséquences des coupes budgétaires sur le Plan France Très Haut Débit au regard des enjeux de déploiement de résilience et de la fermeture du réseau cuivre
- **Avis n°2024-05 du 4 septembre 2024** sur les enjeux politiques et économiques du schéma European Union Cybersecurity Certification Scheme for Cloud Services (EUCS)
- **Avis n°2024-06 du 26 juillet 2024** sur le décret relatif à la méthode d'évaluation du Service Universel Postal
- **Avis n°2024-07 du 3 octobre 2024** sur les enjeux de la transposition de la directive NIS 2 en France
- **Avis n°2024-08 du 28 novembre 2024** « Pour une politique nationale d'inclusion numérique adaptée aux besoins de nos concitoyens »
- **Avis n°2024-09 du 11 décembre 2024** sur le cout net de la mission d'aménagement du territoire confiée au Groupe La Poste en 2023

AVIS N° 2024-01 DU 17 JANVIER 2024 POUR MIEUX ENCADRER L'USAGE DE L'INTELLIGENCE ARTIFICIELLE

Le développement de l'intelligence artificielle (IA) et notamment l'intelligence artificielle générative constituent un saut technologique et sans doute une révolution technologique et économique dont les effets sont encore difficiles à mesurer mais dont on devine qu'ils seront majeurs pour notre société et nos démocraties.

Dans son avis n°2020-08 du 12 juin 2020 publié dans le cadre de la consultation publique sur le livre blanc européen sur l'intelligence artificielle (IA) , la Commission supérieure du numérique et des postes (CSNP) avait eu l'occasion d'exprimer sa position sur les enjeux posés par le développement de l'IA en préconisant des investissements massifs pour rattraper le retard pris par l'Europe, l'adoption d'une régulation appropriée préservant les libertés fondamentales du citoyen et du consommateur européen, sans que cet encadrement freine ou pénalise les initiatives publiques et privées et la création d'un écosystème d'excellence permettant de soutenir le développement de l'IA dans les services publics et dans la sphère économique en renforçant la capacité des centres de recherche européens.

Trois années ont passé et force est de constater que ces recommandations sont plus que jamais d'actualité en matière d'investissements, que la première phase de la stratégie française en matière d'IA a donné de premiers résultats mais que les positions sur ce que doit être une réglementation européenne de l'IA se clivent entre les partisans d'une régulation ultra-protectrice des droits individuels et les partisans d'une réglementation minimum qui n'entraverait pas l'innovation et la recherche. Ce clivage a été renouvelé et accentué avec la mise sur le marché en novembre 2022 d'une IA générative à la portée du grand public et du plus grand nombre d'entreprises.

C'est dans ce contexte que les membres de la CSNP ont confié à Mme Mireille Clapot, Députée de la Drôme et Présidente de la CSNP, la responsabilité d'un groupe de travail sur l'intelligence artificielle en lui demandant 1./ d'analyser les enjeux de la régulation l'intelligence artificielle pour, le cas échéant, formuler des recommandations sur ce sujet, 2./ d'identifier les obstacles et les leviers pour favoriser le développement d'une IA française et européenne et 3./ de formuler des recommandations pour un meilleur usage de l'intelligence artificielle dans les services publics.

Au cours de ces travaux, le développement de l'IA a été envisagé selon les axes de l'intérêt général, de la souveraineté, de la sécurité et de la sobriété.

Il ressort des auditions et des travaux conduits par Mme Mireille Clapot plusieurs constats :

- Le développement de l'IA doit être étudié sous l'angle social et sociétal, de la conformité et de la règlementation, des impacts environnementaux et des compétences.

- Il est encore temps de développer une IA française et européenne. Les big techs américaines et chinoises ont pris de l'avance mais ce retard est rattrapable si nous nous en donnons les moyens dès à présent.

- La régulation européenne de l'IA ne doit pas pénaliser nos chercheurs et nos entreprises. Le RGPD devait protéger les données des citoyens européens mais au final, les GAFAM et les big techs détiennent et utilisent ces mêmes données pour développer un avantage comparatif sur les entreprises européennes et imposer leurs produits et leurs services.

- Il n'y aura pas d'IA française ou européenne sans un meilleur accès et un meilleur partage des données au niveau national et européen.

A l'issue de ces travaux, la Commission supérieure du numérique et des postes est en mesure de formuler des recommandations portant sur la régulation et la gouvernance de l'IA, sur la nécessité stratégique de développer des jeux de données français et européens, sur le renforcement de la recherche, sur les problèmes de financement rencontrés par les entreprises françaises, sur les enjeux de formation, sur les développement de l'IA dans les services publics, sur l'impact de l'IA sur l'environnement et sur l'usage de l'IA au service de nos concitoyens et des services publics.

- **Sur les impacts sociaux et sociétaux de l'intelligence artificielle**

Recommandation 1 : **Anticiper les impacts sociaux du développement de l'IA en demandant aux acteurs économiques et sociaux et aux pouvoirs publics de planifier des plans de formation continue et de reconversion**

Recommandation 2 : Intégrer les conséquences du développement des services d'IA dans les politiques éducatives en veillant à continuer à intégrer les fondamentaux tels que les mathématiques et l'orthographe

- **Sur la régulation et la gouvernance des services d'intelligence artificielle**

Recommandation 3 : Elaborer une définition juridiquement robuste de l'IA

Recommandation 4 : Poursuivre les négociations relatives à l'IA Act en veillant à mettre en place une régulation équilibrée qui offre transparence et protection mais qui n'entrave pas la recherche, l'innovation et le développement entrepreneurial, et adaptable aux évolutions rapides des technologies et des usages liés à l'intelligence artificielle

Recommandation 5 : Engager dès à présent, au niveau européen, des travaux notamment sur la régulation de la propriété intellectuelle pour combler les vides juridiques liés au développement de l'IA générative

Recommandation 6 : Peser au niveau international le plus approprié pour élaborer un traité international de l'IA (sur le modèle du droit de la mer ou de l'espace aérien)

Recommandation 7 : Instituer au niveau national une autorité indépendante en charge de l'intelligence artificielle

Recommandation 8 : Intégrer le Ministère de la Culture dans les administrations coordonnées par le Coordinateur national pour l'IA

- **Sur l'accès aux jeux de données**

Recommandation 9 : Impulser une politique publique ambitieuse sur le plan qualitatif et quantitatif de création de cohortes de données placée sous la responsabilité de l'INRIA

Recommandation 10 : Surmonter les freins administratifs et politiques pour accélérer les délais d'accès aux jeux de données disponibles au sein de la sphère publique et au bénéfice de la recherche

Recommandation 11 : Développer des solutions de stockage souveraines pour les données les plus sensibles notamment pour les entrepôts de données de santé utilisées dans le cadre de la recherche et de l'innovation

- **Sur la recherche en intelligence artificielle**

Recommandation 12 : Revaloriser les salaires des chercheurs français au même niveau que ceux de leurs pairs européens

Recommandation 13 : Renforcer les financements européens destinés à la recherche en IA, aux supercalculateurs européens, et intensifier la mise en réseau des centres de recherche européens sur l'IA, en encourageant les partenariats avec des pays-tiers sur des projets spécifiques. Une attention particulière pourrait être portée sur notre dépendance aux puces électroniques et à la mise en œuvre effective de l'European Chips Act

- **Sur les financements dédiés à l'intelligence artificielle**

Recommandation 14 : Orienter les investissements publics pour favoriser le développement d'une IA de confiance associant un cloud de confiance ainsi qu'une puissance de calcul française et européenne

Recommandation 15 : Optimiser le recours des entreprises françaises aux financements européens, tels que le programme « Horizons 2020 » et la participation aux Projets Importants d'Intérêt Européen Commun (IPCEI) en les accompagnant en matière d'ingénierie financière.

Recommandation 16 : Faciliter le financement des startups et les projets en phase *early stage* mais garantir un mécanisme de remboursement en cas de rachat par un acteur économique étranger

- **Sur l'impact de l'intelligence artificielle sur l'environnement**

Recommandation 17 : Créer un consortium dédié à l'IA frugale, visant à développer des technologies d'IA plus respectueuses de l'environnement et efficaces en termes de consommation de ressources en eau et en énergie

Recommandation 18 : Développer les instruments de mesure de l'impact carbone du secteur de l'IA et initier un référentiel international sur l'impact environnemental de l'IA, sous l'égide de l'OCDE ou de l'ONU

- **Sur l'usage de l'intelligence artificielle dans les services publics**

Recommandation 19 : Veiller à ce que l'utilisation des services d'IA dans les services publics soient toujours supervisés par des humains

Recommandation 20 : Informer les usagers sur l'utilisation de l'IA dans la prise de décision administrative

Recommandation 21 : Inciter chaque ministère à travailler sur un ou deux projets emblématiques d'IA pour améliorer les démarches administratives des usagers

Recommandation 22 : Vérifier l'adaptation des règles de la commande publique à l'achat de services d'IA souverain pour stimuler le développement d'acteurs européens

Recommandation 23 : Former les managers de l'Etat aux enjeux de l'IA, inclure dans les écoles de formation (INSP, ENM, …) des stages ou la conduite de projets associant des experts de l'IA

Recommandation 24 : Désigner un référent IA dans les administrations publiques et les établissements de formation

- **Sur les enjeux de compétence liés au développement de l'intelligence artificielle**

Recommandation 25 : Renforcer le niveau en mathématiques et en maîtrise du langage des élèves français

Recommandation 26 : Développer des programmes de formation en IA pour les bac+2 et bac+3.

Recommandation 27 : Mettre en place des indicateurs fiables pour mesurer le nombre d'étudiants en IA (tous niveaux confondus), afin de suivre et d'analyser l'évolution de la formation dans ce secteur et doubler le nombre d'étudiants en IA dans les cinq prochaines années pour répondre aux besoins croissants en compétences dans ce secteur

Recommandation 28 : S'assurer de la mise à niveau des compétences des formateurs tout au long de leur engagement professionnel

Recommandation 29 : Promouvoir la féminisation dans le secteur de l'IA, en mettant en place des initiatives spécifiques pour attirer et soutenir les femmes dans ce domaine

Recommandation 30 : Créer un réseau européen de formation de l'IA, favorisant les échanges d'étudiants pour renforcer les projets portés par l'Europe dans le domaine de l'IA

I. Sur les impacts sociaux et sociétaux de l'intelligence artificielle

Depuis plusieurs années déjà, le déploiement des systèmes d'intelligence artificielle est étudié notamment dans le domaine du travail et de l'emploi en prenant en compte plusieurs dimensions : la destruction ou la création d'emplois induite par l'IA, le sens du travail, l'autonomie et la responsabilisation des salariés et naturellement l'évolution des compétences et des savoir-faire.

Une étude de l'organisation de coopération et de développement économiques (OCDE) sur le marché de l'emploi estime que 27 % des emplois seraient menacés par l'IA[1] dans les secteurs manufacturiers et financiers.

D'autres études confirment cette transformation et cette destruction d'emplois dans différents secteurs économiques[2].

En avril 2002, Joseph Stiglitz, prix Nobel d'Economie, se montrait très pessimiste sur les conséquences économiques d'un développement non maitrisé de l'intelligence artificielle notamment sur les modèles économiques des pays développés mais également dans les pays en voie de développement.

Les membres de la CSNP considèrent comme essentiel que les pouvoirs publics anticipent au plus tôt ces impacts. Des réflexions sont déjà en cours au sein des instances qui réunissent des acteurs économiques. Il est désormais urgent de planifier rapidement des plans de formation et de reconversion. Le déploiement de l'IA renforce plus que jamais la nécessité d'une formation continue adaptée aux évolutions technologiques au cours des parcours professionnels.

Au- delà de ses impacts sur l'emploi et le travail, les services d'IA aura des conséquences majeures sur le développement cognitif des futures générations. Nous sommes tous déjà impactés à des degrés divers par l'usage du numérique dans notre rapport à l'espace, au temps et dans de très nombreux usages de la vie quotidienne.

Alors que le Ministre de l'éducation vient d'annoncer l'introduction d'une intelligence artificielle dans des classes de seconde dès février 2024 pour aider les élèves en français et en maths, les membres de la CSNP appellent les pouvoirs publics et notamment ceux en charge de la petite enfance et de la jeunesse à intégrer ces développements dans leur approche éducative et sanitaire en direction des jeunes et de leurs parents.

Le développement de l'IA est porteur d'opportunités mais peut également potentiellement creuser la fracture numérique qui existe déjà dans notre pays, en raison de l'illectronisme mais également celle-liée à l'insuffisance des infrastructures et des équipements notamment dans la ruralité. Cela constitue un point de vigilance pour les membres de la CSNP.

Recommandation 1 : **Anticiper les impacts sociaux du développement de l'IA en demandant aux acteurs économiques et sociaux et aux pouvoirs publics de planifier des plans de formation continue et de reconversion**

Recommandation 2 : Intégrer les conséquences du développement des services d'IA dans les politiques éducatives en veillant à continuer à intégrer les fondamentaux tels que les mathématiques et l'orthographe

[1] The impact of AI on the workplace: Main findings from the OECD AI surveys of employers and workers | Documents de travail de l'OCDE sur les questions sociales, l'emploi et les migrations | OECD iLibrary (oecd-ilibrary.org)
[2] Intelligence artificielle : une transformation sans précédent (gsam.com)

II. Sur la régulation et la gouvernance des services d'intelligence artificielle

L'IA et les services d'IA sont régulés depuis mai 2019 par les principes de l'OCDE qui encouragent une utilisation de l'IA qui soit innovante et digne de confiance et qui respecte les droits de l'homme et les valeurs démocratiques. Ces principes ont été conçus pour s'adapter aux innovations technologiques de l'IA. L'apparition de l'IA générative a néanmoins accéléré au cours des derniers mois les travaux en cours pour adopter des codes de conduite et des règlementations nationales ou multilatérales dans le cadre du G7, du G20, des Nations -Unies, du Conseil de l'Europe avec, au niveau européen, l'adoption imminente du règlement sur l'IA ou *IA Act*.

En effet, le 8 décembre dernier, le Commissaire Thierry Breton a annoncé un accord sur le règlement sur l'intelligence artificielle. Ce texte doit encore faire l'objet de réunions techniques avant d'être voté par le Parlement et le Conseil européens au 1er trimestre 2024. A l'issue de la réunion du Coreper du 15 décembre 2023, plusieurs pays dont la France, l'Allemagne, l'Italie mais également la Hongrie, la Pologne et la Finlande indiquaient attendre de disposer du texte définitif de l'accord pour se prononcer sur son adoption.

Le sujet de la régulation et de la gouvernance des services d'IA a été abordé dans la quasi-totalité des auditions conduites par le groupe de travail.

Sur cette base et en l'absence de texte définitif, les membres de la CSNP souhaitent aborder plusieurs enjeux cruciaux liés à la régulation et la gouvernance des services d'IA.

1. Sur la définition de l'intelligence artificielle

C'est, à ce stade, la nouvelle définition de l'intelligence artificielle reformulée en novembre 2023 par l'OCDE qui a été retenue par l'Union européenne :

« *Un système d'IA est un système basé sur une machine qui, pour des objectifs explicites ou implicites, déduit, à partir des informations qu'il reçoit, comment générer des résultats tels que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels. Les différents systèmes d'IA varient dans leurs niveaux d'autonomie et d'adaptabilité après le déploiement. » demander la traduction officielle à l'OCDE »*[3]

De l'aveu même des responsables de l'OCDE, obtenir un consensus sur la définition d'un système d'intelligence artificielle qui soit pertinente pour l'ensemble des secteurs et validée par les groupes d'experts, a été un exercice compliqué.

Pour les membres de la Commission supérieure, il est essentiel que cette définition soit juridiquement solide. Les membres de la CSNP anticipent en effet que cette définition pourrait emporter un très grand nombre de **conséquences dans l'interprétation des textes réglementaires et notamment en cas de litiges.** Compte tenu des enjeux liés à cette définition, il est important que nos concitoyens et les acteurs économiques ne soient pas soumis aux aléas d'une jurisprudence trop aléatoire et insuffisamment prévisible de la Cour de justice de l'Union européenne.

2. Sur la nécessité d'adopter un dispositif équilibré pour réguler l'intelligence artificielle

A ce stade, les instances multilatérales et les Etats-Unis ont choisi de réguler l'IA par des code de

[3] Traduction non officielle en français

conduite ou des grands principes.

L'Union européenne est la première organisation à vouloir adopter un règlement plus contraignant pour les services d'IA. Fondé sur une approche basée sur le risque, le texte initial de l'IA Act entendait apporter une réponse graduée en fonction des risques liés aux usages.

Avec l'apparition des premières applications d'IA générative destinées au grand public, le texte initial de la Commission ne paraissait pas suffisamment contraignant pour les parlementaires européens qui ont également appelé de leurs vœux un encadrement plus strict de la reconnaissance faciale.

La position des autorités françaises est de réguler les usages et non les modèles, de ne pas imposer une surrégulation qui aurait pu nuire à l'innovation. Dans un non papier publié fin novembre, la France, avec l'Allemagne et l'Italie, ont plaidé pour un code de conduite.

Le texte issu des trilogues tel qu'il a été présenté par le Commissaire Thierry Breton semble trouver un point d'équilibre entre la préservation de l'Etat de droit et des libertés fondamentales, d'une part, et le développement de l'innovation, d'autre part.

Le règlement sur l'IA classe les usages en quatre catégories en fonction des risques potentiels : minime, limité, élevé et interdit.

Les usages interdits concernent les applications contraires aux valeurs européennes comme le *social scoring*.

Les systèmes à "haut risque" seront contrôlés. Ce sera le cas des infrastructures critiques, l'éducation, les ressources humaines ou encore le maintien de l'ordre. Pour les systèmes à haut risque, un système de marquage CE, de conformité européenne, sera imposé. Ces systèmes devront se soumettre à une évaluation de conformité et obtenir un label.

Les "larges modèles" (les modèles d'IA avec une faible puissance de calcul) devront remplir des obligations de transparence ou d'information sur leurs données d'entraînement.

A ce stade, aucune contrainte ne pèserait sur la recherche et le développement des larges modèles. Lorsqu'ils seront mis sur le marché, les services d'IA issus de la recherche devront remplir des obligations de transparence et d'information sur leurs données d'entrainement.

Ce n'est que lorsqu'ils deviendront systémiques, c'est-à-dire au-dessus de 10^{25} flops qu'ils seront soumis à des règles précises de prévention des risques.

En pratique, seuls GPT-4 d'Open AI et, peut être, Gemini de Google atteignent à ce jour cette puissance.

Si ce texte de compromis paraît équilibré, **il paraît important pour les membres de la CSNP de revoir sur des bases régulières l'application de l'IA ACt à l'épreuve des faits et surtout pour tenir compte des évolutions technologiques extrêmement rapides dans ce domaine.** Il conviendrait d'ores-et-déjà de prévoir une clause de revoyure pour adapter si nécessaire le cadre règlementaire aux évolutions technologique et aux usages.

3. Sur le traitement des droits d'auteur et du droit de propriété intellectuelle

L'IA générative va induire un bouleversement dans le traitement des droits d'auteur et du droit de la propriété intellectuelle.

Sur les jeux de données, au printemps 2023, le Japon a indiqué que le droit d'auteur ne s'appliquerait pas aux données utilisées pour la formation des modèles d'intelligence artificielle (IA). Cette politique permet à l'IA d'utiliser n'importe quelle donnée *« qu'il s'agisse d'un usage à but non lucratif ou*

commercial, qu'il s'agisse d'un acte autre que la reproduction ou qu'il s'agisse de contenu obtenu à partir de sites illégaux ou autrement ».

A ce stade, l'IA Act comprendrait des mesures protectrices du copyright en imposant certaines obligations aux créateurs de modèles d'IA génératives (publication des contenus utilisés pour l'entrainement de leurs algorithmes, respect du droit d'auteur européen, respect des clauses d'opt-out permettant une opposition à l'utilisation des données par les systèmes d'IA).

Encore une fois, il est nécessaire de disposer des dispositions précises du texte de l'IA Act pour mesurer l'efficacité de ces mesures et des contraintes raisonnables qu'elles font peser sur les développeurs d'IA.

Les membres de la Commission supérieure considèrent toutefois que des travaux sur la Directive « droits d'auteur » devront être lancés après les élections européennes de juin 2024 pour tenir compte des incidences de l'IA générative sur les droits d'auteurs et plus largement sur la propriété intellectuelle et industrielle.

A cet égard, il nous semble que le Ministère de la Culture pourrait utilement intégrer le champ des ministères coordonnés par le coordonnateur national pour l'IA.

4. Sur la mise en œuvre du règlement sur l'intelligence artificielle

La mise en œuvre de l'IA Act supposera une période de transposition d'ici 2025 au cours de laquelle il conviendra d'examiner comment organiser l'articulation entre les organes de contrôle mis en place au niveau européen et les organes responsables de son application en France.

Au cours de ses travaux, les membres de la CSNP ont pu identifier deux scénarii : un organe de contrôle dont la coordination serait assurée par une autorité indépendante (sur le modèle de la coordination assurée par l'ARCOM dans la loi SREN) ou la création d'une autorité créée *ad hoc*. Les principaux partisans de cette deuxième option manifestant des craintes quant au trop grand rôle que pourrait jouer la CNIL dans la régulation de l'IA en France.

5. Sur l'articulation des textes européens et internationaux

L'intelligence artificielle fait l'objet de régulations unilatérales (*Executive order on safe, secure and trustworthy artificial intelligence* aux Etats-Unis, législations nationales en Inde, en Chine et au Royaume- Uni), de recommandations de l'OCDE et d'un code de conduite adopté par les pays du G7 avec le processus d'Hiroshima. D'autres initiatives sont portées par le Conseil de l'Europe et les Nations-Unies notamment.

Les membres de la CSNP considèrent que la régulation de l'IA, à l'instar de ce qui a été fait pour la régulation de l'espace aérien et l'espace maritime, pourrait légitimer l'émergence d'un traité international de l'IA.

L'émergence de ce droit international nécessitera du temps et de l'ambition et suscitera sans doute de nombreuses résistances. Mais à l'évidence, nous sommes rentrées dans une ère nouvelle où le modèle de nos sociétés, nos droits de citoyens sont ou vont être bouleversés par cette nouvelle technologie.

Les travaux de l'OCDE qui dispose, avec son observatoire des politiques relatives à l'IA, de la matrice et de l'expérience pour conduire ces négociations pourraient constituer une base solide pour ces

négociations. La déclaration de New Delhi adoptée à l'issue du sommet du Partenariat global sur l'intelligence artificielle le 13 novembre 2023 démontre que les positions évoluent et que des consensus peuvent émerger.

Recommandation 3 : Elaborer une définition juridiquement robuste de l'IA

Recommandation 4 : Poursuivre les négociations relatives à l'IA Act en veillant à mettre en place une régulation équilibrée qui offre transparence et protection mais qui n'entrave pas la recherche, l'innovation et le développement entrepreneurial, et adaptable aux évolutions rapides des technologies et des usages liés à l'intelligence artificielle

Recommandation 5 : Engager dès à présent, au niveau européen, des travaux notamment sur la régulation de la propriété intellectuelle pour combler les vides juridiques liés au développement de l'IA générative

Recommandation 6 : Peser au niveau international le plus approprié pour élaborer un traité international de l'IA (sur le modèle du droit de la mer ou de l'espace aérien)

Recommandation 7 : Instituer au niveau national une autorité indépendante en charge de l'intelligence artificielle

Recommandation 8 : Intégrer le Ministère de la Culture dans les administrations coordonnées par le Coordinateur national pour l'IA

III. Sur l'accès aux jeux de données

L'apprentissage d'un système d'IA nécessite l'entrainement des algorithmes de Machine Learning et de Deep Learning à partir d'un volume très important de données provenant de multiples sources différentes. L'objectif de cet entrainement est d'améliorer la performance des services d'IA en faisant appel à des données riches et variées qui, après des centaines de cycles d'apprentissages, sont en mesures de rendre des résultats équivalents ou supérieurs à l'intelligence humaine, en quelques secondes.

Cet entrainement nécessite, dès lors, d'avoir accès à des jeux de données fiables afin d'éviter un apprentissage biaisé qui rendrait les résultats obtenus via de l'intelligence artificielle inopérants, car faussés par des biais.

La difficulté d'accès à ces données d'apprentissage réside généralement dans l'usage et la finalité des services d'IA : les données stockées sont majoritairement créées pour un usage général ou au contraire très précis et ne répondent pas nécessairement au besoin recherché par un utilisateur.

Par ailleurs, ces jeux de données ne sont pas toujours transparents sur la manière dont ils ont été constitués.

L'apprentissage d'un système d'IA et l'accès aux jeux de données sont soumis au principe de la protection des données et de propriété intellectuelle et notamment au respect des règles édictées par la Loi Informatique et Libertés et le Règlement général sur la protection des données (RGPD). A cet égard, la CNIL précise que « *pour respecter le RGPD, un système d'intelligence artificielle reposant sur l'exploitation de données personnelles doit toujours être développé, entrainé, et déployé avec une finalité (objectif) bien définie* [4] ».

[4] https://www.cnil.fr/fr/intelligence-artificielle/ia-comment-etre-en-conformite-avec-le-rgpd

Si l'accès à un jeu de données volumineux est, en apparence, indispensable à l'entrainement de l'intelligence artificielle ; la masse d'informations récoltées n'est pas synonyme de qualité et de pertinence des données au regard d'une finalité spécifique.

Au cours des auditions conduites par la CSNP, nos interlocuteurs nous ont confirmé les difficultés rencontrées pour accéder à des données de qualité pour développer des systèmes d'IA. Il ne s'agirait pas de difficultés portant sur la quantité de données mais également sur la qualité de celles-ci.

L'accès aux jeux de données est rendu difficile en raison du silotage des données entre les différentes administrations ou organisations. Ce problème avait déjà été identifié dans le rapport « Donner un sens à l'intelligence artificielle », de Cédric Villani publié en 2018[5]. Peu de progrès ont été réalisés depuis ce constat.

Il semblerait que ces difficultés dans l'accès aux données soient moins le résultat d'une contrainte législative ou règlementaire que le résultat de pratiques très conservatrices des propriétaires de données ou de leurs services juridiques. Il nous a été indiqué lors des auditions qu'un chercheur devait attendre en moyenne près de 10 mois pour accéder à des données de santé par exemple.

L'approche développée par l'INRIA d'un apprentissage fédéré (plusieurs machines entrainent collaborativement un modèle d'intelligence artificielle tout en gardant leurs données localement) est sans doute une approche à développer plus massivement.

Les membres de la CSNP appellent à les pouvoirs publics à développer au niveau européen et au niveau national une véritable politique de la donnée pour que les données utilisées pour des services d'IA français et européens ne soient pas uniquement entrainés par des données américaines ou chinoises.

En France, cette politique publique pourrait être placée sous l'autorité de l'INRIA.

Cette politique publique devra naturellement intégrer pour les données les plus sensibles des solutions souveraines de stockage.

Recommandation 9 : Impulser une politique publique ambitieuse sur le plan qualitatif et quantitatif de création de cohortes de données placée sous la responsabilité de l'INRIA

Recommandation 10 : Surmonter les freins administratifs et politiques pour accélérer les délais d'accès aux jeux de données disponibles au sein de la sphère publique et au bénéfice de la recherche

Recommandation 11 : Développer des solutions de stockage souveraines pour les données les plus sensibles notamment pour les entrepôts de données de santé utilisées dans le cadre de la recherche et de l'innovation

-

[5] https://www.enseignementsup-recherche.gouv.fr/fr/rapport-de-cedric-villani-donner-un-sens-l-intelligence-artificielle-ia-49194

IV. Sur la recherche en intelligence artificielle

La première phase de la stratégie nationale pour l'intelligence artificielle a permis de mettre en œuvre plusieurs recommandations du rapport de Cédric Villani notamment avec le financement du supercalculateur Jean Zay, la mise en place de quatre instituts interdisciplinaires d'intelligence artificielle (le MIAI de Grenoble, le 3IA Côte d'Azur à Nice, PRAIRIE à Paris, ANITI à Toulouse) et la mise en œuvre d'actions prioritaires dans les secteurs de la santé, de l'écologie, des transports et de la mobilité et de la défense et de la sécurité.

Les membres de la CSNP saluent la mise en œuvre de cette première phase et le lancement de la deuxième phase de la stratégie nationale de l'IA dotée de financements comparables.

Cependant, plusieurs obstacles demeurent notamment les difficultés ou les délais dans l'accès aux jeux de données pour les chercheurs (cf. chapitre dédié à ce sujet).

Les membres de la CSNP ont pris note des annonces faites le 7 décembre 2023 par le Chef de l'Etat relatives au renforcement stratégique de l'écosystème de la recherche française et la transformation de l'Institut national de recherche en sciences et technologies du numérique (Inria) en agence de programme spécialisée pour le numérique et le logiciel.

Le PDG de l'INRIA, que nous avons auditionné, nous a indiqué que ce nouveau statut permettra de renforcer le pilotage stratégique de la politique conduite par l'Institut en matière d'IA.

L'annonce le 16 novembre 2023 du centre de recherche Kyutai par MM. Xavier Niel, Président de Free-Iliad, Rodolphe Saade, Président de CMA-CGM, et Eric Schmidt, ancien PDG de Google, valide à la fois la très grande attractivité de la France pour l'écosystème de la recherche en IA mais également la nécessité de renforcer les moyens de la recherche française en matière d'IA en revalorisant les salaires des chercheurs français par rapport à leurs homologues européens et internationaux.

Cet investissement massif (300 M €) d'une fondation privée à but non lucratif nous paraît devoir être salué et confirme que la France dispose d'atouts en matière de recherche notamment grâce à l'excellence de ses formations en mathématiques.

De fait, parmi les sujets d'interrogation qui ont émergé des travaux de la CSNP, figure le bon niveau de coopération européenne en matière d'IA. Des exemples de coopération avec l'Allemagne existent . Ils pourraient sans doute être plus étroits. Le fait que la recherche dans l'IA soit portée en Allemagne par de grands groupes industriels conduirait à la définition d'une stratégie très nationale peu tournée vers la coopération.

Par ailleurs, le sujet d'une coopération plus étroite avec le Royaume-Uni se pose alors que ce pays ne fait plus partie de l'Union européenne et qu'il entretient une très grande proximité avec les Etats-Unis. Le Royaume-Uni fait partie des pays qui accueille le plus d'investissements privés en matière d'IA après les Etats-Unis et la Chine. Un renforcement d'une coopération de l'Union européenne et de la France avec le Royaume-Uni nous parait devoir être explorée en tenant compte de ces réalités.

Recommandation 12 : Revaloriser les salaires des chercheurs français au même niveau que ceux de leurs pairs européens

Recommandation 13 : Renforcer les financements européens destinés à la recherche en IA, aux supercalculateurs européens, et intensifier la mise en réseau des centres de recherche européens sur l'IA, en encourageant les partenariats avec des pays-tiers sur des projets spécifiques. Une attention particulière pourrait être portée sur notre dépendance aux puces électroniques et à la mise en œuvre effective de l'European Chips Act

V. Sur les financements destinés au développement de l'IA en France en Europe

- Les financements publics français

La première phase de la stratégie nationale pour l'intelligence artificielle lancée en 2018 était dotée de 1,5 milliard d'euros sur la période 2018-2022 orientée principalement vers la recherche (création et développement des instituts interdisciplinaires d'intelligence artificielle 3IA, financement de chaires d'excellence en IA et de programmes doctoraux, financement du supercalculateur Jean Zay).

La seconde phase de la stratégie nationale pour l'IA lancé le 8 novembre 2022 prévoit un financement de 2,22 milliards d'euros sur cinq ans dont 1,5 milliard d'euros de financements publics et 506 millions d'euros de cofinancements privés. Cette seconde phase a pour objectif de diffuser l'IA au sein de l'appareil productif et de privilégier l'innovation dans certains secteurs.

Un comité piloté par le coordinateur national pour l'intelligence artificielle s'assure de la bonne allocation de ces fonds.

Les membres de la CSNP souhaiteraient disposer de plus d'informations sur le fléchage des financements publics à destination des entreprises et start-ups bénéficiaires notamment pour s'assurer de l'orientation des investissements pour le développement d'une IA de confiance.

L'option d'une défiscalisation du recours aux services d'IA par le secteur privé a été abordée au sein des membres de la CSNP et pourrait être étudiée par les pouvoirs publics.

- Les financements européens

Le programme pour une Europe numérique (Digital Europe Programme - DIGITAL) a mis en place des financements de 7,5 Mds EUR pour le développement de supercalculateurs, de service d'intelligence artificielle, de cybersécurité et compétences numériques avancées. Dans ce cadre, une dotation de 2,1 Mds EUR est dédiée au développement de l'IA par les entreprises et les administrations, notamment pour le développement et le stockage de jeux de données.

En matière de recherche, Horizon Europe, le programme-cadre de l'Union européenne pour la recherche et l'innovation pour la période 2021/2027, dispose d'un budget d'environ 95,5 Mds EUR.

D'une manière générale, les membres de la Commission supérieure notent que le niveau de sollicitation des entreprises et des unités de recherche françaises aux instruments financiers européens est relativement faible par rapport aux autres pays membres. **Il paraît important de mobiliser d'avantage les entreprises et les chercheurs français sur ces financements en leur proposant un accompagnement en ingénierie financière, qui pourrait être confié à BPIFrance.**

- Accès aux financements privés

Entre 2013 et 2022[6], les investissements privés en IA aux Etats-Unis ont cumulé 248, 9 Mds USD, contre 95,1 Mds USD pour la Chine, 18,2 Mds USD pour le Royaume-Uni, 10,8 Mds USD pour Israël, 8,8 Mds

[6] AI Index Report 2023 – Artificial Intelligence Index (stanford.edu)
Le classement des pays dans lesquels les investissements privés en IA sont les plus importants en 2022 établi par l'Université de Stanford positionne la France en 9ème position avec 1,77 Md USD derrière les Etats-Unis (47,36 Mds USD), la Chine (13,41 Mds USD), le Royaume-Uni (4,37 Mds USD), Israël (3,24 Mds USD), l'Inde (3,24 Mds USD), la Corée du Sud (3,10 Mds USD), l'Allemagne (2,35 Mds USD), le Canada (1,83 Mds USD).

USD pour le Canada, 7,7 Mds USD pour l'Inde, 7 Mds USD pour l'Allemagne et 6,6 Mds USD pour la France.

Les levées de fonds de Mistral AI de 113 M USD au printemps 2023 et de 415 MUSD en décembre 2023 sont donc aussi spectaculaires que peu représentatives du financement par capital risque des start-ups françaises.

Ce problème d'accès au capital risque pour financer la phase initiale de développement des start-ups françaises n'est pas propre aux entreprises spécialisées dans l'IA. Les associations représentatives des entreprises du numérique souhaiteraient que l'Etat ou les pouvoirs publics se substituent dans cette phase dite *early stage* aux investisseurs institutionnels qui préfèrent se positionner lorsque le cycle de développement de l'entreprise ou de la start-up leur apparaît moins risqué.

Les membres de la CSNP constatent cette carence du marché et invitent les pouvoirs publics à y remédier via BPIFrance notamment. Dans cette perspective, ils recommandent de s'inspirer du mécanisme public israélien de soutien à l'innovation mis en place par l'Israel Innovation Authority qui oblige l'acquéreur étranger d'une start-up israélienne à rembourser près de trois fois le montant de l'aide publique qui a été mobilisée pour accompagner un projet.

Recommandation 14 : Orienter les investissements publics pour favoriser le développement d'une IA de confiance associant un cloud de confiance ainsi qu'une puissance de calcul française et européenne

Recommandation 15 : Optimiser le recours des entreprises françaises aux financements européens, tels que le programme « Horizons 2020 » et la participation aux Projets Importants d'Intérêt Européen Commun (IPCEI) en les accompagnant en matière d'ingénierie financière.

Recommandation 16 : Faciliter le financement des startups et les projets en phase *early stage* mais garantir un mécanisme de remboursement en cas de rachat par un acteur économique étranger

VI. Sur l'impact de l'intelligence artificielle sur l'environnement

L'intersection entre l'intelligence artificielle (IA) et l'environnement a émergé comme un sujet de préoccupation majeur, tout en offrant un potentiel considérable pour orienter notre avenir. L'IA, en tant que vecteur de transformation numérique, présente un ensemble complexe d'effets.

D'une part, l'IA pourrait révolutionner notre approche des défis climatiques, en renforçant notre compréhension des phénomènes environnementaux, en optimisant l'utilisation des ressources, et en proposant des solutions novatrices pour atténuer le réchauffement climatique. Les services d'IA permettent une gestion plus efficace de l'énergie, favorise la détection précoce des catastrophes naturelles, et stimule des avancées significatives dans des domaines tels que l'agriculture durable et la transition vers les énergies renouvelables. Les services d'IA peuvent jouer un rôle crucial pour orienter nos écosystèmes vers des modèles de développement plus respectueux de l'environnement.

Inversement, le déploiement massif de centres de données et d'infrastructures de calcul haute performance, nécessaires pour alimenter les algorithmes d'IA, s'accompagne d'une augmentation significative de la consommation d'énergie, posant un défi majeur en matière de durabilité.

La course à l'innovation dans le domaine de l'IA peut également susciter des pratiques dites de "techno-blanchiment", où les progrès technologiques sont utilisés comme prétexte pour dissimuler les

véritables répercussions écologiques de certaines activités. L'IA ne peut être considérée comme une panacée pour résoudre les problèmes environnementaux, mais plutôt comme un outil puissant qui, lorsqu'il est utilisé avec discernement, peut sensibiliser aux enjeux du réchauffement climatique, faciliter la prise de décision éclairée, et contribuer à l'atténuation des menaces pesant sur notre planète.

Les membres de la CSNP constatent que le volet environnemental de l'IA fait partie de la stratégie nationale de l'IA. Ils recommandent que les calculs de l'impact environnemental des services d'IA soient mieux documentés et qu'un consortium dédié à l'IA frugal soit mis en place. Pour ne pas faire peser les contraintes environnementales sur les seuls services d'IA français et européens, les membres de la CSNP proposent qu'un référentiel commun soit mis en place au niveau international

Recommandation 17 : Créer un consortium dédié à l'IA frugale, visant à développer des technologies d'IA plus respectueuses de l'environnement et efficaces en termes de consommation de ressources en eau et en énergie

Recommandation 18 : Développer les instruments de mesure de l'impact carbone du secteur de l'IA et initier un référentiel international sur l'impact environnemental de l'IA, sous l'égide de l'OCDE ou de l'ONU

VII. Sur l'usage de l'intelligence artificielle dans les services publics

Certains services d'IA sont déjà déployés au sein des services publics, à une échelle encore limitée, pour la lutte contre la fraude (usage des services d'IA au sein de la Direction générale des finances publiques pour détecter des piscines non déclarées), en matière de sécurité intérieure (test sur les caméras de surveillance) ou en matière de cartographie et de prédiction des crues par exemple.

M. Stanislas Guerini, Ministre de la Transformation et de la Fonction publiques, a présenté, le 5 octobre 2023, sa stratégie pour développer et accompagner le déploiement de l'intelligence artificielle dans la fonction publique.

Le double objectif du déploiement des services d'IA dans les services publics est de faciliter les démarches administratives pour les usagers et de faciliter et rendre plus efficace le travail des agents. 1000 agents de l'Etat se sont portés volontaires pour tester un outil (chatbot), de réponses aux usagers, basé sur de l'IA générative.

A ce stade, les résultats présentés quelques semaines après leur mise en place sont prometteurs :

- plus de 70% des réponses proposées par l'IA sont pertinentes, soit 10 points de plus, en termes de satisfaction de l'usager
- les délais moyens de réponse aux usagers sont passés de sept jours à trois jours[7].

Cet outil intitulé « Claude » n'exclut pas, par ailleurs, le contrôle humain avant tout envoi de réponse à l'usager.

Au-delà de cette expérimentation, les enjeux de partage de données au sein de la fonction publique sont essentiels. La France est plutôt « bonne élève » en matière de données ouvertes mais des efforts

[7] https://www.banquedesterritoires.fr/retours-positifs-des-tests-dia-dans-les-services-publics-selon-le-gouvernement?pk_campaign=newsletter_quotidienne&pk_kwd=2023-12-14&pk_source=Actualit%C3%A9s_Localtis&pk_medium=newsletter_quotidienne

doivent cependant être engagés, notamment en matière de partage de la donnée entre l'Etat et les collectivités territoriales.

Le déploiement des services d'IA dans la fonction publique sont liés à la transformation numérique de l'Etat que la CSNP a abordé dans un avis récent : le développement des compétences numériques au sein des ministères, le recrutement accéléré de spécialistes du numérique, la ré-internalisation de certains emplois ou missions.

Le Ministre de la Transformation et de la Fonction publiques a indiqué aux membres de la CSNP que le gouvernement allait créer 500 postes supplémentaires dans le numérique en 2024.

Ainsi, dans le cadre de l'accélération du développement de l'usage de l'IA dans l'administration, la CSNP préconise d'inclure dans les écoles de formation (INSP, ENM, …) des stages ou des conduites de projets associant des experts de l'IA. Cette formation initiale pourrait être complétée par des formations continues à destination des agents et managers de la fonction publique.

Les membres de la Commission estiment qu'un référent IA devrait être désigné dans les administrations publiques et les écoles de formation, au même titre qu'un référent cybersécurité.

Les membres de la Commission se montrent favorables à l'utilisation de l'intelligence artificielle au sein des services publics à condition que la décision administrative soit toujours placée sous le contrôle ou la supervision d'un agent et que les utilisateurs soient informés, en toute transparence, qu'une IA a été utilisée dans le cadre de la prise de décision administrative dont ils ont fait l'objet.
Cette information leur permettra, sur demande, de disposer des informations nécessaires pour, le cas échéant, contester les décisions qu'ils jugeraient injustement défavorables.

Les membres de la CSNP appellent naturellement à une vigilance particulière sur l'absence et/ou la correction de biais dans les services D'IA employés par les services publics.

Les membres de la CSNP sont favorables aux recommandations formulées par le Conseil d'Etat qui préconise pour développer les cas d'usage de proposer à chaque administration de développer un ou deux projets d'intelligence artificielle emblématiques destinés à faciliter les démarches administratives des usagers et/ou de leurs agents[8].

Comme dans l'ensemble des secteurs, l'IA est une révolution dont il est nécessaire d'anticiper les conséquences sur les services publics et les emplois publics.

Recommandation 19 : Veiller à ce que l'utilisation des services d'IA dans les services publics soient toujours supervisés par des humains

Recommandation 20 : Informer les usagers sur l'utilisation de l'IA dans la prise de décision administrative

Recommandation 21 : Inciter chaque ministère à travailler sur un ou deux projets emblématiques d'IA pour améliorer les démarches administratives des usagers

Recommandation 22 : Vérifier l'adaptation des règles de la commande publique à l'achat de services d'IA souverain pour stimuler le développement d'acteurs européens

[8] Rapport « Intelligence artificielle et action publique : construire la confiance, servir la performance » du Conseil d'Etat – Mars 2022 etudePM IA_1 (1).pdf

Recommandation 23 : Former les managers de l'Etat aux enjeux de l'IA, inclure dans les écoles de formation (INSP, ENM, …) des stages ou la conduite de projets associant des experts de l'IA

Recommandation 24 : Désigner un référent IA dans les administrations publiques et les établissements de formation

VIII. Sur les enjeux de compétence liés au développement de l'intelligence artificielle

Le développement de l' IA engendre une demande croissante de professionnels hautement qualifiés, plaçant les experts en IA au cœur des défis technologiques et sociaux de notre époque.

La France dispose d'un atout considérable dans le développement des compétences liés à l'intelligence artificielle grâce à l'excellence de ses formations de haut niveau en mathématiques dont les étudiants sont chassés et recrutés par les Big Techs américaines notamment.

Pourtant, ainsi que l'a confirmé le dernier classement PISA, le niveau général en mathématiques des élèves français s'est effondré. L'enseignement des mathématiques et de la technologie dans les établissements scolaires secondaires devient une priorité. Les fondements mathématiques sont indispensables pour comprendre en profondeur les concepts sous-jacents à l'IA, tandis que l'accès précoce à un enseignement de pointe en technologie peut susciter des vocations précoces dans ce domaine en constante évolution.

Le développement des compétences suppose une meilleure attractivité des métiers liés au développement de l'IA. Il est manifeste que le métier d'ingénieur en IA doit connaître une revalorisation significative. Les compétences en IA sont devenues essentielles dans de nombreuses industries, offrant de nouvelles perspectives professionnelles aux ingénieurs et technologues.

La faible féminisation des métiers du numérique se pose également avec acuité pour les métiers liés à l'IA. Les femmes restent sous-représentées. Promouvoir la féminisation dans le secteur de l'IA est non seulement une question d'équité, mais également une nécessité pour bénéficier de la diversité de talents et de perspectives.

Pour combler les besoins en compétence, les pouvoirs publics doivent se fixer des objectifs ambitieux et introduire des formations qualifiantes en IA pour des bac+ 2 et bac +3. La stratégie nationale pour l'IA propose le développement des formations supérieures mais à ce stade, les indicateurs mis en place pour évaluer le nombre d'étudiants spécialisés en IA, ne sont pas performants.
Il convient donc de mettre en place des outils de pilotage efficaces et de fixer des objectifs ambitieux pour augmenter de manière significative le nombre de jeunes diplômés.

Recommandation 25 : Renforcer le niveau en mathématiques et en maîtrise du langage des élèves français

Recommandation 26 : Développer des programmes de formation en IA pour les bac+2 et bac+3.

Recommandation 27 : Mettre en place des indicateurs fiables pour mesurer le nombre d'étudiants en IA (tous niveaux confondus), afin de suivre et d'analyser l'évolution de la formation dans ce secteur et doubler le nombre d'étudiants en IA dans les cinq prochaines années pour répondre aux besoins croissants en compétences dans ce secteur

Recommandation 28 : S'assurer de la mise à niveau des compétences des formateurs tout au long de leur engagement professionnel

Recommandation 29 : Promouvoir la féminisation dans le secteur de l'IA, en mettant en place des initiatives spécifiques pour attirer et soutenir les femmes dans ce domaine

Recommandation 30 : Créer un réseau européen de formation de l'IA, favorisant les échanges d'étudiants pour renforcer les projets portés par l'Europe dans le domaine de l'IA

AUDITIONS

ALLIANCE FRANÇAISE DES INDUSTRIES DU NUMERIQUE (AFNUM)

Mme Stella MORABITO, Déléguée Générale
M. Léo LAFARGE, Chargé de mission « Nouvelles technologies et Affaires Européennes »
Mme Eva MARXER, Chargée de mission « Affaires publiques et Communication »

COMMISSION EUROPEENNE

Mme Evangelia MARKIDOU, Cheffe du Secteur « Technologie de l'Intelligence Artificielle »
M. Martin ULBRICH, Responsable du « Développement et Coordination de la Politique d'Intelligence Artificielle » - DG CONNECT
Mme Andrea HALMOS, Responsable de l'Unité « Mobilité Intelligente et Vie » - DG CONNECT
M. Antoine-Alexandre ANDRE, Chargé Politique et Juridique au sein de la DG CONNECT

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES (CNIL)

M. Bertrand PAILHES, Directeur des technologies et de l'innovation (DTI)
M. Thomas DAUTIEU, Directeur de l'accompagnement juridique
Mme Chirine BERRICHI, Conseillère pour les questions parlementaires et institutionnelles

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE (INRIA)

M. Bruno SPORTISSE, Président-Directeur Général
M. Stéphane GRUMBACH, Directeur de recherche et spécialiste des données

Maître Olivier ITEANU, Avocat spécialisé *data* et données personnelles, cybersécurité, propriété intellectuelle et e-commerce

META FRANCE - M. Martin SIGNOUX, Responsable des Affaires publiques

MINISTERE DE L'ECONOMIE, DES FINANCES ET DE LA SOUVERAINETE INDUSTRIELLE ET NUMERIQUE

M. Guillaume AVRIN, Coordonnateur de la stratégie nationale pour l'intelligence artificielle - DGE
M. Loïc DUFLOT, Chef du Service à l'économie numérique – DGE
M. Frédéric SAUVAGE, Chargé de négociations multilatérales numériques - DGE
Mme Manon LAFITTE, Cheffe de projet « Intelligence artificielle » - DGE

MINISTERE DE LA TRANSFORMATION ET DE LA FONCTION PUBLIQUES

M. Stanislas GUERINI, Ministre de la Transformation et de la Fonction Publiques
M. Damien SEUX, Conseiller « Transformation numérique de l'Etat » au sein du cabinet du Ministre

M. Boris MAZEAU, Conseiller parlementaire au sein du cabinet du Ministre

NUMEUM

M. Michel COMBOT, Délégué Général
Mme Marine GOSSA, Déléguée aux Affaires publiques

REPRESENTATION PERMANENTE DE LA FRANCE AUPRES DE L'ORGANISATION DE COOPERATION ET DE DEVELOPPEMENT ECONOMIQUES (OCDE)

Mme Amélie DE MONTCHALIN, Représentante permanente de la France
M. Didier LE MOINE, Conseiller « Innovation, numérique, industrie et PME »

OVHCLOUD

M. Kevin AMIL, Directeur Technique IA
Mme Blandine EGGRICKX, Responsable des Affaires publiques

SCALEWAY / ILIAD

M. Lucas BUTHION, Responsable des Affaires publiques Iliad
Mme Constance MORALES, Responsable Marketing IA

M. Cédric VILLANI, Mathématicien, Ancien Député et co-auteur du rapport « Donner un sens à l'intelligence artificielle » (2018)

BIBLIOGRAPHIE

VILLANI Cédric, « Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne. » Rapport remis au Premier Ministre Edouard PHILIPPE, 2018, disponible sur : Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne (vie-publique.fr).

VILLANI Cédric « Les enjeux de l'IA pour la Défense de demain », *Revue Défense Nationale*, vol. 820, no. 5, 2019

CNIL « Intelligence artificielle : le plan d'action de la CNIL » Mai 2023 Intelligence artificielle : le plan d'action de la CNIL | CNIL

Conseil d'Etat, « Intelligence artificielle et action publique : construire la confiance, servir la performance » Mars 2022, disponible sur : etudePM IA_1 (2).pdf.

Cour des Comptes, « La stratégie nationale de recherche en intelligence artificielle - Une stratégie à structurer et à pérenniser » Avril 2023

HALMOS Andrea, KOTOGLOU Stefanos, DG DIGIT B2, Interoperability Unit, Commission Européenne, « EDIH Working Group on Public Administration, with main focus on Artificial Intelligence », 2023, disponible sur : AI4PA_EDIH WG_workshop_20230428_FINAL.pdf (europa.eu).

European Law Institue « Model Rules on Impact Assessment of Algorithmic Decision-Making Systems Used by Public Administration. », 2022, disponible sur : ELI_Model_Rules_on_Impact_Assessment_of_ADMSs_Used_by_Public_Administration.pdf (europeanlawinstitute.eu).

OCDE « The impact of AI on the workplace: Main findings from the OECD AI surveys of employers and workers » OECD iLibrary (oecd-ilibrary.org)

The White House. « Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence », 30 octobre 2023, disponible sur : Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence | The White House.

DESBIOLLES Jean-Philippe, et COLOMBET Grégoire « Humain ou IA ? Qui décidera le futur ? Défis et opportunités d'un monde où l'IA nous dépasse » Dunod, 2023.

ATIF Jamal, BURGESS J. Peter, RYL Isabelle « Géopolitique de l'IA - Les relations internationales à l'ère de la mise en données du monde » Le Cavalier bleu, 2022.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

COMMISSION SUPERIEURE DU NUMERIQUE ET DES POSTES

AVIS N°2024-02 DU 15 AVRIL 2024

SUR LE PROJET DE DECRET RELATIF A LA METHODE D'EVALUATION UTILISEE POUR LE CALCUL DU COUT NET DE LA MISSION DE SERVICE UNIVERSEL POSTAL.

Vu la directive 97/67/CE du Parlement Européen et du Conseil du 15 décembre 1997 modifiée concernant les règles communes pour le développement du marché intérieur des services postaux de la Communauté et l'amélioration de la qualité du service

Vu la décision de la Commission européenne du 7 décembre 2023, notifiée sous le numéro C (2023)8708/3161649 autorisant le versement d'une aide d'Etat à La Poste en contrepartie du service universel postal au titre des années 2021-2025 ; Vu le code des postes et des communications électroniques, notamment ses articles L. 2- 2, L. 5-2, R. 1-1-27 à R. 1-1-29 ;

Vu le code des postes et des communications électroniques, notamment ses articles L. 2-2 et L. 5-2

Vu la loi n° 90-568 du 2 juillet 1990 relative à l'organisation du service public de La Poste et à France Télécom

Vu le contrat d'entreprise conclu entre l'Etat et La Poste du 26 juin 2023.

La Commission supérieure du numérique et des postes a été saisie le 4 mars 2024 par la Direction générale des entreprises en vue de rendre un avis sur le projet de décret relatif à la méthode d'évaluation du coût net lié aux obligations de service universel postal, pris en application de l'article L. 2-2 du Code des postes et des communications électroniques (CPCE), et portant diverses adaptations de la partie réglementaire du même code.

Le nouvel article 2.2 du CPCE, modifié par la loi n°2021-1900 du 30 décembre 2021 de finances pour 2022, entré en vigueur le 1er janvier 2022, dispose:

I- Le prestataire du service universel postal reçoit de l'Etat une compensation au titre de sa mission de service universel postal définie à l'article L. 1 et dans les textes pris pour son application, dans les conditions fixées par le contrat d'entreprise prévu à l'article 9 de la loi n° 90-568 du 2 juillet 1990 relative à l'organisation du service public de la poste et à France Télécom.

II. - Chaque année, l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse évalue le coût net du service universel postal. Le prestataire du service universel postal transmet à l'autorité, à la demande de celle-ci, les informations et les documents comptables nécessaires à cette évaluation.

Un décret en Conseil d'Etat, pris après avis de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse et de la Commission supérieure du numérique et des postes, précise la méthode d'évaluation utilisée pour le calcul du coût net de la mission de service universel postal

L'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse, après avis de la Commission supérieure du numérique et des postes, remet chaque année au Gouvernement et au Parlement un rapport sur le coût net du service universel postal »

Le projet de décret soumis pour avis à la Commission supérieure du numérique et des postes a pour objet de :

- supprimer les dispositions relatives au fonds de compensation qui figuraient au chapitre 1er du titre I de la partie II (Décrets en Conseil d'Etat) du CPCE,

- préciser la méthode d'évaluation du coût net lié aux obligations de service universel postal afin de permettre à l'Arcep de déterminer le montant du coût net supporté par le prestataire de service universel postal.

1 Sur les dispositions relatives à la suppression du fonds de compensation du service universel postal

Conformément aux articles 2 et 6 de la loi du 2 juillet 1990, l'Etat a confié à La Poste quatre missions de service public :

- Le service universel postal,

- La contribution de La Poste à l'aménagement et au développement du territoire,

- La mission d'accessibilité bancaire,

- Le transport et la distribution de la presse.

Ces missions sont par ailleurs encadrées par le contrat d'entreprise signé entre l'Etat et La Poste le 26 juin 2023 pour la période 2023-2027.

S'agissant plus particulièrement de la mission du service universel postal, les membres de la Commission supérieure rappellent que cette mission est devenue déficitaire pour la première fois en 2018 à hauteur de 365 millions d'euros.

Ce déficit s'explique par la baisse tendancielle du volume du courrier (6 milliards d'objets distribués en 2023 contre 9 milliards d'objets distribués en 2019). Le déclin de l'activité courrier a fait perdre au groupe La Poste plus de 6 milliards d'euros de recettes en dix ans.

Cette contraction spectaculaire du volume du courrier distribué a donc creusé très significativement le déficit du service universel postal qui s'est établi à 617 millions d'euros en 2021 (en coûts complets, hors effet des dépréciations des actifs courrier, après actualisation du réseau accessible). Le déficit du service universel postal pour l'année 2022 est en cours d'évaluation dans le cadre des travaux menés, comme chaque année, par l'Arcep.

Suivant une position constante, les membres de la Commission supérieure appellent l'Etat à compenser La Poste du coût net des missions de service public qui lui sont confiées et ont sollicité dès 2020 la tenue du comité de suivi de haut niveau afin de traiter ces sujets (avis n°2020-09 du 30 juin 2020).

Les membres de la Commission supérieure ont salué la décision prise par le gouvernement à l'issue de la réunion du comité de suivi de haut niveau le 22 juillet 2021, auquel la CSNP était représentée, de compenser le déficit de la mission de service universel postal et de verser à La Poste une dotation budgétaire annuelle, qui sera modulée en fonction des résultats de qualité de service entre 500 et 520 millions d'euros.

2 Sur la méthode d'évaluation du cout net lié aux obligations de service universel postal par l'Arcep

Les articles R.1-1-27, R.1-1-28 et R.1-1-29 précisent la définition du coût net du service universel postal, le principe de compensation financière par l'Etat du coût net de la mission du service universel postal et la méthode d'évaluation de ce coût net par l'Arcep, comme suit:

Article R.1-1-27 :

Le coût net du service universel postal correspond à la différence entre le coût net supporté par le prestataire du service universel postal lorsqu'il est soumis aux obligations résultant des dispositions législatives et réglementaires afférentes à l'exercice du service universel et celui qui est supporté par le même prestataire lorsqu'il n'est pas soumis à ces obligations.

Pour le calcul du coût net, il est également tenu compte de tous les autres éléments pertinents, notamment des bénéfices immatériels et des avantages commerciaux dont bénéficie le prestataire du service universel postal en raison de la prestation de ce service, et de son droit de réaliser un bénéfice raisonnable.

Article R.1-1-28 :

Les obligations de service universel auxquelles est soumis le prestataire du service universel postal en vertu des dispositions législatives et réglementaires afférentes à l'exercice du service universel constituent une charge financière inéquitable pour le prestataire du service universel postal ouvrant droit à compensation lorsque le coût net calculé à l'article R. 1-1-27 est positif.

Article R.1-1-29 :

Après avoir recueilli les observations du prestataire du service universel postal, l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse procède à l'évaluation du coût net du service universel postal selon la méthode définie à l'article R.1-1-27, à partir des informations et des documents comptables nécessaires à cette évaluation, transmis à l'autorité, à sa demande, par le prestataire du service universel postal. »

Les membres de la Commission supérieure relèvent que les dispositions des articles R.1-1-27, R.1-1-28 et R.1-1-29 reprennent les dispositions de la directive 97/67/CE du Parlement européen et du Conseil du 15 décembre 1997 modifiée concernant des règles communes pour le développement du marché intérieur des services postaux de la Communauté et l'amélioration de la qualité du service.

3 Avis de la Commission supérieure du numérique et des postes

La Commission supérieure constate que le projet de décret qui lui est soumis pour avis acte la suppression d'un fonds de compensation (ancienne section 3 du chapitre Ier du CPCE) qui n'avait jamais été activé et que le projet de décret précise les mesures d'application du nouvel article L2.2 du CPCE relatives au coût et au financement du service universel postal précisées aux articles R-1-1-27, R.1-1-28 et R.1-1-29 de ce texte.

La Commission supérieure du numérique et des postes se félicite que le présent projet de décret n'entraîne pas de surtransposition de la directive 97/67/CE et explicite l'article 7, paragraphe 3, de la directive en précisant dans son article R-1-1- 28 la notion de « charge financière inéquitable » pour le prestataire du service universel postal ouvrant droit à compensation lorsque le coût net, calculé conformément à l'article R. 1-1-27, est positif.

La Commission supérieure du numérique et des postes souligne l'engagement inscrit dans le contrat d'entreprise entre l'Etat et La Poste d'une compensation garantie sur les années 2023, 2024 et 2025. Cet engagement pluriannuel est indispensable pour permettre à l'ensemble des parties prenantes d'inscrire efficacement leurs actions dans la durée (déploiement des effectifs, dotations).

Par courrier en date du 31 janvier 2024, la Commission supérieure du numérique et des postes a sollicité auprès du Ministre de l'économie, des finances et de la souveraineté industrielle et numérique une réunion du comité de suivi du haut niveau pour s'assurer du financement des missions de service public confiées au groupe La Poste. Les membres de la Commission supérieur regrettent que le Ministre de l'économie et des finances ait répondu défavorablement à cette proposition par courrier en date du 12 mars 2024.

La Commission supérieure du numérique et des postes restera vigilante sur l'évolution de cette compensation dans le cadre des discussions à venir pour la désignation du prestataire de service public au-delà de 2025.

La Commission supérieure du numérique et des postes réaffirme sa position pour une juste compensation du coût des missions de service public confiées à La Poste, essentielle pour garantir dans le temps le niveau de qualité de service et la présence postale due à nos concitoyens.

Dans ces conditions, la Commission supérieure du numérique et des postes émet un avis favorable sur le projet de décret relatif à la méthode d'évaluation utilisée pour le calcul du coût net du service universel postal.

AVIS N° 2024-03 DU 21 MAI 2024 SUR LE PROJET DE LOI RELATIF A LA RESILIENCE DES ACTIVITES D'IMPORTANCE VITALE, A LA PROTECTION DES INFRASTRUCTURES CRITIQUES, A LA CYBERSECURITE ET A LA RESILIENCE OPERATIONNELLE NUMERIQUE DU SECTEUR FINANCIER

AVIS N° 2024-03 DU 21 MAI 2024 SUR LE PROJET DE LOI RELATIF A LA RESILIENCE DES ACTIVITES D'IMPORTANCE VITALE, A LA PROTECTION DES INFRASTRUCTURES CRITIQUES, A LA CYBERSECURITE ET A LA RESILIENCE OPERATIONNELLE NUMERIQUE DU SECTEUR FINANCIER

Vu la directive (UE) n°2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n°910/2014 et la directive (UE) 2018/1972 et abrogeant la directive (UE) 2019/1148 ; directive dite « NIS II » ;

Vu la loi n°2018- 133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité ;

Vu le projet de loi relatif à la résilience des activités d'importance vitale, à la protection des infrastructures critiques, à la cybersécurité et à la résilience opérationnelle numérique du secteur financier ;

Vu la saisine de l'ANSSI en date du 7 mai 2024 sur le titre II du projet de loi consacré à la cybersécurité ;

***

En mars 2024, les membres de la CSNP ont confié à M. Damien Michallet, sénateur de l'Isère et président de la CSNP, et Mme Anne Le Hénanff, députée du Morbihan, le pilotage d'un groupe de travail sur la transposition de la directive NIS 2 pour lequel Mme Anne Le Hénanff a été nommée rapporteur.

Le groupe de travail a instruit et présenté aux membres de la CSNP le présent avis portant sur le titre II du projet de loi consacré à la cybersécurité et présentera en juin 2024 un rapport plus complet sur les enjeux posés par la transposition de la directive NIS2.

Le présent avis formule 14 recommandations :

- **Sur l'élargissement du périmètre des entités soumises aux dispositions de la directive NIS 2**

Recommandation n°1 : Les membres de la CSNP regrettent que le projet de loi renvoie à des décrets en Conseil d'Etat et des décrets simples la liste des secteurs économiques critiques et hautement critiques ainsi que les seuils déterminant les entreprises soumises au projet de loi (nombre de salariés, chiffre d'affaires et bilan) pourtant précisés dans la directive NIS 2 et ses annexes et proposent que ces informations soient réintégrées dans la loi.

Recommandation n°2 : Les dispositions de la directive NIS 2 entreront en vigueur le 17 octobre 2024 et, à ce stade, la très grande majorité des 15 000 nouvelles entités qui entreront dans le périmètre du projet de loi ne sont pas informées de ces nouvelles mesures qui leur seront applicables. La CSNP recommande aux pouvoirs publics d'organiser une véritable campagne de communication à destination des entreprises et des collectivités locales. Cette campagne d'information à large échelle pourrait également inclure le grand public.

Recommandation n°3 : Les membres de la CSNP recommandent aux pouvoirs publics d'axer la communication sur les bénéfices de la mise en œuvre de la directive NIS2 et sur les atouts que représente le relèvement du niveau de sécurité numérique pour nos entreprises et nos collectivités locales et la sécurisation des données des clients et des usagers. Une labellisation NIS2 pourrait constituer une mesure incitative pour les entités qui auront fait l'effort de déployer les moyens nécessaires à la mise en conformité avec la directive NIS 2.

- **Sur les nouvelles obligations qui vont peser sur les nouvelles entités essentielles et importantes**

Recommandation n°4 : Les représentants des entreprises et des collectivités locales souhaitent que les obligations introduites par la directive NIS 2 soient hiérarchisées en fonction de leur niveau de priorité. Les membres de la CSNP recommandent à l'ANSSI de préciser et de classer les actions prioritaires à mettre en œuvre en fonction de l'état de préparation des structures.

Recommandation n°5 : Les membres de la CSNP recommandent à l'ANSSI d'ajuster les couts réels induits par la mise en conformité des nouvelles entités essentielles et importantes, soumises aux dispositions de loi de transposition de la directive NIS2.

Recommandation n°6 : L'application de la directive NIS 2 aux sous-traitants des entités essentielles et importantes suppose une adaptation des obligations contractuelles qui les lient. La CSNP recommande de développer des lignes directrices spécifiques sur la gestion des relations contractuelles avec les sous-traitants, y compris des clauses types pour les contrats et les obligations de conformité à des normes de sécurité précises. Les entités devraient également être encouragées à réaliser des audits réguliers de leurs sous-traitants et à obtenir des attestations de conformité de la part de ceux-ci.

Recommandation n°7 : Les membres de la CSNP recommandent de préciser dans le texte de loi la notion d'« incident important » en publiant une liste de critères objectivables par les entités essentielles et importantes. Par ailleurs, la CSNP recommande que le projet de loi prévoie des mécanismes explicites de protection des informations divulguées lors de signalement d'incidents, afin de garantir la confidentialité des données sensibles et stratégiques des entreprises qui pourraient être transmises dans le cadre d'une notification.

Recommandation n°8 : La CSNP propose que le projet de loi prévoie une clause d'adaptabilité aux évolutions technologiques liées, notamment, à l'usage de l'intelligence artificielle en matière de cybersécurité.

- **Sur le nécessaire accompagnement des nouvelles entités essentielles et importantes**

Recommandation n°9 : Les membres de la CSNP recommandent un renforcement de la présence de l'ANSSI en région, la clarification du rôle des CSIRT régionaux et la montée en puissance du dispositif www.cybermalveillance.gouv.fr pour accompagner les nouvelles entités essentielles et importantes dans leur mise en conformité avec la directive NIS2. Pour coordonner les initiatives qui se mettent en place, la CSNP recommande d'introduire dans le projet de loi un dispositif d'accompagnement territorial coordonné par l'ANSSI et les services de l'Etat, et articulant les différents organismes publics et privés concernés par la mise en œuvre des obligations inscrites dans le projet de loi, notamment les organismes consulaires, le GIP ACYMA, les CSIRT, les Campus Cyber, les organisations professionnelles et d'élus représentatives.

Recommandation n°10 : La CSNP recommande un accompagnement financier pour les entités ne disposant pas des moyens nécessaires à leur mise en conformité.

- **Sur le mécanisme de sanctions prévu par le projet de loi**

Recommandation n°11 : Les membres de la CSNP considèrent que la commission des sanctions indépendante, composée de magistrats du Conseil d'État, de la Cour de cassation et de la Cour des comptes, ainsi que de personnalités qualifiées est de nature rassurer les professionnels du droit et des parties prenantes sur l'indépendance de cette commission vis-à-vis de l'ANSSI qui exerce les fonctions de conseil et de superviseur. Compte tenu des délais trop courts de transposition, la CSNP recommande une souplesse dans l'appréciation des infractions aux obligations jusqu'au 31 décembre 2027.

- **Sur les délais de mise en conformité avec les dispositions de la directive NIS 2**

Recommandation n°12 : Pour tenir compte de ce principe de réalité, et pour créer une sécurité juridique des entités entrant dans le périmètre de la loi, les membres de la CSNP souhaitent que la loi précise que les délais de mise en conformité sont fixés au 31 décembre 2027. Si les décrets et textes règlementaires étaient pris avec beaucoup de retard, comme cela avait été le cas dans le cadre de la transposition de la directive NIS1, le législateur serait en mesure de voter une loi rectificative.

- **Sur l'harmonisation européenne de la transposition de la directive NIS 2**

Recommandation n°13 : La CSNP recommande de promouvoir une approche harmonisée au niveau de l'Union européenne dans la transposition de la directive NIS 2, afin de faciliter la conformité pour les entreprises opérant à l'échelle européenne et d'éviter l'apparition de différentiels de régulation pouvant créer des effets de concurrence entre les législations européennes.

- **Sur l'obligation d'information sur les risques numériques et les précautions à adopter**

Recommandation n°14 : Pour renforcer la sécurité générale, les fournisseurs de produits et services numériques pourraient être tenus de fournir une information claire et complète à leurs utilisateurs sur les risques numériques et les précautions à prendre.

I. Eléments de contexte

L'Agence nationale de sécurité des systèmes informatiques (ANSSI) a saisi le 7 mai 2024 la Commission supérieure du numérique et des postes (CSNP) pour rendre un avis sur les dispositions du titre II « Cybersécurité », consacré à la transposition de la directive NIS 2, du projet de loi relatif à la résilience des activités d'importance vitale, à la protection des infrastructures critiques, à la cybersécurité et à la résilience opérationnelle numérique du secteur financier.

La directive NIS 2 a été adoptée le 14 décembre 2022 et devra être transposée dans tous les États membres le 17 octobre 2024 au plus tard. En France, cette transposition est pilotée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

La Directive NIS 2, dont l'adoption a été portée et soutenue par les autorités françaises, vise à renforcer le niveau de cybersécurité introduit par la directive dite NIS 1[1] qui était centrée sur les opérateurs de services essentiels (OSE), et les fournisseurs de services numériques (FSN).

La directive NIS 1 avait identifié six secteurs essentiels (Energie, transports, Banque et marchés financiers, Santé, Eau potable, Infrastructures numériques), auxquels la France avait ajouté six autres secteurs dont les enjeux étaient jugés prioritaires au niveau national (Assurance, Restauration, Traitement des eaux, Education, Emploi et formation, Organismes sociaux).

Dans son annexe I, la directive NIS 2 reprend et complète certains secteurs inclus par la France au niveau national en 2018. Elle établit une liste des secteurs hautement critiques : l'énergie (électricité, réseaux de chaleur et de froid, pétrole, gaz, hydrogène), les transports (transports aériens, transports ferroviaires, transports par eau, transports routiers) le secteur bancaire, les infrastructures de marchés financiers, la santé, l'eau potable, les eaux usées, l'infrastructure numérique, la gestion des services TIC, l'administration publique, l'espace.

Dans son annexe II, la directive NIS 2 établit également une liste des secteurs critiques : les services postaux et d'expédition, la gestion des déchets, la fabrication, production et distribution de produits chimiques, la production, transformation et distribution de denrées alimentaires, la fabrication de certains produits (dispositifs médicaux notamment de diagnostic in vitro, de produits informatiques, électroniques et optiques, d'équipements électriques, de véhicules automobiles, remorques et semi-remorques, de matériel de transport, autres produits), les fournisseurs numériques et la recherche.

En intégrant dans son champ d'application, des collectivités territoriales de plus de 30 000 habitants et des entreprises privées répondant aux critères de seuils établis par la recommandation de la Commission européenne C (2003) 1422 du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises, la directive NIS 2 introduit un changement de paradigme en instaurant un niveau de sécurité collectif.

Au vu de l'augmentation exponentielle du nombre de cyberattaques motivées par la recherche de gains financiers, l'espionnage ou la déstabilisation et de ses conséquences désastreuses pour les entreprises françaises mais également pour des services publics aussi essentiels que les hôpitaux, pour la protection des données personnelles et sensibles de nos concitoyens et des infrastructures françaises, les membres de la CSNP ne peuvent que se féliciter du relèvement du niveau global de la sécurité numérique que va permettre la mise en application de la directive NIS2.

Pour autant, les membres de la CSNP sont également très conscients des contraintes qui vont peser

[1] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union

sur les structures, parfois de taille moyenne, qui n'étaient pas concernées par la directive NIS1 et se retrouvent désormais dans la catégorie des entités importantes.

Enfin, contrairement au dispositif issu de la directive NIS1, le projet de loi prévoit des sanctions financières et pénales dans le cas de certains manquements à ses dispositions.

II. Sur l'élargissement du périmètre des entités soumises à la directive NIS 2

L'article 6 du projet de loi distingue les entités essentielles actives pour l'essentiel dans des secteurs hautement critiques des entités importantes *cf. encadré n°1*.

Les entités essentielles sont des organisations appartenant à des secteurs d'activité hautement critiques, fixés par décret en Conseil d'Etat, dont les effectifs, le chiffre d'affaires annuel et le total du bilan annuel excèdent des seuils définis par voie règlementaire. Ces entités incluent des établissements publics à caractère industriel et commercial, des opérateurs de services de confiance qualifiés, des offices d'enregistrement, des fournisseurs de service de système de noms de domaine, ainsi que certaines administrations publiques et collectivités territoriales.

Les entités importantes appartiennent à des secteurs critiques, également fixés par décret, qui ne répondent pas aux critères des entités essentielles mais dépassent des seuils définis par voie règlementaire. Elles comprennent, entre autres, des opérateurs de service de confiance, des communautés de communes et des établissements d'enseignement menant des activités de recherche.

Le Premier ministre peut désigner des entités comme essentielles ou importantes, indépendamment de leur taille, si elles répondent à des critères spécifiques tels que l'unicité de leur service sur le territoire national, l'impact potentiel de leur perturbation sur la sécurité publique, ou leur importance systémique.

En France, une grande partie des entités essentielles sont des structures déjà sensibilisées ou confrontées à la menace cyber et sont déjà soumises aux dispositions de la directive NIS1 et/ou au dispositif de sécurité des activités d'importance vitale (SAIV).

Le projet de loi prévoit une application sans restriction des dispositions de la directive NIS 2 relatives à la définition des entités concernées mais renvoie pour la fixation des critères et seuils, des secteurs hautement critiques et critiques à un décret en Conseil d'Etat.

Pour le secteur privé, les seuils fixés par la directive NIS 2 sont les suivants :

Taille Entité	**Nombre d'employés**	**Chiffre d'affaires (millions €)**	**Bilan annuel (millions €)**	**Classification Annexe 1**	**Classification Annexe 2**
Intermédiaire et grande	Supérieur à 250	Supérieur à 50	Supérieur à 43	Entités essentielles	Entités importante
Moyenne	Entre 50 et 250	Compris entre 10 et 50	Compris entre 10 et 43	Entités importantes	Entités importante
Micro et petite	Inférieur à 50	Inférieur à 10	Inférieur à 10	Non concernées	Non concernées

Source : ANSSI

Le changement majeur introduit par la transposition de la directive NIS 2 porte sur l'extension aux entités importantes, aux collectivités locales de plus de 30 000 habitants et aux entreprises privées qui dépasseront certains seuils (nombre de salariés, chiffre d'affaires, bilan) qui seront définis par décret tel que le renvoie le projet de loi qui a été soumis aux membres de la CSNP.

Article 6 du projet de loi

I. – Sont des entités essentielles :

1° Les entités appartenant à une catégorie relevant des secteurs d'activité hautement critiques fixés par décret en Conseil d'Etat, et dont les effectifs, le chiffre d'affaires annuel ou le total du bilan annuel excèdent des seuils définis par voie réglementaire ;

2° Les établissements publics à caractère industriel et commercial rattachés à une administration mentionnée au 7°, appartenant à une catégorie relevant des secteurs d'activité hautement critiques fixés par décret en Conseil d'Etat et répondant aux critères et seuils définis par voie règlementaire ;

3° Les opérateurs mentionnés au 15° de l'article L. 32 du code des postes et des communications électroniques dont les effectifs, le chiffre d'affaires annuel ou le total du bilan annuel excèdent des seuils définis par voie réglementaire ;

4° Les prestataires de service de confiance qualifiés ;

5° Les offices d'enregistrement ;

6° Les fournisseurs de services de système de noms de domaine ;

7° Les administrations suivantes :a) Les administrations de l'Etat et leurs établissements publics administratifs, à l'exception des administrations de l'État qui exercent leurs activités dans les domaines de la sécurité publique, de la défense et de la sécurité nationale, de la répression pénale , ou des missions diplomatiques et consulaires françaises et de leurs réseaux et systèmes d'information, et de leurs établissements publics administratifs qui exercent dans les mêmes domaines ou qui sont désignés entité importante ou exclus par voie règlementaire ;

b) Les régions, les départements, les communes d'une population supérieure à 30 000 habitants, leurs établissements publics administratifs dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques prévus par décret en Conseil d'Etat ;

c) Les centres de gestion mentionnés à l'article L. 452-1 du code général de la fonction publique ;

d) Les services départementaux d'incendie et de secours mentionnés à l'article L. 1424-1 du code général des collectivités territoriales ; … »

e) Les communautés urbaines, les communautés d'agglomération et les métropoles, leurs établissements publics administratifs dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques fixés par décret en Conseil d'Etat ;

f) Les syndicats mentionnés aux articles L. 5212-1, L. 5711-1 et L. 5721-2 du code général des collectivités territoriales dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques fixé par décret en Conseil d'Etat et dont la population est supérieure à 30 000 habitants ;

g) Les institutions et organismes interdépartementaux mentionnés à l'article L. 5421-1 du code général des collectivités territoriales dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques fixés par décret en Conseil d'Etat ;

h) Et les autres organismes publics ou privés chargés d'une mission de service public administratif, à l'exception de ceux qui sont qui sont désignés entité importante ou exclus par voie règlementaire ;

8° Les opérateurs mentionnés à l'article L. 1332-8 du code de la défense ;

9° Les entités désignées avant le 16 janvier 2023 par le Premier ministre comme opérateurs de services essentiels en application des dispositions de l'article 5 de la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité ;

10° Les établissements d'enseignement menant des activités de recherche désignés par le Premier ministre, sous réserve de justifier cette désignation au regard de l'un des critères mentionnés au III du présent article.

*II. – **Sont des entités importantes :***

1° Les entités appartenant à une catégorie relevant des secteurs d'activité hautement critiques ou critiques fixés par décret en Conseil d'Etat qui ne sont pas des entités essentielles et dont les effectifs, le chiffre d'affaires annuel ou le total du bilan annuel excèdent des seuils définis par voie réglementaire ;

2° Les opérateurs mentionnés au 15° de l'article L. 32 du code des postes et des communications électroniques qui ne sont pas des entités essentielles ;

3° Les prestataires de services de confiance qui ne sont pas des entités essentielles ;

4° Les communautés de communes et leurs établissements publics administratifs dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques fixés par décret en conseil d'Etat ;

5° Les établissements d'enseignement menant des activités de recherche qui ne sont pas des entités essentielles, sauf s'ils sont exclus par voie réglementaire ;

6° Les établissement publics administratifs mentionnés au a du 7° du I expressément désignés comme telles ;

Dans son projet d'étude d'impact, l'ANSSI estime que 1489 collectivités territoriales, groupements de collectivités territoriales et certains organismes sous leur tutelle devraient être concernés au titre des entités essentielles. 992 communautés de communes métropolitaines et d'outre-mer seront, quant à elles, concernées au titre des entités importantes.

Le nombre d'entreprises privées concernées seraient, selon l'ANSSI, de l'ordre de 14 000. Après consultation des organisations représentatives des entreprises, ce nombre pourrait être plus élevé.

Au vu des auditions conduites par le groupe de travail sur la transposition de la directive NIS2, des interrogations subsistent sur la faculté pour certaines entités de savoir précisément si elles relèveront du champ d'application de la nouvelle loi.

C'est notamment le cas des collectivités locales. Le seuil de 30 000 habitants introduit par la directive NIS 2 et repris par l'article 6 du projet de loi paraît très facilement applicable mais certaines collectivités locales qui ne sont pas concernées par ce seuil s'interrogent malgré tout sur leur possible entrée dans le champ d'application de la loi dès lors qu'elle fournisse un service qui relève de l'annexe I ou de l'annexe II de la directive NIS 2, notamment un service de gestion lié au traitement ou de gestion de fourniture d'énergie, d'eau potable, des eaux usées ou de déchets.

C'est également le cas pour certaines entreprises qui ne sont pas concernées en raison des critères de seuils mais dont l'activité relève des secteurs économiques critiques et hautement critiques.

La plateforme mis en place par l'ANSSI pour répondre à ces interrogations ne répondrait pas totalement aux préoccupations de ces entités. Il est important que l'ANSSI puisse apporter une réponse claire et précise sur ce point aux entités potentiellement concernées.

Recommandation n°1 : Les membres de la CSNP regrettent que le projet de loi renvoie à des décrets en Conseil d'Etat et des décrets simples la liste des secteurs économiques critiques et hautement critiques ainsi que les seuils déterminant les entreprises soumises au projet de loi (nombre de salariés, chiffre d'affaires et bilan) pourtant précisés dans la directive NIS 2 et ses annexes et proposent que ces informations soient réintégrées dans la loi.

Après l'adoption du projet de loi et l'entrée en vigueur de la directive NIS2, le nombre d'entités relevant du champ d'application de ces textes va passer de 500 entités sous le régime de la directive NIS 1 à 15 000 entités entrant dans le périmètre de NIS 2.

Il convient de préciser que, contrairement aux entités régulées par la directive NIS1, les entités concernées par la directive NIS 2 ne seront pas désignées par l'ANSSI mais devront analyser, elles-mêmes, les critères et seuils qui leur permettront de définir si elles sont ou non assujetties à la directive NIS 2 et au projet de loi.

L'ANSSI a procédé depuis l'automne 2023 à des consultations très larges pour recueillir les préoccupations des parties prenantes. Les fédérations et les organisations représentatives des entreprises et des collectivités locales qui ont participé à ces consultations ont été, pour la plupart d'entre elles, auditionnées par le groupe de travail constitué par la CSNP.

Il ressort de ces auditions qu'à quelques mois de l'entrée en vigueur de la directive NIS2, le 17 octobre prochain, il est plus que vraisemblable que de très nombreuses entreprises et collectivités locales ne sont pas pleinement informées de l'existence de cette entrée en vigueur, des nouvelles obligations qui pèseront sur elles et des mesures qu'elles devront prendre pour s'y conformer.

Du point de vue des membres de la CSNP, il est essentiel d'activer une campagne d'information nationale pour informer ces acteurs. Cette information à large échelle, qui pourrait inclure le grand public, est une demande récurrente de toutes les organisations professionnelles auditionnées.

Recommandation n°2 : Les dispositions de la directive NIS 2 entreront en vigueur le 17 octobre 2024 et, à ce stade, la très grande majorité des 15 000 nouvelles entités qui entreront dans le périmètre du projet de loi ne sont pas informées de ces nouvelles mesures qui leur seront applicables. La CSNP recommande aux pouvoirs publics d'organiser une véritable campagne de communication à destination des entreprises et des collectivités locales. Cette campagne d'information à large échelle pourrait également inclure le grand public.

Recommandation n°3 : Les membres de la CSNP recommandent aux pouvoirs publics d'axer la communication sur les bénéfices de la mise en œuvre de la directive NIS2 et sur les atouts que représente le relèvement du niveau de sécurité numérique pour nos entreprises et nos collectivités locales et la sécurisation des données des clients et des usagers. Une labellisation NIS2 pourrait constituer une mesure incitative pour les entités qui auront fait l'effort de déployer les moyens nécessaires à la mise en conformité avec la directive NIS 2.

III. Sur les nouvelles obligations qui vont peser sur les nouvelles entités essentielles et importantes

A. Les nouvelles obligations introduites par la directive NIS 2

Les obligations qui pèsent sur les entités essentielles et importantes sont contenues dans le projet de loi, mais également et pour l'essentiel, seront définies par décrets.

A ce stade, ces obligations portent :

- sur leur déclaration auprès de l'ANSSI (article 7 du projet de loi) qui doit elle-même établir et notifier une liste des entités essentielles à la Commission européenne fin 2025 ;
- sur l'adoption de mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et systèmes d'information qu'elles utilisent dans le cadre de leurs activités ou de la fourniture de leurs services, ainsi que pour éliminer ou réduire les conséquences que les incidents ont sur les destinataires de leurs services et sur d'autres services (article 9 du projet de loi).
- sur la formation à la cybersécurité les membres des comités exécutifs et les personnels exposés aux risques de services (article 9 du projet de loi)
- Sur la protection des réseaux et systèmes d'information, y compris en cas de recours à la sous-traitance (article 9 du projet de loi) ;
- sur la mise en place d'outils et de procédures pour assurer la défense des réseaux et systèmes d'information et gérer des incidents (article 9 du projet de loi) ;
- sur l'adoption d'un plan de résilience des activités (article 9 du projet de loi) ;
- sur la notification sans retard injustifié à l'ANSSI de tout incident ayant un impact important sur la fourniture de leurs services (article 11 du projet de loi).

Un décret en Conseil d'Etat doit fixer la nature de gestion des risques auxquelles doivent se conformer ces entités.

Il n'appartient pas aux membres de la CSNP de se prononcer sur les aspects techniques des obligations qui seront imposées aux entreprises et collectivités locales qui seront précisées dans un référentiel fixé par décret en Conseil d'Etat.

Les membres de la CSNP relèvent cependant que les représentants des entreprises et des collectivités locales souhaitent que les obligations introduites par la directive NIS 2 soient hiérarchisées en fonction de leur niveau de priorité.

Recommandation n°4 : Les membres de la CSNP recommandent à l'ANSSI de préciser et de classer les actions prioritaires à mettre en œuvre en fonction de l'état de préparation des structures.

B. Nécessité de disposer d'une étude d'impact plus précise

La mise en place des mesures et procédures prévues à l'article 9 du projet de loi suppose pour de nombreuses entités l'élaboration d'un diagnostic de l'existant, de recours à des services de consultants, de l'achat de solutions numériques, de la mise en place de plan de formation à la cybersécurité. Ces mesures ont un coût et supposent des ressources humaines qui ne sont pas forcément disponibles.

Dans son projet d'étude d'impact, l'ANSSI indique que le niveau d'ambition pour les entités importantes n'excèdera pas celui des règles d'hygiène informatique largement préconisées par l'ANSSI. Pour une entité importante de moins de 100 salariés, le coût total pour atteindre les objectifs, en partant d'un niveau initial proche de zéro, se situe dans un ordre de grandeur de 100 000 à 200 000€. Selon l'ANSSI, il est toutefois rare qu'une entité parte d'un niveau si faible en matière de sécurité numérique. Ainsi, de nombreux services et équipements numériques intègrent nativement des éléments de cybersécurité, même élémentaires.

En tout état de cause, les représentants des collectivités locales auditionnés ont indiqué que des budgets de l'ordre de 50 000 euros à 100 000 euros étaient, pour certaines entités, difficile à financer. Il est donc essentiel d'encourager l'élaboration de guides pratiques et de cadres de référence, financés par l'Etat, pour aider et accompagner les entités publiques et privées les plus petites à appréhender de façon simple le processus de conformité de manière économiquement viable, et à le maintenir dans la durée.

Quant aux représentants des entreprises, ils considèrent que ces données sont très en deçà des couts effectifs que va générer la mise en conformité.

Recommandation n°5 : Les membres de la CSNP recommandent à l'ANSSI d'ajuster les couts réels induits par la mise en conformité des nouvelles entités essentielles et importantes soumises aux dispositions de loi de transposition de la directive NIS2.

C. Extension du périmètre aux sous-traitants

L'article 9 impose la protection des réseaux et systèmes d'information, y compris en cas de recours à la sous-traitance. Cette extension aux sous-traitants interroge et inquiète.

En effet, de nombreux représentants des entités considèrent qu'une grande majorité de celles-ci ne dispose pas des moyens d'obtenir une vision complète et détaillée des mesures de sécurité numériques mises en œuvre par leurs fournisseurs et sous-traitants. La directive NIS 2 souligne l'importance de sécuriser la chaine d'approvisionnement mais sans spécifier le niveau de diligence ou les mesures de sécurité précises à exiger des fournisseurs.

Combinée au nouveau pouvoir de sanction qui est conféré à l'ANSSI, cette disposition leur fait craindre aux entités concernées qu'elles pourront être mises en cause pour des défaillances observées chez leurs sous-traitants. Pour anticiper et se prémunir ces défaillances, les entités essentielles et importantes vont devoir entamer un travail lourd et long de révision des contrats qui les lient à leurs fournisseurs et sous-traitants qui pourraient, selon certains juristes, prendre à l'échelle nationale, plus de deux ans.

Recommandation n°6 : L'application de la directive NIS 2 aux sous-traitants des entités essentielles et importantes suppose une adaptation des obligations contractuelles qui les lient. La CSNP recommande de développer des lignes directrices spécifiques sur la gestion des relations contractuelles avec les sous-traitants, y compris des clauses types pour les contrats et les obligations de conformité à des normes de sécurité précises. Les entités devraient également être encouragées à réaliser des audits réguliers de leurs sous-traitants et à obtenir des attestations de conformité de la part de ceux-ci.

D. Précisions attendues sur la notion de « tout incident ayant un impact important »

L'obligation de notification « sans retard injustifié » à l'ANSSI de « tout incident ayant un impact important » sur la fourniture de leurs services paraît insuffisamment précis.

En effet, il n'est pas rare qu'une attaque cyber ne soit pas immédiatement identifiée et que l'ampleur de son impact- important ou pas - soit parfois difficilement évaluable.

La notion d'incident important retenue par l'ANSSI est celle de la Loi de Programmation Militaire et correspond à la jurisprudence construite de manière itérative dans le cadre de NIS1.

Pour une entreprise ou une collectivité locale, cette notion peut évoluer et être appréciée différemment au fil du temps et de la découverte des conséquences d'un incident sur le fonctionnement des SI.

Un décret en Conseil d'Etat précisera la procédure applicable et les critères d'appréciation des caractères importants et critiques des incidents et vulnérabilités ainsi que les délais de notification des incidents et des vulnérabilités.

Les membres de la CSNP sont confiants dans le fait que l'ANSSI appréciera avec une grille de lecture adaptée et contextualisée cette obligation mis en place par l'article 11 du projet de loi mais alertent sur les risques juridiques qui pourront peser pour les entités essentielles et importantes en cas de contentieux avec leurs clients, leurs administrés, leurs fournisseurs ou leurs sous-traitants.

Un guide de bonnes pratiques est souhaité et attendu par les entités interrogées.

Recommandation n°7 : Les membres de la CSNP recommandent de préciser dans le texte de loi la notion d'« incident important » en publiant une liste de critères objectivables par les entité essentielles et importantes. Par ailleurs, la CSNP recommande que le projet de loi prévoie des mécanismes explicites de protection des informations divulguées lors de signalement d'incidents, afin de garantir la confidentialité des données sensibles et stratégiques des entreprises qui pourraient être transmises dans le cadre d'une notification.

Recommandation n°8 : La CSNP propose que le projet de loi prévoie une clause d'adaptabilité aux évolutions technologiques liées notamment à l'usage de l'intelligence artificielle en matière de cybersécurité.

IV. Sur le nécessaire accompagnement des nouvelles entités essentielles et importantes

L'élargissement considérable du périmètre des entités couvertes par le projet de loi transposant la directive NIS2 suppose un accompagnement approprié des entités potentiellement concernées.

Au-delà des couts, c'est la possibilité même de trouver des personnels suffisamment qualifiés pour mettre en œuvre ces dispositions qui est questionnée dans certaines régions où les ressources humaines sont rares et les contraintes salariales liées aux grilles indiciaires de la fonction publique territoriale sont inadaptées au marché de l'emploi.

L'ANSSI indique, dans le projet d'étude d'impact, qu'elle utilisera les relais, notamment sectoriels, qui faciliteront les échanges d'information avec les entités régulées. Les membres de la CSNP appellent l'ANSSI à ne pas sous-évaluer la disparité de situation et d'expertise selon les territoires.

En effet, certains territoires ne disposent tout simplement pas des ressources humaines ou des prestataires compétents en matière de cybersécurité pour accompagner les nouvelles entités essentielles ou importantes au sens de la directive NIS2.

Il apparait donc essentiel de prévoir un accompagnement de ces entités. Pour les membres de la CSNP, cet accompagnement passe par un renforcement de la présence de l'ANSSI en région, par la clarification du rôle des CSIRT régionaux et par la montée en puissance du dispositif www.cybermalveillance.gouv.fr

A. Accompagnement par l'ANSSI

Pour passer de 600 entités concernées par la directive NIS1 à 15 000 entités environ concernées par la directive NIS2, l'ANSSI sollicite la création de 60 emplois temps plein.

L'ANSSI estime que son organisation actuelle est dimensionnée pour entretenir une relation de relative proximité avec les 600 OIV et les OSE mais que « *le changement d'échelle induit par les critères retenus dans la directive NIS 2 ne sera cependant pas répercuté dans les mêmes proportions au sein de l'autorité nationale. Les mécanismes de régulation retenus, et notamment celui consistant à demander aux entités assujetties de se déclarer elles-mêmes auprès de l'autorité nationale, permettront d'alléger la charge de travail administratif de l'autorité. Par ailleurs, l'expérience de plusieurs années d'accompagnement et d'évaluation permet à l'autorité nationale de développer des outils numériques afin d'automatiser une importante partie de la relation avec les assujettis, ce qui limitera également le besoin de renfort en effectif. ».*

Les membres de la CSNP ne sont pas pleinement convaincus par cette analyse et préconisent de renforcer la présence de l'ANSSI en région, limitée actuellement à deux seuls ETP par région.

B. Clarification du rôle jouée par les CSIRT régionaux

Pour les membres de la CSNP, il paraît important de préciser le positionnement des CSIRT régionaux ou sectoriels dans le dispositif d'accompagnement du projet de loi. Les membres de la CSNP ne souhaitent pas une surtransposition de la directive NIS2 mais considèrent que l'adoption de la loi pourrait être l'occasion de clarifier le rôle des CSIRT régionaux dans le dispositif français de la cybersécurité.

C. Montée en puissance du dispositif cybermalveillance.gouv.fr

Le dispositif *cybermalveillance.gouv.fr* mis en place en 2017 avec le GIP ACYMA semble recueillir la confiance des usagers, des collectivités locales et des entreprises. Comme le préconise le rapport de

la Cour des comptes de mars 2022, une montée en puissance et un renforcement des moyens du dispositif serait de nature à combler la « diagonale du vide » dont souffrent certains territoires.

Recommandation n°9 : Les membres de la CSNP recommandent un renforcement de la présence de l'ANSSI en région, la clarification du rôle des CSIRT régionaux et la montée en puissance du dispositif www.cybermalveillance.gouv.fr pour accompagner les nouvelles entités essentielles et importantes dans leur mise en conformité avec la directive NIS2. Pour coordonner les initiatives qui se mettent en place, la CSNP recommande d'introduire dans le projet de loi un dispositif d'accompagnement territorial coordonné par l'ANSSI et les services de l'Etat, et articulant les différents organismes publics et privés concernés par la mise en œuvre des obligations inscrites dans le projet de loi, notamment les organismes consulaires, le GIP ACYMA, les CSIRT, les Campus Cyber, les organisations professionnelles et d'élus représentatives.

Recommandation n°10 : La CSNP recommande un accompagnement financier pour les entités ne disposant pas des moyens nécessaires à leur mise en conformité.

V. Sur le mécanisme de sanctions prévu par le projet de loi

Pour homogénéiser les sanctions prévues dans le dispositif SAIV, dans la mise en œuvre de la directive NIS 2 révisée et des règlements CSA et eIDAS, il est prévu le principe de l'instauration de sanctions administratives applicables aux manquements de toutes ces réglementations. Celles-ci prennent selon les cas la forme d'amendes administratives, d'astreintes, d'une suspension de certaines activités pour une entité ou d'interdiction temporaire d'exercice de ses responsabilités par son dirigeant, d'une abrogation d'une certification, d'une qualification ou d'une autorisation.

Le chapitre III du projet de loi précise les modalités de la supervision et de la constatation des manquements.

La commission des sanctions aura la faculté de décider dans chaque cas d'un montant individualisé, proportionné à la gravité des faits dans la limite du niveau maximum à savoir 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial hors taxes ou 7 millions d'euros ou 1,4 % du chiffre d'affaires annuel mondial hors taxes en fonction des entités concernées.

Compte tenu des délais de mise en conformité, la CSNP recommande une souplesse dans l'appréciation des infractions aux obligations jusqu'au 31 décembre 2027

Recommandation n°11 : Les membres de la CSNP considèrent que la commission des sanctions indépendante, composée de magistrats du Conseil d'État, de la Cour de cassation et de la Cour des comptes, ainsi que de personnalités qualifiées est de nature rassurer les professionnels du droit et des parties prenantes sur l'indépendance de cette commission vis-à-vis de l'ANSSI qui exerce les fonctions de conseil et de superviseur. Compte tenu des délais trop courts de transposition, la CSNP recommande une souplesse dans l'appréciation des infractions aux obligations jusqu'au 31 décembre 2027.

VI. Sur les délais de mise en conformité avec les dispositions de la directive NIS 2

La transposition française entrera en application au plus tard le 17 octobre 2024. Dès l'entrée en vigueur de la loi, les entités concernées auront l'obligation de s'enregistrer auprès de l'autorité nationale de cybersécurité.

Le projet d'étude d'impact produit par l'ANSSI indique que « *la réglementation NIS 2, telle que mise en œuvre en France, définira des délais de mise en conformité qui tiendront compte des efforts de compréhension, de montée en compétence et d'investissement que les exigences imposent aux*

assujettis. Les lignes directrices et les objectifs de haut niveau font partie des textes publiés depuis fin 2022, mais les textes précis de transposition ne seront connus du grand public qu'à la suite de la phase règlementaire[2]. Une mise en œuvre de contrôles susceptibles de découler sur des sanctions n'est pas envisagée avant plusieurs années. »

Au vu des auditions conduites par la CSNP, le délai de trois ans pour permettre à certaines entités essentielles et importantes, les moins préparées, de se conformer aux exigences de l'article 9 du projet de loi paraît incompressible. Il sera sans doute nécessaire d'établir des étapes intermédiaires avec des délais spécifiques, en fonction de la nature et des moyens dont disposent les différentes catégories d'entités régulées, pour la mise en place des mesures de sécurité.

Recommandation n°12 : Pour tenir compte de ce principe de réalité, et pour créer une sécurité juridique des entités entrant dans le périmètre de la loi, les membres de la CSNP souhaitent que la loi précise que les délais de mise en conformité sont fixés au 31 décembre 2027. Si les décrets et textes règlementaires étaient pris avec beaucoup de retard comme cela avait été le cas dans le cadre de la transposition de la directive NIS1, le législateur serait en mesure de voter une loi rectificative.

VII. Sur l'harmonisation européenne de la transposition de la directive NIS 2

Les risques d'hétérogénéité dans la transposition de la directive NIS2 entre Etats membres, pourrait entrainer des difficultés pour les entreprises opérant à l'échelle européenne, ainsi que l'apparition de pavillons de complaisance de la conformité, comme ce fût le cas avec l'application du RGPD par exemple.

Recommandation n°13 : La CSNP recommande de promouvoir une approche harmonisée au niveau de l'Union européenne dans la transposition de la directive NIS 2, afin de faciliter la conformité pour les entreprises opérant à l'échelle européenne et d'éviter l'apparition de différentiels de régulation pouvant créer des effets de concurrence entre les législations européennes.

VIII. Sur l'obligation d'information sur les risques numériques et les précautions à adopter

Tous les fournisseurs de produits et services numériques, notamment les éditeurs de logiciels, les fabricants et revendeurs d'équipements, de matériels, indépendamment de leur statut d'entité essentielle et ou importante, pourraient être tenus de fournir à leurs clients, particulièrement lorsque ceux-ci sont des entités importantes, une documentation détaillée sur les risques numériques associés à l'utilisation de leurs produits et de leurs services dans le cadre de la directive NIS 2. Cette documentation régulièrement mise à jour permettrait aux utilisateurs de disposer, dans un style clair et pédagogique destiné à des non-initiés, des informations les plus récentes et pertinentes pour garantir la sécurité et l'usage conforme de leurs services ou produits, et des recommandations d'usage sécurisé adaptées aux entités importantes ne disposant pas de compétences de haut niveau en matière de cybersécurité.

Recommandation n°14 : Pour renforcer la sécurité générale, les fournisseurs de produits et services numériques pourraient être tenus de fournir une information claire et complète à leurs utilisateurs sur les risques numériques et les précautions à prendre.

[2] Un décret en Conseil d'Etat doit préciser la liste des secteurs d'activité critiques et hautement critiques. Trois décrets simples seront pris pour préciser les seuils pour les entités essentielles, les entités importantes et les opérateurs du code des postes et des communications électroniques, les modalités de désignation unitaire de certaines entités par le Premier ministre et les modalités de communication des informations nécessaires à l'établissement de la liste des entités.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

COMMISSION SUPERIEURE DU NUMERIQUE ET DES POSTES

AVIS N° 2024-04 DU 06 JUIN 2024

« LES CONSEQUENCES DES COUPES BUDGETAIRES SUR LE PLAN FRANCE TRES HAUT DEBIT, AU REGARD DES ENJEUX DE DEPLOIEMENT, DE RESILIENCE ET DE LA FERMETURE DU RESEAU CUIVRE. »

LES RECOMMANDATIONS DE LA COMMISSION SUPERIEURE DU NUMERIQUE ET DES POSTES (CSNP)

AVIS N° 2024-04 DU 6 JUIN 2024 SUR « LES CONSEQUENCES DES COUPES BUDGETAIRES SUR LE PLAN FRANCE TRES HAUT DEBIT, AU REGARD DES ENJEUX DE DEPLOIEMENT, DE RESILIENCE ET DE LA FERMETURE DU RESEAU CUIVRE. »

Le gouvernement a annoncé la 21 février 2024, par décret[1], des coupes budgétaires massives. Les coupes budgétaires, de l'ordre de 38 millions € d'autorisations d'engagement sur les 96 millions € qui étaient prévus ainsi que 117 millions € de crédits de paiement annulés, soit au total 155 millions € de dotations en moins, interrogent sur la fin du déploiement du Plan France Très haut Débit.

Les membres de la Commission Supérieure du Numérique et des Postes (CSNP) ont confié à Monsieur le Sénateur Christian Redon-Sarrazy et Monsieur le député Xavier Batut, le pilotage d'un groupe de travail pour mesurer l'impact de ces coupes budgétaires sur l'avancement du Plan France Très Haut Débit et formuler des recommandations pour assurer la bonne fin de ce programme.

Le Plan France Très Haut Débit a permis de mobiliser des investissements massifs pour le déploiement du Très haut Débit et de la fibre optique. Si la mise en œuvre de ce PFTHD place notre pays en position très favorable au niveau européen dans le déploiement des réseaux en fibre optique avec 86% des foyers[2] qui sont raccordables, les raccordements longs et complexes doivent encore être finalisés.

Les membres de la Commission Supérieure du Numérique et des Postes ont déjà eu l'occasion de prendre position sur le « reste à faire » et ont indiqué que des aides publiques supplémentaires seront nécessaires pour mener à terme le PFTHD et passer du « 100% raccordables au 100% raccordés ».

A l'issue de ses travaux, le groupe de travail piloté par Monsieur Christian Redon-Sarrazy et Monsieur Xavier Batut a formulé 12 recommandations :

- **Des coupes budgétaires importantes alors que le PFTHD nécessite des crédits supplémentaires**

Recommandation 1 : Les membres de la Commission préconisent de réintégrer dans le projet de loi de finances pour 2025 les autorisations d'engagement et les crédits de paiement annulés en février 2024 pour mener à terme le PFTHD.

Recommandation 2 : la Commission recommande la mise en place d'un accompagnement financier public pour les déploiements et raccordements complexes en zone privative.

Recommandation n°3 : Pour accompagner financièrement les particuliers exposés à des raccordements complexes et couteux dans les phases d'expérimentations de fermeture du cuivre, les membres de la CSNP recommandent une dotation spécifique de 5 millions € en 2025 et de 13 millions € en 2026.

Recommandation n°4 : les membres de la CSNP recommandent d'appuyer le dispositif d'accompagnement financier sur le guichet unique « cohésion numérique des territoires » sous la responsabilité de l'ANCT.

[1] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000049180270
[2] L'Observatoire de la transition numérique des territoires 2024 - InfraNum

- **Un mécanisme de péréquation à revoir**

Recommandation 5 : les membres de la Commission considèrent qu'il est essentiel que l'ARCEP et les pouvoirs publics proposent un mécanisme de péréquation efficace pour que nos concitoyens ne soient pas pénalisés par les ajustements tarifaires liés aux difficultés de raccordement.

- **Un besoin d'engagement accru des opérateurs en zones très dense et sur fonds propres**

Recommandation 6 : Les parlementaires de la CSNP souhaitent rappeler les opérateurs à leurs obligations de déploiements et les engagent à poursuivre les efforts et la cadence de déploiements afin de mener à terme le Plan France Très Haut Débit, prévu fin 2025.

- **Une amélioration nécessaire de la résilience et de la sécurisation des réseaux**

Recommandation 7 : les membres de la CSNP réitèrent leur position et considèrent que l'entretien et la sécurisation du réseau de télécommunications va au-delà du seul enfouissement des lignes et appellent à une évaluation indépendante et la plus exhaustive possible des coûts d'entretiens des réseaux.

Recommandation 8 : Afin de lutter efficacement contre les actes de malveillance, la CSNP souhaite que les sanctions prévues par le Code pénal soient alourdies en créant une circonstance aggravante de « biens essentiels ».

- **Un meilleur accompagnement en vue de la fermeture du réseau cuivre**

Recommandation 9 : En vue d'accompagner la fermeture du réseau cuivre, les membres de la Commission se montrent favorables à ce qu'un opérateur d'infrastructure, lors d'un cas de refus tiers d'être raccordé à la fibre optique, ne déploie pas de réseau optique, tout en autorisant l'opérateur historique à fermer son réseau cuivre.

Recommandation 10 : Toute nouvelle demande de raccordement optique, après un refus tiers (exemple d'une copropriété), sera aux dépens du demandeur.

Recommandation 11 : La Commission invite l'opérateur historique Orange à mettre à jour sa base de données cuivre dans l'objectif d'une meilleure efficience dans les missions de déploiement des opérateurs d'infrastructure.

- **Conclusion**

Recommandation 12 : La CSNP propose qu'une mission de contrôle soit confiée par la Secrétaire d'Etat chargée du numérique à des parlementaires pour évaluer objectivement le bilan opérationnel et financier du Plan France Très Haut Débit.

I – Des coupes budgétaires importantes alors que le PFTHD nécessite des crédits supplémentaires

Lancé en février 2013, le Plan France Très Haut débit vise à proposer un accès à Internet performant à l'ensemble des logements, des entreprises et des administrations en couvrant l'intégralité du territoire en très haut débit d'ici fin 2025. Pour atteindre cet objectif, il mobilise un investissement de plus de 35 milliards d'euros partagé entre les opérateurs privés à hauteur de 22,4 milliards € (toutes zones confondues), les collectivités territoriales à hauteur de 8,84 milliards €, l'Etat à hauteur de 3,5 milliards € et l'Europe à hauteur de 0,55 milliards €[3].

Si les membres de la Commission saluent les investissements massifs des opérateurs privés, des collectivités territoriales et de l'Etat, ils s'inquiètent de la finalisation du Plan France Très Haut Débit, prévu pour 2025, c'est-à-dire dans moins d'un an.

Il reste encore beaucoup à faire et le plus difficile reste à venir. En effet, la complétude des déploiements ne pourra être atteinte si le financement des raccordements complexes, en domaine public et privé, n'est pas rapidement mis en œuvre, en trouvant une source de financement à la hauteur des enjeux.

Les parlementaires de la CSNP ont pris connaissance, avec regret et stupéfaction, de l'annonce de l'annulation de 38 millions € d'autorisations d'engagement et de 117 millions € de crédits de paiement du programme 343, dédié au financement du PFTHD.

A l'approche de l'accélération du décommissionnement du cuivre, faut-il craindre un ralentissement des déploiements en fibre optique ?

Selon les informations communiquées par Mme la Secrétaire d'Etat chargée du numérique, et les représentants de la Direction générale des entreprises et de l'Agence nationale de cohésion des territoires (ANCT), les annulations d'autorisation d'engagement et de crédits de paiement du programme 343 décidées en février 2024 n'auront pas d'incidence sur le déploiement du PFTHD en 2024.

- **L'annulation des crédits de paiement serait rendue possible par un ajustement plus fin des volumes de décaissement en 2024 et 2025**

Pour que cette annulation de crédit de paiement à hauteur de 117 millions € ne ralentisse pas le déploiement du PFTHD, la Secrétaire d'Etat a demandé à l'administration d'affiner au plus près de la réalité le montant des décaissements du programme 343 au titre de l'année 2024.

Cet exercice finalisé en mars 2024 a donc évalué à une centaine de millions d'euros la « réserve de précaution » du programme 343 et confirmerait que l'annulation de crédit de paiement décidé par décret ne ralentirait pas le déploiement du PFTHD en 2024, notamment le déploiement des RIP par les collectivités locales.

Si le versement des financements publics sur les réseaux d'initiative publique ne semble pas remis en cause pour l'année 2024, il existe certaines réserves, voire des incertitudes quant à l'année 2025.

[3] https://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/fs-2023-rapport-thd-janvier.pdf

- **L'annulation des autorisations d'engagement à hauteur de 38 millions € portent principalement sur le déploiement de la fibre à Mayotte**

Sur le montant de 50 millions € d'autorisation d'engagement initialement prévu en 2024 pour financer la nouvelle phase de déploiement de la fibre à Mayotte, Mme Elisabeth Borne, alors Première ministre, a « sanctuarisé »12,9 millions € pour lancer dès 2024 la contractualisation des appels d'offre à Mayotte.

Le gouvernement estime que cette réduction significative de l'autorisation d'engagement tient compte des retards et des difficultés observées sur le terrain pour le déploiement de la fibre mais ne pénalise ni les collectivités territoriales, ni les opérateurs qui souhaiteront répondre à l'appel d'offre.

- **La CSNP portera une vigilance particulière sur les décaissements du programme 343 en 2024**

Les membres de la CSNP prennent acte de ces ajustements et restent vigilants sur le rythme de décaissement du programme en étant très attentifs aux difficultés et aux retards de paiement éventuels que pourraient rencontrer des collectivités locales dans le cadre du déploiement des RIP.

Les membres de la CSNP se réservent le droit de solliciter ponctuellement à Mme la Secrétaire d'Etat en charge du numérique sur l'état des décaissements du programme 343**.**

En tout état de cause, les membres de la Commission préconisent de réintégrer dans le projet de loi de finances pour 2025 les autorisations d'engagement et les crédits de paiement annulés en février 2024 pour mener à terme le PFTHD et mener à terme l'objectif, fixé par le Président de la République, d'une généralisation de la fibre optique à fin 2025.

Recommandation 1 : Les membres de la Commission préconisent de réintégrer dans le projet de loi de finances pour 2025 les autorisations d'engagement et les crédits de paiement annulés en février 2024 pour mener à terme le PFTHD.

- **Des financements publics supplémentaires sont nécessaires pour achever les raccordements complexes**

La majorité des déploiements restants à réaliser sur le territoire national sont principalement des déploiements complexes qui nécessitent des coûts d'investissements considérables de la part des opérateurs d'infrastructures. Pour mener à terme la complétude des réseaux optiques d'ici la fin d'année 2025, les membres de la Commission estiment qu'il est nécessaire que l'Etat accompagne, via des financements publics, les déploiements les plus difficiles à réaliser.

Fin 2021, le gouvernement a annoncé une enveloppe supplémentaire de 150 millions € pour accompagner les collectivités locales dans les RIP mise en œuvre par l'arrêté du 19 avril 2022.

Cette enveloppe supplémentaire, annoncée fin 2021, qui pourra être décaissée durant les dix prochaines années (durée pendant laquelle les territoires, qui auront conventionné avec l'ANCT, pourront adresser des demandes de versement), est toujours en phase d'instruction par les services de l'Agence Nationale de la Cohésion des Territoires, qui étudie les demandes de conventionnement avec les territoires ayant déposé un dossier.

Les membres de la Commission invitent à accélérer la mise en œuvre de cette enveloppe compte tenu des échéances à venir et du « reste à faire ».

En effet, fin 2023, selon le dernier observatoire d'INFRANUM, on dénombrait encore 440 000 raccordements complexes au niveau national. Le surcout moyen estimé pour ces raccordements complexes se situerait entre 2 000 et 3 000 euros, soit des montants très supérieurs au coût moyen d'un raccordement standard.

Comme cela avait été précisé dans l'avis n°2023-08 du 18 octobre 2023, les membres de la commission estiment que les raccordements complexes en zone publique relèvent de l'opérateur d'infrastructure mais qu'une étude, indépendante et exhaustive, doit être réalisée afin de déterminer le coût du « reste à faire » pour mener à terme la complétude des réseaux et de vérifier si des financements supplémentaires de l'Etat sont nécessaires.

S'agissant des raccordements complexes en zone privative, les membres de la CSNP estiment qu'un accompagnement financier doit être mis en place.

Actuellement, les frais de déploiement de la fibre sur la partie privée du terrain sont à la charge du propriétaire. En zone rurale, compte tenu de la surface des terrains privés, ces frais peuvent rapidement être prohibitifs pour les ménages les moins aisés financièrement.

Les membres de la CSNP rappellent que dans le cadre du service universel, tout personne pouvait bénéficier d'un raccordement fixe à un réseau ouvert au public et bénéficier d'un service téléphonique de qualité à un tarif abordable.

Ainsi, afin de garantir un accès au Très Haut Débit à tous, la CSNP propose que les raccordements complexes en zone privative fassent l'objet d'un accompagnement financier public pour les résidences principales.

Les membres de la CSNP proposent de mettre à profit les phases d'expérimentation de la fermeture du réseau cuivre en 2025 et 2026 pour tester et évaluer le dispositif d'aide le plus approprié et affiner les montants de ces aides.

Selon les données communiquées au cours des auditions aux membres de la CSNP, une enveloppe de 5 millions € en 2025 et 13 millions € en 2026 permettrait de tester ce dispositif.

Comme cela avait été proposé dans l'avis n° 2023-08 du 18 octobre 2023, ce dispositif d'accompagnement pourrait s'appuyer sur le guichet « Cohésion numérique des territoires », piloté par l'Agence Nationale de la Cohésion des Territoires.

Recommandation 2 : la Commission recommande la mise en place d'un accompagnement financier public pour les déploiements et raccordements complexes en zone privative.

Recommandation n°3 : Pour accompagner financièrement les particuliers exposés à des raccordements complexes et couteux dans les phases d'expérimentations de fermeture du cuivre, les membres de la CSNP recommandent une dotation spécifique de 5 millions € en 2025 et de 13 millions € en 2026.

Recommandation n°4 : les membres de la CSNP recommandent d'appuyer le dispositif d'accompagnement financier sur le guichet unique « cohésion numérique des territoires » sous la responsabilité de l'ANCT.

II. Un mécanisme de péréquation à renforcer

Les membres de la CSNP rappellent leur soutien à un mécanisme de péréquation efficace qui permettrait de compenser les différences de coûts considérables du déploiement de la fibre selon le territoire : les coûts d'exploitation peuvent être de 2 à 3 fois plus élevés selon que l'on se situe en zone rurale ou en zone urbaine.

Très concrètement, l'accès à l'infrastructure du cuivre existante auprès de l'opérateur historique (loué à un tarif national via le contrat GCBLO) est souvent inutilisable en zone rurale pour passer le câble de fibre. Il est fréquent de constater que le câble téléphonique a été enterré sans gaine ce qui oblige à réaliser du génie civil en domaine public et donc engendre des surcouts financiers très importants.

Par ailleurs, en zone rurale, l'habitat dispersé entraîne souvent des sur-longueurs de raccordements et par conséquent des surcouts non négligeables.

Pour ces raisons, la CSNP avait proposé en juillet 2022[4], la mise en œuvre du fonds de péréquation institué en 2009, pour lutter contre la fracture numérique. En effet, le fonds d'aménagement numérique des territoires (FANT), créé par la loi n° 2009-1572 du 17 décembre 2009 relative à la lutte contre la fracture numérique, devait être alimenté progressivement par le fonds national pour la société numérique (FSN), afin d'amorcer le développement des réseaux en fibre optique dans les zones peu denses.

Or, ce fonds n'a jamais fait l'objet de textes d'applications et n'a jamais été abondé. Aussi, les membres de la Commission rappellent qu'ils sont favorables à une mise en œuvre, dans les meilleurs délais, d'un fonds de péréquation.

A titre d'illustration, pour tenir compte de ces réalités, le 14 février 2024, la société publique locale Nouvelle Aquitaine Très Haut Débit a notifié à l'ARCEP les nouveaux tarifs d'équilibre des raccordements qu'elle souhaite pratiquer. Le 2 avril 2024, l'ARCEP a rendu son avis[5] en considérant que la démarche d'ajustement tarifaire est fondée en droit, en vertu de l'article L.1425-1 du Code général des collectivités territoriales[6], mais qu'il existe un risque que les opérateurs commerciaux répercutent sur les tarifs de détail pratiqués sur le réseau de NATHD la différence de coût par rapport au reste du territoire national induite par ces nouveaux tarifs.

En définitive l'ARCEP se montre prudente sans fermer la porte à une réévaluation plus transparente, objective et proportionnée.

Recommandation 5 : les membres de la Commission considèrent qu'il est essentiel que l'ARCEP et les pouvoirs publics proposent un mécanisme de péréquation efficace pour que nos concitoyens ne soient pas pénalisés par les ajustements tarifaires liés aux difficultés de raccordement.

[4] https://csnp.fr/wp-content/uploads/2022/07/Avis-n%C2%B02022-05-du-27-juillet-2022-sur-le-financement-des-infrastructures-de-telecommunications-2.pdf
[5] https://www.arcep.fr/uploads/tx_gsavis/24-0745.pdf
[6] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000039248089

III – Un besoin d'engagement accru des opérateurs en zones très dense et en fonds propres

En 2013, le Plan France Très Haut Débit a succédé au programme national très haut début lancé en 2010. Depuis, le PFTHD a été poursuivi et amplifié afin d'accélérer le déploiement de la fibre optique sur l'ensemble du territoire national en vue de sa généralisation d'ici la fin 2025.

Plus précisément, le PFTHD a pour objectif de :

- d'ici 2020, garantir à tous un accès au bon haut débit (>8 Mbit/s) ou au très haut débit,
- d'ici 2022, doter tous les territoires d'infrastructures numériques de pointe en donnant accès à tous au très haut débit (>30 Mbit/s),
- d'ici 2025, généraliser la fibre optique sur l'ensemble du territoire[7].

Les forts investissements privés et publics permettent à la France d'être le premier pays européen en nombre de foyers raccordables à la fibre. Cette dynamique se poursuit, même si une légère décélération du rythme de déploiement s'observe, pour porter le nombre de locaux raccordables à la fibre optique à hauteur de 86%. Cela représente 38 millions de locaux raccordables.

Le ralentissement du déploiement de la fibre peut s'expliquer par l'approche de la fin du Plan. A titre d'illustration, 0,99 millions de locaux ont été rendus raccordables à la fibre au T4 2023, ce qui représente une baisse de 25% par rapport au T4 2022[8].

En revanche, l'adoption de la fibre optique par nos concitoyens ne cesse de progresser pour atteindre 24,2 millions d'abonnements en THD, dont 21,4 millions d'abonnements en fibre optique.

Toutefois, même si la progression des déploiements continue dans l'ensemble des zones de déploiements, il faut noter une baisse comparée aux années précédentes.

➔ En effet, **en zone d'initiative privée**, sur le dernier trimestre 2023 :

- Environ 130 000 locaux ont été rendus éligibles en zone AMII (-19% par rapport au T4 2022)
- 50 000 dans les zones très denses (-40% par rapport au T4 2022)

Soit un total de 22,6 millions de locaux éligibles au FttH en zones d'initiative privée, soit 92% des locaux.

➔ Également, **en zone d'appel à manifestation d'engagements locaux** (AMEL), sur le dernier trimestre 2023 :

- 118 000 locaux ont été rendus raccordables dans les territoires concernés par des AMEL (-22% par rapport au T4 2022) et 29 000 locaux dans ceux concernés par des déploiements en fonds propres des opérateurs privés (-37% par rapport au T4 2022)

Soit un total de 1,7 million de locaux raccordables au FttH dans ces territoires sur les 2,3 millions de locaux, soit 74% des locaux.

➔ Enfin, **en zone d'initiative publique**, sur le dernier trimestre 2023 :

[7] https://www.economie.gouv.fr/plan-de-relance/mesures/plan-france-tres-haut-debit-fibre-optique
[8] Source Agence nationale de la cohésion des territoires

- 0,66 million de locaux ont été rendus raccordables au FttH en zone d'initiative publique (-25% par rapport au T4 2022)

Soit un total de 13,7 millions de locaux raccordables au FttH sur les 17,1 millions de locaux que compte la zone d'initiative publique, soit 80% des locaux.

Aussi, les membres de la Commission observent que le Plan France Très Haut Débit a progressé ces dernières années mais constatent néanmoins qu'une baisse des déploiements est à déplorer dans chacune des zones précitées, et particulièrement dans les zones très denses et les zones en fonds propres des opérateurs.

Recommandation 6 : Les parlementaires de la CSNP souhaitent rappeler les opérateurs à leurs obligations de déploiements et les engagent à poursuivre les efforts et la cadence de déploiements afin de mener à terme le Plan France Très Haut Débit, prévu fin 2025.

IV – Une amélioration nécessaire de la résilience et de la sécurisation des réseaux

La résilience des réseaux ne peut être dissociée de la notion de qualité des réseaux et des infrastructures. Pour rappel, en septembre 2022, les opérateurs se sont engagés, devant le Ministre chargé des communications électroniques et la Présidente de l'ARCEP, notamment, à reprendre les infrastructures dégradées en mettant en place des plans de reprise, à renforcer la formation des intervenants, les contrôles « à chaud » et à mieux contrôler la qualité des raccordements.

Les membres de la Commission prennent acte des engagements pris par les opérateurs et constatent que de nombreuses actions ont été mises en place comme l'auto-certification des sous-traitants, les plans nationaux de reprise des réseaux accidentogènes et dégradés, mais également les plans spécifiques de reprise comme en Essonne[9]. Les quatre opérateurs commerciaux travaillent de concert avec Altitude Infra pour la mise en place d'une opération « coup de poing » spécifique à l'Essonne afin de répondre au taux élevé d'incidents dans la zone et améliorer rapidement l'expérience client.

Dans son observatoire de février 2024[10], l'ARCEP note une situation contrastée en fonction des réseaux considérés mais que globalement, les taux de pannes sont plutôt stables par rapport au dernier observatoire. Concernant les taux d'échec au raccordement, l'ARCEP observe une tendance à l'amélioration des taux d'échecs au raccordement sur certains territoires.

Les membres de la Commission soulignent cependant les actions menées par les opérateurs d'infrastructures et les opérateurs commerciaux sur les territoires et les incitent à persévérer dans cette voie d'amélioration de la qualité des réseaux.

[9] https://actu.fr/economie/cinq-operateurs-s-unissent-pour-ameliorer-la-qualite-du-reseau-de-fibre-optique-en-essonne_60809145.html
[10] https://www.arcep.fr/cartes-et-donnees/nos-publications-chiffrees/qualite-des-reseaux-ftth/derniers-chiffres.html

Toutefois, il apparait légitime d'encourager l'ARCEP à contrôler davantage les engagements pris par les opérateurs et d'inciter l'autorité de régulation à user, en tant que de besoin, de son pouvoir de sanction.

Les membres de la CSNP rappellent, par ailleurs qu'ils soutiennent l'article 4 de la proposition de loi visant à assurer la qualité et la pérennité des réseaux de communications électroniques à très haut débit en fibre optique présentée par le sénateur Patrick CHAIZE[11], et adoptée au Sénat le 2 mai 2023.

En outre, dans leurs avis du 27 juillet 2022[12] et du 18 octobre 2023[13], les membres de la CSNP avaient déjà alerté sur les coûts d'entretien et de sécurisation des réseaux, et des infrastructures télécoms qui devaient être anticipés rapidement.

Lorsque le PFTHD a été imaginé, il y a plusieurs années, les sujets de la résilience et de la durabilité des réseaux n'ont pas été inclus dans les réflexions. Or, les récentes tempêtes et les aléas climatiques rappellent à quel point les réseaux peuvent être fragiles.

Ces derniers montrent déjà quelques signes de vulnérabilité tandis que la complétude des réseaux n'est pas encore achevée.

Or, des réseaux durables et pérennes ne peuvent se concevoir s'ils ne sont pas résilients et sécurisés. Ainsi, avant même que la complétude des réseaux soit achevée, il convient de s'interroger sur l'évaluation et le financement des coûts d'entretien et de sécurisation.

Recommandation 7 : les membres de la CSNP réitèrent leur position et considèrent que l'entretien et la sécurisation du réseau de télécommunications va au-delà du seul enfouissement des lignes et appellent à une évaluation indépendante et la plus exhaustive possible des coûts d'entretiens des réseaux.

De plus, la pérennité des réseaux passera également par l'aggravation des sanctions pénales contre les actes de sabotage et de dégradation que subissent nos infrastructures numériques. Selon la Fédération française des télécoms, au cours des mois de novembre 2023 à février 2024, 550 actes de vandalisme ont été recensés sur les réseaux fixes des opérateurs avec en particulier des atteintes sur les armoires de rues.

Le Code pénal prévoit deux ans d'emprisonnement et 30.000 euros d'amende pour toute dégradation ou détérioration d'un bien[14]. Il apparait que cette réponse pénale n'est plus adaptée à la réalité des dommages et à leur impact sur la vie du pays.

En effet, au regard des risques potentiels sur la vie humaine, la Commission propose d'engager une réflexion avec les Ministères de l'Intérieur et de la Justice pour alourdir les sanctions en cas de dégradations volontaires des armoires de rue ou des antennes-relais. En effet, ces actes de malveillance peuvent avoir des conséquences dramatiques pour les personnes sous assistance, les

[11] https://www.assemblee-nationale.fr/dyn/16/textes/l16b1177_proposition-loi#D_TITRE_V_10

[12] https://csnp.fr/wp-content/uploads/2022/07/Avis-n%C2%B02022-05-du-27-juillet-2022-sur-le-financement-des-infrastructures-de-telecommunications-2.pdf

[13] https://csnp.fr/wp-content/uploads/2023/10/Avis-n%C2%B02023-08-du-18-octobre-2023-sur-renforcer-la-couverture-et-la-qualite-des-reseaux-de-telecommunications-1.pdf

[14] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000047053456

personnes devant appeler les services de secours, mais également ces dégradations et ces coupures de service ont un impact significatif sur la vie quotidienne des particuliers et des professionnels.

Recommandation 8 : Afin de lutter efficacement contre les actes de malveillance, la CSNP souhaite que les sanctions prévues par le Code pénal soient alourdies en créant une circonstance aggravante de « biens essentiels ».

V – Un meilleur accompagnement en vue de la fermeture du réseau cuivre

La fibre optique est une avancée historique en France et il convient, avant toute chose, de mener le déploiement à son terme avant d'imaginer la fermeture définitive du réseau cuivre.

Orange a engagé la fermeture de son réseau historique en cuivre pour un achèvement prévu en 2030 selon deux étapes :

- Une fermeture commerciale
- Une fermeture technique

Plusieurs expérimentations de fermeture du réseau cuivre ont déjà été menées en France et se sont déroulées dans de bonnes conditions.

Les membres de la Commission ont rappelé à plusieurs reprises qu'il est essentiel que le décommissionnement du cuivre n'ait pas lieu dans les territoires où la fibre n'est pas encore présente. Or, il est constaté que dans certains cas le déploiement de la fibre optique ne peut avoir lieu en raison de « cause tiers » : refus de copropriété, élagage non réalisé.

Dans ces conditions, les parlementaires de la Commission se montrent favorables à ce qu'un opérateur d'infrastructure lors d'un cas de refus tiers d'être raccordé à la fibre optique, de ne pas déployer de réseau optique et de permettre à l'opérateur historique la fermeture du réseau cuivre.

Recommandation 9 : En vue d'accompagner la fermeture du réseau cuivre, les membres de la Commission se montrent favorables à ce qu'un opérateur d'infrastructure, lors d'un cas de refus tiers d'être raccordé à la fibre optique, ne déploie pas de réseau optique, tout en autorisant l'opérateur historique à fermer son réseau cuivre.

Recommandation 10 : Toute nouvelle demande de raccordement optique, après un refus tiers (exemple d'une copropriété), sera aux dépens du demandeur.

De plus, dans le cadre du processus de fermeture du réseau cuivre, la fermeture d'une zone est conditionnée à la présence d'un réseau FTTH intégralement déployé pour couvrir l'ensemble des utilisateurs et des sites de la zone concernée. Aussi, pour s'assurer du respect de cette condition, l'opérateur historique, Orange, doit transmettre aux opérateurs d'infrastructure un « recollement » entre la base de données des adresses raccordées au réseau cuivre et les données d'éligibilité au FttH.

Or, il est constaté par certains opérateurs d'infrastructure que les données d'adresses du réseau cuivre transmises par Orange sont gravement lacunaires.

La base d'Orange contient, de plus, un grand nombre d'adresses erronées ou incohérentes. Les opérateurs d'infrastructure sont ainsi contraints de réaliser des vérifications immeuble par immeuble pour identifier la présence d'une ligne cuivre présente à l'adresse et l'éligibilité de l'adresse aux réseaux FttH. Cela représente, en plus d'une masse de travail et d'un coût considérables, des retards non négligeables sur la complétude des réseaux et par voie de conséquence sur la fermeture du réseau cuivre.

Ainsi, il parait nécessaire qu'Orange fournisse des données plus précises concernant les locaux raccordés au réseau DSL pour sécuriser le processus de fermeture du cuivre sans induire pour les opérateurs d'infrastructure charge opérationnelle trop lourde.

Recommandation 11 : La Commission invite l'opérateur historique Orange à mettre à jour sa base de données cuivre dans l'objectif d'une meilleure efficience dans les missions de déploiement des opérateurs d'infrastructure.

VI – Conclusion

Les membres de la commission reconnaissent que le Plan France Très Haut Débit est une réussite, qui a permis de placer notre pays en position très favorable au niveau européen dans le déploiement des réseaux en fibre optique avec près de 84% des foyers qui sont raccordables. Toutefois, les membres reconnaissent qu'il reste encore beaucoup à faire pour apporter le Très Haut Débit à tous les français.

Ainsi, la CSNP demande qu'une mission de contrôle soit confiée par la Secrétaire d'Etat chargée du numérique à des parlementaires afin d'évaluer objectivement le bilan opérationnel et financier du Plan France Très Haut Débit.

Cette mission de contrôle aura pour objectif d'examiner les engagements pris par l'Etat et les opérateurs privés sur le déploiement, l'avancement et le financement du Plan ainsi que la fermeture du réseau cuivre.

Recommandation 12 : La CSNP propose qu'une mission de contrôle soit confiée par la Secrétaire d'Etat chargée du numérique à des parlementaires pour évaluer objectivement le bilan opérationnel et financier du Plan France Très Haut Débit.

Personnes auditionnées

Mme Marina Ferrari, Secrétaire d'Etat chargée du Numérique

Agence nationale de la cohésion des territoires –

- M. Zacharia Alahyane, Directeur des missions FTHD et France mobile

Altitude

- M. David Elfassy, Vice-Président d'Altitude
- M. Martial Houlle, Secrétaire général altitude
- Mme Ilham Djehaich, Directrice générale d'altitude Infra
- M. Bruno Sablière, Directeur des affaires publiques

ARCEP

- Mme Laure de la Raudière, Présidente

Direction générale des entreprises

- M. Antoine Jourdan, Sous-directeur des communications électroniques et des postes

Fédération française des télécoms

- Mme Marie Lhermelin, Secrétaire générale adjointe d'Altice
- M. Hervé de Tournadre, Directeur des affaires réglementaires de Bouygues Telecom
- M. Romain Bonenfant, Directeur Général de la FFT
- M. Olivier Riffard, Directeur Général adjoint de la FFT

Fédération nationale des collectivités concédantes et régies

- M. Patrick Chaize, Sénateur
- M. Jean-Luc Sallaberry, Chef du département numérique

Infranum

- M. Philippe Le Grand, Président

Nouvelle aquitaine très haut débit

- M. Pascal Goudy, Directeur général

Orange

- M. Laurentino Lavezzi, Directeur des affaires publiques

COMMISSION SUPERIEURE DU NUMERIQUE ET DES POSTES

AVIS N°2024-05 DU 4 SEPTEMBRE 2024
SUR LES ENJEUX POLITIQUES ET ECONOMIQUES DU SCHEMA EUROPEEN DE CERTIFICATION DE SECURITE DES SERVICES CLOUD

Les membres de la Commission supérieure du numérique et des postes (CSNP) souhaitent attirer l'attention des pouvoirs publics et celle des membres de la représentation nationale sur les enjeux politiques et économiques du schéma européen de certification de sécurité des services cloud (EUCS) et formuler des recommandations pour renforcer la protection des données sensibles, à caractère personnel ou non, de nos concitoyens, de nos entreprises et de nos administrations publiques.

En effet, alors que la Commission nationale de l'information et des libertés (CNIL) vient de s'exprimer sur les lacunes et risques du projet de certification européenne EUCS[1] et qu'un nouvel exécutif se met en place au niveau européen, il est essentiel que ces enjeux de souveraineté soient portés au plus haut niveau.

Il est également important de rappeler que la sécurité numérique repose sur trois principes :

- intégrité des systèmes d'information, des données et des traitements associés ;
- disponibilité des systèmes d'information et des données ;
- confidentialité des données et des traitements associés.

La confidentialité des données et des traitements associés consiste à s'affranchir de deux types de menaces majeures, mais bien distinctes :

- les accès illégitimes et illégaux, de nature criminelle, qu'ils soient le fait d'organisations criminelles ou d'agences étatiques ;
- les accès par des agences de renseignement qui agissent dans un cadre légal mais secret, et bien entendu illégitimes pour les organismes qui en sont les victimes.

De nombreux opposants à toute forme de protection contre les accès légaux aux données détenus par les opérateurs de services cloud, entretiennent à dessein une confusion sur la confidentialité entre les enjeux de cybersécurité contre les accès illégitimes et illégaux aux données sensibles et stratégiques des européens et les dispositions de protection des données

[1] Cloud : les risques d'une certification européenne permettant l'accès des autorités étrangères aux données sensibles | CNIL

sensibles et stratégiques contre ces accès légaux. Ces dispositions sont en effet mises en œuvre par les agences de renseignement pour tout type d'activité, notamment pour mener des activités d'intelligence économique au profit de leurs entreprises et au détriment des entreprises des concurrents économiques.

I. Genèse du schéma européen de certification des services cloud (EUCS)

Face à l'expansion rapide des services cloud et à leur adoption croissante par les entreprises et les administrations publiques, l'Union Européenne a jugé nécessaire d'instaurer un cadre réglementaire pour assurer la sécurité et la conformité de ces services sur le marché européen. Cette initiative a conduit à la création du Schéma Européen de Certification des Services Cloud (EUCS). L'objectif de ce schéma est de renforcer la confiance des utilisateurs dans les services cloud en garantissant un haut niveau de sécurité, de protection des données, et de conformité aux lois européennes.

Le projet EUCS s'inscrit dans la stratégie plus large de l'Union Européenne visant à construire un marché numérique résilient et sécurisé. L'adoption du **Règlement 2019/881**, dénommé **Cybersecurity Act**, a posé les bases d'un cadre commun pour la certification en matière de cybersécurité. L'Agence de l'Union Européenne pour la Cybersécurité (ENISA) a été mandatée pour développer et gérer différents schémas de certification, parmi lesquels l'EUCS occupe une place centrale. L'EUCS a pour ambition de fournir un cadre juridique homogène au sein de l'Union, non seulement pour protéger les données sensibles, qu'elles soient personnelles ou non, mais aussi pour renforcer la souveraineté numérique de l'Europe face à la concurrence mondiale.

II. L'arrêt de la CJUE invalidant le Privacy Shield et ses implications

Le 16 juillet 2020, la Cour de justice de l'Union européenne (CJUE)[2] a rendu un arrêt crucial qui a invalidé le Privacy Shield, un accord régissant le transfert des données à caractère personnel entre l'Union Européenne et les États-Unis. Cet arrêt a mis en lumière les pratiques des agences de renseignement américaines, qui accèdent aux données personnelles des citoyens européens via des fournisseurs de services cloud américains. Ces données, lorsqu'elles sont hébergées par des prestataires américains, sont soumises à des législations, notamment **la section 702 du Foreign Intelligence Surveillance Act (FISA)**, qui permettent aux États-Unis de collecter des données, de façon massive, à priori, et sans mandat judiciaire, sans offrir les garanties de proportionnalité exigées par le droit de l'Union Européenne. Le considérant 184 de cet arrêt souligne que ces législations ne respectent pas les garanties minimales requises par l'Union, car les programmes de surveillance qui en découlent ne sont pas limités à ce qui est strictement nécessaire.

[2] Arrêt C-311/18 du 16 juillet 2020 Data Protection Commissioner contre Facebook Ireland Ltd/ Maximillian Schrems EUR-Lex - 62018CJ0311 - EN - EUR-Lex (europa.eu)

En invalidant le Privacy Shield, la CJUE a principalement mis en avant la protection des données à caractère personnel. Toutefois, la section 702 de la FISA ne se limite pas aux données personnelles et s'étend également aux données non personnelles, et permet l'accès à tout type de données sensibles ou stratégiques. Cela exacerbe les préoccupations concernant la sécurité des informations économiques européennes.

Le Data Privacy Framework (DPF), adopté en juillet 2023 pour remplacer le Privacy Shield, ne couvre l'adéquation des transferts vers les États-Unis que pour les données à caractère personnel. En revanche, la protection des données non personnelles sensibles ou stratégiques vis-à-vis des activités des agences de renseignement fait toujours face à un vide juridique au sein de l'Union européenne.

Ce cadre lacunaire souligne la nécessité d'une distinction claire entre les besoins légitimes des États-Unis en matière de lutte contre le terrorisme et le crime international, et les risques que peuvent engendrer les activités abusives d'intelligence économique à l'encontre des entreprises européennes visant à avantager leur économie. Par ailleurs, un risque majeur persiste, constitué par la différence d'interprétation des principes de proportionnalité et de nécessité entre l'Union européenne et les États-Unis. Ces principes sont au cœur des garanties apportées par le DPF (Data Privacy Framework), mais leur application dépend largement du contexte juridique et culturel de chaque juridiction. En Europe, la protection des données personnelles est un droit fondamental strictement encadré, et toute limitation de ce droit doit être nécessaire, proportionnée et justifiée de manière rigoureuse.

Les autorités européennes, y compris la CJUE, interprètent ces principes dans un cadre où les droits individuels priment, même face à des enjeux de sécurité. Aux États-Unis, ces mêmes principes sont interprétés dans un contexte où la sécurité nationale occupe une place prépondérante. Le cadre juridique américain, notamment sous la section 702 du Foreign Intelligence Surveillance Act (FISA), autorise une surveillance extensive des personnes (physiques ou morales) étrangères pour des motifs de sécurité nationale, ce qui peut inclure la collecte massive de données.

Malgré les réformes introduites par le décret présidentiel 14086, adopté par le Président Biden pour permettre la mise en œuvre du DPF, et qui visent à renforcer les protections dont bénéficient les données à caractère personnel des européens, le concept de « nécessité » aux États-Unis peut inclure des actions que les autorités européennes pourraient juger excessives. Cette divergence d'interprétation pourrait devenir une source de tensions à l'avenir.

Si les autorités européennes estiment que les principes de proportionnalité et de nécessité ne sont pas appliqués selon les standards du RGPD, elles pourraient contester la validité du Data Privacy Framework. Un tel désaccord pourrait entraîner une nouvelle invalidation de l'accord, comme ce fut le cas pour le Privacy Shield. Ce risque met en lumière les défis inhérents à l'harmonisation des normes de protection des données entre deux systèmes juridiques qui, bien que partenaires, sont fondamentalement différents.

III. Le cadre de labellisation de Gaia-X

En novembre 2021, l'association Gaia-X a adopté un cadre de certification pour les services cloud, organisé autour de trois niveaux de labellisation. Le niveau le plus élevé de ce cadre inclut des exigences en matière d'immunité contre les législations non européennes à portée extraterritoriale. Ce consensus parmi les membres européens de Gaia-X reflète une volonté claire, tant des bénéficiaires de services cloud labellisés que des fournisseurs de ces services, de protéger les espaces de partage des données les plus sensibles contre les ingérences légales mais potentiellement abusives des législations étrangères.

IV. Le référentiel SecNumCloud et la loi SREN

Le référentiel SecNumCloud, élaboré par l'ANSSI en 2016, est un cadre de sécurité destiné à qualifier les prestataires de services cloud. Il s'appuie sur la norme ISO/IEC 27001 et répond aux exigences européennes, notamment en matière de protection des données, tout en garantissant un haut niveau de sécurité technique, opérationnelle et juridique. La version 3.2 du référentiel, publiée en 2022, renforce les protections contre les lois extra-européennes, conformément à l'arrêt « Schrems II » de la Cour de justice de l'Union européenne. Elle est par ailleurs cohérente avec les exigences du niveau High+ de la précédente version de l'EUCS.

Ce référentiel vise à créer un environnement cloud sécurisé, à encourager le développement d'acteurs nationaux des services cloud notamment pour répondre aux besoins de l'État, et à assurer une confiance durable entre les prestataires qualifiés et leurs utilisateurs, en particulier pour les administrations publiques qui gèrent des données sensibles. La certification SecNumCloud, matérialisée par le Visa de sécurité ANSSI, est un gage de fiabilité et de conformité aux normes de sécurité les plus élevées, offrant ainsi une protection accrue contre les cyberattaques et les risques juridiques.

L'incertitude juridique demeure, mais il est fort probable que l'adoption de l'EUCS, qu'il intègre ou non le niveau High+, rendrait caduque le référentiel SecNumCloud. Dans l'hypothèse de l'adoption par la Commission européenne d'un EUCS qui n'intègrerait pas des exigences d'immunité aux législations non européennes à portée extraterritoriale, et qui se substituerait en Europe à tous les autres référentiels nationaux de certification de services cloud, l'État français se trouverait démuni pour mettre en œuvre sa stratégie dite « cloud au centre ». Par ailleurs, dans une telle hypothèse, la mise en œuvre des articles 31 et 32, relatifs à la protection des données stratégiques et sensibles sur le marché de l'informatique en nuage, de la loi visant à sécuriser et à réguler l'espace numérique, dite loi SREN, du 21 mai 2024 serait difficile. Ces articles font, en effet, sans le nommer mais de manière transparente, référence au référentiel SecNumCloud.

V. Le niveau High+ de l'EUCS

C'est dans ce contexte, que la première version de l'EUCS a intégré dans son niveau de certification le plus élevé, également appelé **High+, des critères techniques et juridiques**

d'immunité des services cloud aux législations non européennes à portée extraterritoriale. Si de nombreux Etats disposent de ce genre de disposition légale, le niveau High+ vise en premier lieu les Etats dont dépendent les principaux opérateurs mondiaux de services cloud. La Chine dispose, avec sa loi du 28 juin 2017 sur le renseignement national, d'une disposition législative qui oblige les opérateurs cloud chinois comme Alibaba, Tencent ou Huawei, de mettre à la disposition des autorités chinoises les données dont elles peuvent disposer sur leurs infrastructures sans en référer à leurs clients. Le mécanisme est assez similaire à celui dont les Etats-Unis disposent avec la section 702 du FISA, mis en exergue par la CJUE, et auquel sont bien entendu soumis les principaux opérateurs de service cloud américain dont les trois principaux qui préemptent en Europe plus de 70% du marché des services cloud.

Ce niveau High+ a été conçu suivant des principes analogues à ceux du référentiel français SecNumCloud, afin d'offrir une protection proportionnée aux entreprises européennes traitant des données dans le cloud et risquant une appropriation illégitime via des voies légales non européennes à portée extraterritoriale. Cette protection, bien que non obligatoire, est jugée essentielle pour ces entreprises.

Il existe au sein de l'écosystème numérique européen, notamment au sein des organismes publics et privés qui expriment le besoin de services cloud immunisés contre les législations non européennes à portée extraterritoriale, un large consensus pour considérer que le niveau High+ est la clé de voûte des dispositifs européens de développement d'une industrie européenne autonome des services cloud. Sans ce dispositif, il sera extrêmement compliqué de sortir de cette situation de dépendance croissante vis-à-vis des opérateurs américains, qui pourrait à terme porter des risques insupportables de nature économique, géopolitique et juridique.

VI. Les critiques américaines

Cette initiative européenne a suscité de vives réactions aux États-Unis. Le 25 mai 2023, plusieurs associations professionnelles américaines, dont la Computer & Communications Industry Association (CCIA) et la Business Software Alliance (BSA), ont adressé une lettre à des membres clés de l'administration Biden, dénonçant le niveau High+ de l'EUCS comme une menace pour la sécurité nationale des États-Unis. Elles écrivent notamment dans ce courrier : « *EUCS is part of a broader concerted effort by Europe to enact a "digital sovereignty" agenda that seeks to disadvantage U.S. firms for the benefit of local alternatives,* ***potentially threatening U.S. economic and national security interests****.* » Selon eux, l'EUCS s'inscrit dans une démarche de «souveraineté numérique » européenne visant à désavantager les entreprises américaines, compromettant ainsi les intérêts économiques et sécuritaires des États-Unis.

En septembre 2023, le secrétaire d'État américain Antony Blinken a envoyé une note diplomatique à la présidente de la Commission européenne, Ursula von der Leyen, avertissant que l'inclusion de ces dispositions dans le schéma final pourrait nuire aux relations bilatérales entre les États-Unis et l'Union Européenne, tant sur le plan économique que sécuritaire : « *Including these provisions in the final scheme* ***could also negatively impact the U.S.-EU bilateral economic and security relationship****.* »

VII. Réactions européennes

En réaction, la Commission européenne a demandé à l'ENISA de revoir le schéma EUCS, ce qui a conduit à une proposition début 2024 d'un schéma expurgé du niveau High+, c'est-à-dire de toute disposition garantissant l'immunité contre les législations non européennes comme la section 702 du FISA. En avril 2024, le Congrès américain a renouvelé pour deux ans la section 702 du FISA, en élargissant par ailleurs son champ d'application.

Le 30 octobre 2023, lors d'un sommet ministériel entre l'Allemagne, la France et l'Italie, consacré à la coopération industrielle dans plusieurs secteurs stratégiques pour l'Union européenne, ces trois pays ont réaffirmé leur intention de renforcer la protection des données sensibles en Europe, en particulier contre les législations extraterritoriales. Cette volonté de protection a toutefois été remise en question, notamment par l'Allemagne, dans le cadre des discussions sur l'EUCS.

Pour de nombreuses entreprises européennes, le niveau de certification High+ de l'EUCS est crucial pour protéger de manière non contraignante leurs données non personnelles sensibles ou stratégiques contre les accès légaux mais indésirables des services de renseignement, notamment américains. Ces entreprises ne souhaitent pas une éviction des fournisseurs de services cloud américains du marché européen, mais affirment qu'une partie substantielle de leurs besoins ne peut être satisfaite par ces opérateurs. Elles insistent sur la nécessité de disposer en Europe de services cloud capables de répondre à leurs exigences de protection de leurs données sensibles et stratégiques, mis en œuvre de manière homogène sur l'ensemble du territoire de l'Union, avec une robustesse garantie par un schéma de certification européen à valeur légale.

Au sein de l'Union européenne, les opposants au niveau High+ de l'EUCS se retrouvent schématiquement dans deux grandes catégories :

- les Etats membres de l'Union Européenne sensibles aux menaces de restriction des garanties de sécurité que les Etats-Unis leur apporte ;
- les secteurs d'activité fortement dépendant du marché des Etats-Unis et sensibles aux menaces de restriction d'accès à ce marché en cas d'adoption du niveau High+ dans l'EUCS.

VIII. Conformité du niveau High+ aux accords de l'Organisation Mondiale du Commerce (OMC)

Une critique récurrente du niveau High+ de l'EUCS consiste à mettre en doute sa conformité aux engagements de l'Union européenne pris dans le cadre des accords de l'OMC, au motif qu'il provoquerait l'éviction des opérateurs américains de certains marchés. Dans un article publié le 1er septembre 2023 sur le site du *Center for Strategic and International Studies* (CSIS), organisme américain de recherche qui se consacre à la promotion d'idées pour relever les grands défis du monde, Meredith Broadbent développe une attaque en règle contre le niveau

High+ de l'EUCS, notamment en affirmant l'incompatibilité du niveau High+ avec les accords de l'OMC.

Cet argument ne tient pas car ce n'est pas le référentiel en lui-même qui pourrait être incompatible avec les termes des accords l'OMC, mais l'usage qui en sera éventuellement fait par les États membres, notamment dans le cadre des marchés publics pour garantir des conditions de concurrence ouvertes, équitables et transparentes, en réservant l'usage du niveau High+ aux cas dérogatoires explicitement prévus dans le traité.

D'ailleurs, l'Union européenne n'a pas prononcé de non-conformité du référentiel SecNumCloud aux accords de l'OMC. En revanche, la première circulaire du Premier Ministre sur la mise en œuvre de la stratégie « cloud au centre », publiée le 5 juillet 2021, a été critiquée par Bruxelles en raison de sa non-conformité aux accords de l'OMC. Elle a dû être actualisée en mai 2023, notamment pour tenir compte des observations de la Commission européenne.

IX. Position de la CNIL

Dans le contexte créé par les doutes sur la robustesse du DPF au regard de la protection des données personnelles les plus sensibles, la Commission Nationale de l'Informatique et des Libertés (CNIL), dans une position publiée le 19 juillet 2024, a critiqué les lacunes du projet actuel de certification EUCS, en particulier en ce qui concerne la protection des données personnelles sensibles contre les accès non autorisés par des autorités étrangères. La CNIL a souligné que l'absence de critères « d'immunité » contre les législations non européennes affaiblit la compétitivité de l'offre cloud européenne et compromet la capacité des acteurs publics et privés à externaliser leurs projets les plus critiques de manière sécurisée. Elle a appelé à réintroduire des dispositions inspirées du cadre SecNumCloud au sein de l'EUCS, permettant aux prestataires européens de cloud de démontrer leur capacité à protéger les données contre toute ingérence étrangère.

X. Les conclusions et recommandations de la CSNP

La Commission supérieure du Numérique et des Postes :

- considère que l'adoption du schéma de certification EUCS, incluant des dispositions garantissant l'immunité contre les législations non européennes, est un enjeu essentiel d'autonomie technologique pour l'Union européenne, la condition de l'émergence d'une industrie européenne des services cloud, et une impérieuse nécessité pour protéger les données sensibles et stratégiques, à caractère personnel ou non, des organismes publics et privés qui ont besoin de préserver leur patrimoine informationnel contre les ingérences étrangères ;

- demande au Gouvernement de présenter à la Représentation nationale l'état des négociations et de lui préciser sa position et son évolution au cours de celle-ci ;

– invite le Gouvernement à solliciter la Commission européenne pour que celle-ci confirme le caractère volontaire d'usage des différents niveaux de certification de l'EUCS par les bénéficiaires des services cloud certifiés ;

– suggère au Gouvernement de demander aux différents États membres de l'UE, opposés au niveau High+, de s'expliquer sur les raisons pour lesquelles ils entendent en priver les entreprises et les administrations publiques qui en expriment le besoin en Europe ou dans leur propre pays ;

– demande au Gouvernement de faire le nécessaire auprès de la Commission européenne pour qu'elle sursoit à toute décision d'adoption de la version actuelle du schéma de certification afin qu'un travail approfondi de prise en compte de tous les besoins puisse être mené avec les différentes parties prenantes, notamment les organisations professionnelles européennes représentatives des potentiels futurs bénéficiaires, publics et privés, de l'EUCS ;

– demande au Gouvernement de mener une analyse approfondie des conséquences géopolitiques à moyen terme des renoncements de l'Union européenne à maintenir dans l'EUCS un niveau de type High+ ;

– demande au Gouvernement de mener une analyse économique sur les conséquences des dépendances européennes à l'industrie américaine des services cloud et sur son impact sur la compétitivité de l'économie européenne ;

– demande au Gouvernement de lui présenter une analyse des risques que l'adoption du niveau High+ dans l'EUCS ferait peser sur l'Union européenne au titre des engagements de celle-ci dans le cadre des accords de l'OMC.

COMMISSION SUPERIEURE DU NUMERIQUE ET DES POSTES

AVIS N°2024-05 DU 26 JUILLET 2024

SUR LE PROJET DE DECRET RELATIF A LA METHODE D'EVALUATION UTILISEE POUR LE CALCUL DU COUT NET DE LA MISSION DE SERVICE UNIVERSEL POSTAL.

Vu la directive 97/67/CE du Parlement Européen et du Conseil du 15 décembre 1997 modifiée concernant les règles communes pour le développement du marché intérieur des services postaux de la Communauté et l'amélioration de la qualité du service

Vu la décision de la Commission européenne du 7 décembre 2023, notifiée sous le numéro C (2023)8708/3161649 autorisant le versement d'une aide d'Etat à La Poste en contrepartie du service universel postal au titre des années 2021-2025 ; Vu le code des postes et des communications électroniques, notamment ses articles L. 2- 2, L. 5-2, R. 1-1-27 à R. 1-1-29 ;

Vu le code des postes et des communications électroniques, notamment ses articles L. 2-2 et L. 5-2

Vu la loi n° 90-568 du 2 juillet 1990 relative à l'organisation du service public de La Poste et à France Télécom

Vu le contrat d'entreprise conclu entre l'Etat et La Poste du 26 juin 2023

Vu l'avis n°2024-02 du 15 avril 2024 de la CSNP sur le projet de décret relatif à la méthode d'évaluation utilisée pour le calcul du coût net de la mission de service universel postal

Après avoir été saisie les 4 mars 2024, la Commission supérieure du numérique et des postes a été une nouvelle fois saisie le 31 mai 2024 puis le 19 juillet 2024 par la Direction générale des entreprises en vue de rendre un avis sur le projet de décret relatif à la méthode d'évaluation du coût net lié aux obligations de service universel postal, pris en application de l'article L. 2-2 du Code des postes et des communications électroniques (CPCE), et portant diverses adaptations de la partie réglementaire du même code.

En effet, cette nouvelle saisine fait suite à une demande du Conseil d'Etat demandant que soit précisée dans le projet de décret la notion de « charge financière inéquitable » visée à l'article R. 1-1-29 du code des postes et des communications électroniques (partie réglementaire : Décrets en Conseil d'Etat).

1 Eléments de contexte sur la compensation du service universel postal

Conformément aux articles 2 et 6 de la loi du 2 juillet 1990, l'Etat a confié à La Poste quatre missions de service public :

- Le service universel postal,

- La contribution de La Poste à l'aménagement et au développement du territoire,

- La mission d'accessibilité bancaire,

- Le transport et la distribution de la presse.

Ces missions sont par ailleurs encadrées par le contrat d'entreprise signé entre l'Etat et La Poste le 26 juin 2023 pour la période 2023-2027.

S'agissant plus particulièrement de la mission du service universel postal, les membres de la Commission supérieure rappellent que cette mission est devenue déficitaire pour la première fois en 2018 à hauteur de 365 millions d'euros.

Ce déficit s'explique par la baisse tendancielle du volume du courrier (6 milliards d'objets distribués en 2023 contre 9 milliards d'objets distribués en 2019). Le déclin de l'activité courrier a fait perdre au groupe La Poste plus de 6 milliards d'euros de recettes en dix ans.

Cette contraction spectaculaire du volume du courrier distribué a donc creusé très significativement le déficit du service universel postal qui s'est établi à 617 millions d'euros en 2021 et 703 millions d'euros en 2022 (en coûts complets, hors effet des dépréciations des actifs courrier, après actualisation du réseau accessible). Le déficit du service universel postal pour l'année 2023 est en cours d'évaluation dans le cadre des travaux menés, comme chaque année, par l'Arcep.

Suivant une position constante, les membres de la Commission supérieure appellent l'Etat à compenser La Poste du coût net des missions de service public qui lui sont confiées et ont

sollicité dès 2020 la tenue du comité de suivi de haut niveau afin de traiter ces sujets (avis n°2020-09 du 30 juin 2020).

Les membres de la Commission supérieure ont salué la décision prise par le gouvernement à l'issue de la réunion du comité de suivi de haut niveau le 22 juillet 2021, auquel la CSNP était représentée, de compenser le déficit de la mission de service universel postal et de verser à La Poste une dotation budgétaire annuelle, qui sera modulée en fonction des résultats de qualité de service entre 500 et 520 millions d'euros.

Le nouvel article 2.2 du CPCE, modifié par la loi n°2021-1900 du 30 décembre 2021 de finances pour 2022, entré en vigueur le 1er janvier 2022, dispose :

I- Le prestataire du service universel postal reçoit de l'Etat une compensation au titre de sa mission de service universel postal définie à l'article L. 1 et dans les textes pris pour son application, dans les conditions fixées par le contrat d'entreprise prévu à l'article 9 de la loi n° 90-568 du 2 juillet 1990 relative à l'organisation du service public de la poste et à France Télécom.

II. - Chaque année, l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse évalue le coût net du service universel postal. Le prestataire du service universel postal transmet à l'autorité, à la demande de celle-ci, les informations et les documents comptables nécessaires à cette évaluation.

Un décret en Conseil d'Etat, pris après avis de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse et de la Commission supérieure du numérique et des postes, précise la méthode d'évaluation utilisée pour le calcul du coût net de la mission de service universel postal

L'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse, après avis de la Commission supérieure du numérique et des postes, remet chaque année au Gouvernement et au Parlement un rapport sur le coût net du service universel postal »

Le projet de décret soumis pour avis à la Commission supérieure du numérique et des postes a pour objet de :

- supprimer les dispositions relatives au fonds de compensation qui figuraient au chapitre 1er du titre I de la partie II (Décrets en Conseil d'Etat) du CPCE,

- préciser la méthode d'évaluation du coût net lié aux obligations de service universel postal afin de permettre à l'Arcep de déterminer le montant du coût net supporté par le prestataire de service universel postal en précisant notamment la notion de « charge financière inéquitable » visée à l'article R. 1-1-29 du code des postes et des communications électroniques (partie réglementaire : Décrets en Conseil d'Etat).

2 Sur la suppression des dispositions relatives au fonds de compensation

L'article 1er du projet de décret soumis pour avis dispose que :

- Dans l'intitulé du chapitre Ier, les mots « fonds de compensation » sont remplacés par le mot : « financement » ;
- Dans l'intitulé de la section 3, les mots « Le fonds de compensation » sont remplacés par les mots suivants : « Coût et financement ».

3 Sur les conditions de versement de la compensation du service universel postal

Le projet de décret soumis pour avis à la CSNP dispose que les articles R. 1-1-27 à R. 1-1-29 du code des postes et des communications électroniques sont remplacés par les dispositions suivantes :

« *Article R. 1-1-27 - L'Etat verse une compensation au prestataire du service universel postal lorsque les deux critères suivants sont remplis :*

1° Le coût net du service universel postal visé à l'article R. 1-1-28 est positif ;

2° La charge financière inéquitable visée à l'article R. 1-1-29 est caractérisée. »

« Article R. 1-1-28 - Le coût net du service universel postal correspond à la différence entre le coût net supporté par le prestataire du service universel postal lorsqu'il est soumis aux obligations résultant des dispositions législatives et réglementaires afférentes à l'exercice du service universel et celui supporté par le même prestataire lorsqu'il n'est pas soumis à ces obligations. »

« Il est tenu compte pour le calcul du coût net de tous les autres éléments pertinents, notamment des bénéfices immatériels et des avantages commerciaux dont bénéficie le prestataire du service universel postal en raison de la prestation de ce service, et de son droit de réaliser un bénéfice raisonnable. »

« Article R.1-1-29 - - Les obligations de service universel postal constituent une charge financière inéquitable pour son prestataire dès lors qu'au moins deux des critères suivants sont atteints :

1° Le coût net de la mission représente au moins un pour cent du chiffre d'affaires du service universel postal ;

2° Le volume des prestations relevant du service universel postal distribuées par le prestataire au cours des cinq dernières années connaît une diminution annuelle de plus de trois pour cent sur trois d'entre elles ;

3° La différence effectuée entre le coût net du service universel postal et les bénéfices immatériels réalisés par le prestataire est positive.

4 Avis de la Commission supérieure du numérique et des postes

La Commission supérieure constate que le projet de décret qui lui est soumis pour avis acte la suppression d'un fonds de compensation (ancienne section 3 du chapitre Ier du CPCE) qui n'avait jamais été activé et que le projet de décret précise les mesures d'application du nouvel article L2.2 du CPCE relatives au coût et au financement du service universel postal précisées aux articles R-1-1-27, R.1-1-28 et R.1-1-29 de ce texte.

La Commission supérieure du numérique et des postes souligne l'engagement inscrit dans le contrat d'entreprise entre l'Etat et La Poste d'une compensation garantie sur les années 2023, 2024 et 2025. Cet engagement pluriannuel est indispensable pour permettre à l'ensemble des parties prenantes d'inscrire efficacement leurs actions dans la durée (déploiement des effectifs, dotations).

Selon une position constante, la Commission supérieure du numérique et des postes estime qu'une juste compensation du coût des missions de service public confiées à La Poste est essentielle pour garantir dans le temps le niveau de qualité de service et la présence postale due à nos concitoyens.

Les membres de la Commission supérieure du numérique et des postes estiment que les critères introduits dans le projet de décret pour définir la notion de « charge financière inéquitable » instaurent des conditions supplémentaires liées au chiffre d'affaires du service universel postal, du volume des prestations et du différentiel entre le coût net du service universel postal et les bénéfices immatériels sans pour autant définir la notion de charge financière inéquitable.

En effet, les membres de la Commission supérieure du numérique et des postes considèrent que la notion de charge financière inéquitable est constatée dès lors que le prestataire en charge du service universel postal subit une perte qui n'est pas compensée par l'Etat. L'Etat ne doit couvrir que ce qui est nécessaire à l'exécution du service public mais l'Etat doit compenser à l'euro près le cout des missions de service public confiées à des tiers. Cet engagement de l'Etat est naturellement assorti de l'obligation pour le groupe La Poste de produire toutes les données comptables nécessaires pour mesurer les charges financières générées par l'exercice des missions de service public.

La Commission supérieure du numérique et des postes constate que la première condition introduite par le décret, à savoir que le coût net de la mission représente plus de 1% du chiffre d'affaires du service universel postal, représente, appliquée aux données actuelles, un montant de l'ordre de 50 millions d'euros.

Si ce critère a été révisé à la baisse en passant de 3% à 1% du chiffre d'affaires du service universel postal à l'issue des réunions de travail entre la Direction générale des entreprises et le groupe La Poste, il n'en demeure pas moins que cette première condition n'est pas compatible avec la position de la Commission supérieure du numérique et des postes qui préconise une juste compensation des missions de service public confiées au groupe La Poste.

La Commission supérieure du numérique et des postes relève en outre que les avantages immatériels dont bénéficie le prestataire du fait de la mission de service public qui lui est

confiée sont d'ores et déjà déduits de la méthode de calcul du coût net de la mission de service public confiée au groupe La Poste.

Au cours des échanges avec la direction générale des entreprises, il a été précisé que les critères retenus dans le projet de décret étaient analogues à la règlementation en vigueur dans trois pays de l'Union européenne seulement (Belgique, Grèce, Portugal) et non dans l'intégralité des pays de l'Union européenne compensant le service universel postal. Il ne faut donc pas écarter le fait que ces dispositions constituent une surtransposition de la directive postale. De fait, de nombreux pays n'ont pas adopté ou ont adopté une définition très différente de la notion de « charge financière inéquitable ».

En décembre 2020[1], la Cour de justice de l'Union européenne a eu l'occasion de se prononcer sur la notion de charge financière inéquitable pesant sur Poczta Polska, la poste polonaise, et a validé la législation polonaise qui considère qu'un déficit du compte du service universel postal entraîne *de facto* une charge financière inéquitable.

Dans ces conditions, la Commission supérieure du numérique et des postes émet un avis réservé sur le projet de décret relatif à la méthode d'évaluation utilisée pour le calcul du coût net du service universel postal et invite la direction générale des entreprises à proposer une définition de la notion de « charge financière inéquitable » plus conforme à une juste compensation par l'Etat des missions de service public confiées à des tiers.

[1] CJUE, 17 décembre 2020, Inpost Paczkomaty / Commission - Affaires C431/19 P et C432/19 P

CSNP

COMMISSION SUPÉRIEURE DU NUMÉRIQUE ET DES POSTES

RAPPORT N° 2024-07 DU 3 OCTOBRE 2024

Les enjeux de la transposition de la directive NIS 2 en France

RAPPORT N°2024-07 DU 3 OCTOBRE 2024

LES ENJEUX DE LA TRANSPOSITION DE LA DIRECTIVE NIS 2 EN FRANCE

PRESENTE PAR

M. DAMIEN MICHALLET, SENATEUR DE L'ISERE, PRESIDENT DE LA CSNP

ET

MME ANNE LE HENANFF, DEPUTEE DU MORBIHAN, RAPPORTEURE

Les enjeux de la transposition de la directive NIS 2 en France

Les membres de la Commission supérieure du numérique et des postes (CSNP) accueillent très favorablement la transposition de la directive NIS 2 qui a été adoptée le 14 décembre 2022 avec le plein soutien des autorités françaises : il est essentiel de relever le niveau de sécurité numérique global et la directive NIS 2 constitue un levier essentiel pour atteindre cet objectif.

Alors que la directive NIS 1 concernait près de 600 entités, c'est un changement d'échelle qui est opéré avec la transposition de la directive NIS 2 puisque près de 15 000 entités seraient désormais concernées selon l'ANSSI. Ce changement d'échelle correspond également à un véritable changement de paradigme en matière de sécurité numérique.

A l'automne 2023, l'ANSSI a lancé une phase de consultations auprès des différents acteurs concernés par la transposition de la directives NIS 2 : les fédérations d'entreprises, les représentants des collectivités locales et territoriales, les fédérations d'acteurs et des usagers…

La restitution de ces consultations a eu lieu le 24 avril 2024 et, en prévision de sa saisine par l'ANSSI, les membres de la CSNP ont confié en mars 2024 à M. Damien MICHALLET, sénateur de l'Isère et président de la CSNP, et Mme Anne LE HÉNANFF, députée du Morbihan, le pilotage d'un groupe de travail sur la transposition de la directive *Network and Information Systems 2*, dite NIS 2 pour lequel Mme Anne Le Hénanff a été nommée rapporteure.

Ce groupe de travail est surtout né de la volonté d'analyser l'impact que les nombreuses nouvelles obligations de la directive auront sur les entités concernées et de la meilleure manière d'adapter notre droit en conséquence avant même que le projet de loi transposant la directive ne soit présenté en conseil des ministres et inscrit à l'ordre du jour du Parlement.

De mars à mai 2024, le groupe de travail a auditionné 41 acteurs, notamment l'Agence nationale de la sécurité des systèmes d'information (ANSSI), des éditeurs de logiciels, des *clouders* européens et extra-européens, des associations représentant des collectivités et des entreprises, des cabinets de conseils, des responsables de systèmes d'information, des juristes, etc…

Il ressort de ces auditions que la transposition de la directive NIS 2 fixée au 17 octobre 2024 soulève un certain nombre de défis pour les entités qui vont se retrouver régies par ces dispositions.

La dissolution de l'Assemblée nationale le 9 juin 2024 a, de fait, perturbé le calendrier d'adoption du projet de loi de transposition de la directive NIS 2.

Au terme de ses travaux, le groupe de travail a présenté au cours de la séance plénière du 18 septembre 2024 aux membres de la CSNP le présent rapport sur les enjeux posés par la transposition de la directive NIS 2 et formule 32 recommandations.

RECOMMANDATIONS

Recommandation n°1 : Organiser une véritable campagne de communication à destination des entreprises et des collectivités locales. Cette campagne d'information à large échelle pourrait également inclure le grand public.

Recommandation n°2 : Axer la communication sur les bénéfices de la mise en œuvre de la directive NIS 2 et sur les atouts que représente le relèvement du niveau de sécurité numérique pour nos entreprises et nos collectivités locales et la sécurisation des données des clients et des usagers. Une labellisation NIS 2 pourrait constituer une mesure incitative pour les entités qui auront fait l'effort de déployer les moyens nécessaires à la mise en conformité avec la directive NIS 2.

Recommandation n°3 : Préciser dans la loi que les délais de mise en conformité sont fixés au 31 décembre 2027. Si les décrets et textes règlementaires étaient pris avec beaucoup de retard, comme cela avait été le cas dans le cadre de la transposition de la directive NIS1, le législateur serait en mesure de voter une loi rectificative.

Recommandation n°4 : Compléter l'étude d'impact sur les coûts humains, techniques et financiers pour les entités ainsi que sur les délais de mise en conformité.

Recommandation n°5 : Créer une commission spéciale pour l'examen du projet de loi *relatif à la résilience des activités d'importance vitale, à la protection des infrastructures critiques, à la cybersécurité et à la résilience opérationnelle numérique du secteur financier.*

Recommandation n°6 : Créer une commission permanente en charge du numérique à l'occasion de la prochaine révision du règlement de l'Assemblée nationale et de celui du Sénat.

Recommandation n°7 : Limiter au maximum le renvoi à des décrets en Conseil d'État.

Recommandation n°8 : Réintégrer dans le projet de loi les seuils et critères précisés dans la directive NIS 2 et ses annexes.

Recommandation n°9 : Confier à l'ANSSI la responsabilité de désigner les collectivités locales soumises à NIS 2.

Recommandation n°10 : Préciser dans le texte de loi la notion d'*« incident important »* en publiant une liste de critères objectivables par les entité essentielles et importantes.

Recommandation n°11 : Prévoir dans la loi des mécanismes explicites de protection des informations divulguées lors de signalement d'incidents, afin de garantir la confidentialité des données sensibles et stratégiques des entreprises qui pourraient être transmises dans le cadre d'une notification.

Recommandation n°12 : Prévoir dans la loi une clause d'adaptabilité aux évolutions technologiques liées notamment à l'usage de l'intelligence artificielle en matière de cybersécurité.

Recommandation n°13 : Respecter le principe de subsidiarité et promouvoir une approche harmonisée au niveau de l'Union européenne dans la transposition de la directive NIS 2 afin de faciliter la conformité pour les entreprises opérant à l'échelle européenne et d'éviter l'apparition de différentiels de régulation pouvant créer des effets de concurrence entre les législations européennes.

Recommandation n°14 : Mettre en place un guichet unique pour déclarer les incidents en élargissant les fonctionnalités de la plateforme 17Cyber

Recommandation n°15 : Uniformiser les formulaires de remontées d'incidents.

Recommandation n°16 : Renforcer la présence de l'ANSSI en région.

Recommandation n°17 : Certifier par l'ANSSI les prestataires privés susceptibles d'intervenir auprès d'une entité soumise à la directive NIS 2.

Recommandation n°18 : Clarifier le rôle des CSIRT territoriaux dans la transposition de NIS 2.

Recommandation n°19 : Créer une mission d'information parlementaire sur le rôle, le fonctionnement et le financement des CSIRT régionaux et sectoriels.

Recommandation n°20 : Allouer des crédits supplémentaires au SGDSN dans le cadre du programme 129 lors du PLF pour 2025, crédits qui seront fléchés vers le GIP ACYMA.

Recommandation n°21 : Accompagner financièrement les entités ne disposant pas des moyens nécessaires à leur mise en conformité.

Recommandation n°22 : Faire auditer par l'ANSSI le degré de maturité des collectivités locales qui seront soumises à la directive NIS 2 et en mesure de se conformer au calendrier de mise en œuvre. Un accompagnement spécifique, technique et financier sera prévu pour celles n'ayant pas les moyens nécessaires. La mobilisation des financements de la stratégie nationale d'accélération cyber vers des outils intégrés conformes aux exigences posées par l'ANSSI doit être étudiée.

Recommandation n°23 : Introduire plus de progressivité dans la mise en œuvre de la directive NIS 2 et réaliser une étude d'impact plus précise pour qualifier les risques, les menaces et les coûts financiers, administratifs, démocratiques des cyberattaques pesant sur les collectivités territoriales. Les membres de la CSNP appuient les demandes des collectivités territoriales exprimées en ce sens.

Recommandation n°24 : Inciter les collectivités, notamment celles qui n'ont pas les moyens humains nécessaires, à faire le choix d'une solution dite SaaS afin de maintenir le meilleur niveau de cybersécurité possible.

Recommandation n°25 : Renforcer le rôle des préfets dans l'accompagnement des collectivités à se conformer aux obligations de la directive NIS 2.

Recommandation n°26 : Prévoir un accompagnement financier des acteurs les plus fragiles afin que la mise en œuvre de la directive NIS 2 constitue un levier puissant pour encourager la mutualisation et renforcer la sécurisation des systèmes d'information des acteurs de la santé.

Recommandation n°27 : Renforcer la concertation entre l'ANSSI, le ministère de la Santé et les entités du secteur de la santé potentiellement concernées par un relèvement de leur statut d'entité importante à entité essentielle en cas de crise sanitaire sur les mesures adaptées et proportionnées à mettre en place.

Recommandation n°28 : Préciser le régime applicable au secteur des assurances en application de la *lex specialis* pour lever les risques de double régulation entre la directive NIS 2 et le règlement DORA.

Recommandation n°29 : Intégrer dans le texte de transposition de la directive NIS 2 la nécessité pour les entités essentielles et importantes de modifier les obligations contractuelles qui les lient à leurs sous-traitants.

Recommandation n°30 : Préciser dans la loi le périmètre de l'article 28 de la directive NIS 2 relatif à la base des données d'enregistrement des noms de domaine.

Recommandation n°31 *(en cas d'évolution du projet de loi)* : Faire le choix de déléguer à une commission *ad hoc* et indépendante le pouvoir de sanctions en cas de non-respect des obligations introduites par la directive.

Recommandation n°32 : Accorder une certaine souplesse dans l'appréciation des infractions aux obligations et les sanctions relatives jusqu'au 31 décembre 2027.

I. LA DIRECTIVE NIS 2 : UN LEVIER PUISSANT POUR RELEVER LE NIVEAU DE SECURITE NUMERIQUE DE LA FRANCE

➢ La directive NIS 2 : un changement de paradigme par rapport à la directive NIS 1

Six ans après son adoption, la directive (UE) 2016/1148 du 6 juillet 2016[1], dite NIS1, est révisée et remplacée par la directive (UE) 2022/2555 du 14 décembre 2022[2] , dite NIS 2. **Cette directive répond à un besoin d'harmonisation des normes communes en matière de cybersécurité et à la nécessité de faire face à l'augmentation des cyberattaques dans l'Union européenne**. La Commission européenne avait soumis, le 16 décembre 2020, une proposition tendant à réviser la Directive NIS 1, qui constituait le premier texte législatif de l'Union européenne sur la cybersécurité et dont le champ d'application devait être étendu.

Cette proposition s'inscrivait dans la ligne des priorités de la Commission pour la stratégie 2020-2025 visant à rendre l'Europe apte à l'ère numérique[3].

Dans un communiqué de presse du 13 mai 2022, Thierry Breton, alors commissaire européen au commerce intérieur, avait souligné l'importance de cette révision de la Directive NIS 1: « *Malgré leurs accomplissements notables et leur incidence positive, ces règles ont dû être mises à jour en raison du degré croissant de numérisation et d'interconnexion de notre société et de l'augmentation des actes de cybermalveillance à l'échelle mondiale*[4]. »

La directive a été publiée au Journal officiel de l'Union européenne le 27 décembre 2022. **Les États-membres doivent désormais transposer les nouvelles dispositions dans leur droit national au plus tard le 17 octobre 2024 et les appliquer à partir du 18 octobre 2024**. L'Article 40 de la directive prévoit un nouveau réexamen par la Commission au plus tard le 17 octobre 2027 et tous les 36 mois par la suite.

Le projet de loi *relatif à la résilience des activités d'importance vitale, à la protection des infrastructures critiques, à la cybersécurité et à la résilience opérationnelle numérique du secteur financier*, transposant notamment la directive NIS 2, devait être présenté en conseil des ministres le 12 juin dernier, en vue d'être inscrit à l'ordre du jour du Parlement. La dissolution de l'Assemblée nationale, annoncée par le Président de la République le 9 juin au soir, a mis un coup d'arrêt au parcours de ce texte de loi avant même son commencement. A l'heure où parait le présent rapport, ledit texte de loi n'a toujours pas été présenté en conseil des ministres, et la date du 17 octobre 2024 approchant, son avenir sous la forme qu'on lui connait, est incertain.

La directive NIS 2, dont l'adoption a été portée et soutenue par les autorités françaises, vise à renforcer le niveau de cybersécurité introduit par la directive dite NIS 1 qui était centrée sur les opérateurs de services essentiels (OSE), et les fournisseurs de services numériques (FSN).

La directive NIS 1 avait identifié six secteurs essentiels. Dans son annexe I, la directive NIS 2 reprend et complète certains secteurs inclus par la France au niveau national en 2018. **Elle établit une liste des secteurs hautement critiques.** Dans son annexe II, **la directive NIS 2 établit également une liste des secteurs critiques.**

---

[1] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016L114

[2] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022L2555&from=FR

[3] https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333#:~:text=The%20NIS2%20Directive%3A%20A%20high%20common%20level%20of%20cybersecurity%20in%20the%20EU,

[4] https://ec.europa.eu/commission/presscorner/detail/fr/ip_22_2985

Tableau comparatif des secteurs concernés

Directive NIS 1	Directive NIS 2
Secteurs essentiels • Energie • Transport • Banques • Infrastructures de marchés financiers • Secteur de la santé • Fourniture et distribution d'eau potable • Infrastructures numériques	**Secteurs hautement critiques** • Energie • Transports • Secteur bancaire • Infrastructures des marchés financiers • Santé • Eau potable • Eaux usées • Infrastructure numérique • Gestion des services TIC (interentreprises) • Administration publique (dont les activités ne portent pas sur la sécurité nationale, sécurité publique, la défense ou l'application de la loi) • Espace **Autres secteurs critiques :** • Services postaux et d'expédition • Gestion des déchets • Fabrication, production et distribution de produits chimiques • Production, transformation et distribution des denrées alimentaires • Fabrication • Fournisseurs numériques • Recherche

En intégrant dans son champ d'application, des collectivités territoriales de plus de 30 000 habitants et des entreprises privées répondant aux critères de seuils établis par la recommandation de la Commission européenne C (2003) 1422 du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises, la directive NIS 2 introduit un changement de paradigme en instaurant un niveau de sécurité collectif.

- **Plus de 15 000 entités concernées par la transposition de la directive NIS 2**

Selon l'ANSSI, ce sont près de 15 000 entités qui seront concernées par la transposition de la directive NIS 2 contre près de 600 entités concernées par la directive NIS 1.

La directive NIS 2 comme le projet de loi transmis par l'ANSSI distingue deux catégories entrant dans son périmètre : **les entités essentielles actives dans des secteurs hautement critiques et les entités importantes.**

Les entités essentielles sont des organisations appartenant à des secteurs d'activité hautement critiques, fixés par décret en Conseil d'Etat, dont les effectifs, le chiffre d'affaires annuel et le total du bilan annuel excèdent des seuils définis par voie règlementaire. Ces entités incluent des

établissements publics à caractère industriel et commercial, des opérateurs de services de confiance qualifiés, des offices d'enregistrement, des fournisseurs de service de système de noms de domaine, ainsi que certaines administrations publiques et collectivités territoriales.

Les entités importantes appartiennent à des secteurs critiques, également fixés par décret, qui ne répondent pas aux critères des entités essentielles mais dépassent des seuils définis par voie règlementaire. Elles comprennent, entre autres, des opérateurs de service de confiance, des communautés de communes et des établissements d'enseignement menant des activités de recherche.

Le Premier ministre peut désigner des entités comme essentielles ou importantes, indépendamment de leur taille, si elles répondent à des critères spécifiques tels que l'unicité de leur service sur le territoire national, l'impact potentiel de leur perturbation sur la sécurité publique, ou leur importance systémique.

En France, une grande partie des entités essentielles sont des structures déjà sensibilisées ou confrontées à la menace cyber et sont déjà soumises aux dispositions de la directive NIS1 et/ou au dispositif de sécurité des activités d'importance vitale (SAIV).

Le changement majeur introduit par la transposition de la directive NIS 2 porte sur l'extension aux entités importantes, **aux collectivités locales de plus de 30 000 habitants et aux entreprises privées qui dépasseront certains seuils** (nombre de salariés, chiffre d'affaires, bilan).

Pour le secteur privé, les seuils fixés par la directive NIS 2 sont les suivants :

Taille Entité	Nombre d'employés	Chiffre d'affaires (millions €)	Bilan annuel (millions €)	Classification Annexe 1	Classification Annexe 2
Intermédiaire et grande	Supérieur à 250	Supérieur à 50	Supérieur à 43	Entités essentielles	Entités importante
Moyenne	Entre 50 et 250	Compris entre 10 et 50	Compris entre 10 et 43	Entités importantes	Entités importante
Micro et petite	Inférieur à 50	Inférieur à 10	Inférieur à 10	Non concernées	Non concernées

Source : ANSSI

Dans son projet d'étude d'impact, **l'ANSSI estime que 1489 collectivités territoriales, groupements de collectivités territoriales et certains organismes sous leur tutelle devraient être concernés au titre des entités essentielles**. **992 communautés de communes métropolitaines et d'outre-mer seront, quant à elles, concernées au titre des entités importantes.**

Le nombre d'entreprises privées concernées seraient, selon l'ANSSI, de l'ordre de 14 000.

Les organisations représentatives des entreprises consultées par la CSNP considèrent que ce nombre pourrait être plus élevé.

II. UNE CAMPAGNE DE COMMUNICATION AMBITIEUSE NECESSAIRE

Il ressort des auditions conduites par la CSNP, qu'à quelques semaines de l'entrée en vigueur de la directive NIS 2, le 17 octobre prochain, il est plus que vraisemblable que de très nombreuses entreprises et collectivités locales ne soient pas pleinement informées de l'existence de cette entrée en vigueur, des nouvelles obligations qui pèseront sur elles et des mesures qu'elles devront prendre pour s'y conformer.

Si l'ANSSI travaille actuellement à un questionnaire en ligne *via* une plateforme qui permettra de répondre aux interrogations des entités concernées, on se rend compte que la transposition de cette directive appelle un travail d'outillage important qu'il conviendra de faire dans les meilleurs délais : guichet unique, communication, guide, etc... Ces outils devront être accessibles, clairs, compréhensibles y compris pour les entités les moins accoutumées au domaine cyber.

Du point de vue des membres de la CSNP, il est essentiel d'activer une campagne d'information d'ampleur nationale pour informer ces acteurs. Cette information à large échelle, qui pourrait inclure le grand public, est une demande récurrente de toutes les organisations professionnelles auditionnées.

Recommandation n°1 : Organiser une véritable campagne de communication à destination des entreprises et des collectivités locales. Cette campagne d'information à large échelle pourrait également inclure le grand public.

Recommandation n°2 : Axer la communication sur les bénéfices de la mise en œuvre de la directive NIS 2 et sur les atouts que représente le relèvement du niveau de sécurité numérique pour nos entreprises et nos collectivités locales et la sécurisation des données des clients et des usagers. Une labellisation NIS 2 pourrait constituer une mesure incitative pour les entités qui auront fait l'effort de déployer les moyens nécessaires à la mise en conformité avec la directive NIS 2.

LA TRANSPOSITION DE LA DIRECTIVE NIS 2

UNE OPPORTUNITE POUR COMMUNIQUER PLUS ET MIEUX SUR LES ENJEUX DE SECURITE NUMERIQUE

La directive NIS 2, marque une évolution significative en matière de cybersécurité en Europe, élargissant considérablement le nombre d'entités assujetties à ses règles de 600 à 15 000.

Cette expansion inclut non seulement les entreprises mais aussi les collectivités locales, qui, pour la plupart, ne sont pas encore pleinement informées des nouvelles obligations qui leur incomberont.

Dans ce contexte, il est crucial de mettre en place une campagne de communication impactante pour sensibiliser ces acteurs aux enjeux de la directive NIS 2.

Actuellement, une majorité des nouvelles entités concernées n'ont pas conscience des mesures à venir et des critères qu'elles devront analyser elles-mêmes pour déterminer leur conformité.

Il est nécessaire d'organiser une campagne de communication nationale pour informer les entreprises et les collectivités locales des nouvelles obligations réglementaires, des mesures de conformité et des bénéfices associés.

Il est impératif d'informer les entités sur les nouvelles exigences de la directive NIS 2. Contrairement à la directive NIS 1, où l'ANSSI désignait les entités régulées, les nouvelles entités devront auto-évaluer leur conformité. Cette auto-évaluation nécessite une compréhension claire des critères et des seuils pertinents.

La communication doit également mettre en avant les avantages de la mise en œuvre de la directive. *En améliorant leur niveau de sécurité numérique, les entreprises et les collectivités locales peuvent protéger plus efficacement les données de leurs clients et usagers, renforcer leur résilience face aux cyberattaques et, par conséquent, augmenter leur compétitivité.* ***Une communication efficace doit souligner ces points pour encourager une adhésion enthousiaste à la directive.***

La mise en place d'un label NIS 2 pour les entités conformes pourrait constituer une incitation supplémentaire*. Ce label pourrait être utilisé comme un gage de qualité et de sécurité, valorisant les efforts des entreprises et des collectivités pour se conformer aux nouvelles régulations. Une telle reconnaissance pourrait également servir de différenciateur compétitif sur le marché.*

Le cyber-mois qui est organisé en octobre chaque année, un événement européen annuel, est une occasion idéale pour sensibiliser aux bénéfices et à la nécessité de la directive NIS 2. *Profiter de cette période permet d'informer sur les nouvelles exigences réglementaires, d'expliquer les bénéfices pour la résilience des infrastructures et de promouvoir des sessions de formation et des mises à niveau de systèmes. Communiquer durant cet événement bénéficiant d'une visibilité accrue permettra de renforcer la confiance des clients et partenaires, et engager les parties prenantes dans les préparatifs nécessaires à la conformité.*

III. DES POINTS DE VIGILANCE IDENTIFIES

➢ Des délais de mise en conformité trop courts

La date d'entrée en vigueur de la directive est fixée au 17 octobre 2024. A quelques semaines de cette échéance, le projet de loi n'a toujours pas été présenté en conseil des ministres et n'a pas encore été présenté devant le Parlement.

Pourtant, dès l'entrée en vigueur de la loi, les entités concernées auront l'obligation de s'enregistrer auprès de l'autorité nationale de cybersécurité.

La directive NIS 2 ne traite pas des délais, c'est un angle mort de ce texte, cependant il est nécessaire que le législateur en tienne compte lors des débats.

Le projet d'étude d'impact produit par l'ANSSI indique que « *la réglementation NIS 2, telle que mise en œuvre en France, définira des délais de mise en conformité qui tiendront compte des efforts de compréhension, de montée en compétence et d'investissement que les exigences imposent aux assujettis. Les lignes directrices et les objectifs de haut niveau font partie des textes publiés depuis fin 2022, mais les textes précis de transposition ne seront connus du grand public qu'à la suite de la phase règlementaire*[5]*. Une mise en œuvre de contrôles susceptibles de découler sur des sanctions n'est pas envisagée avant plusieurs années.* »

Il ressort des auditions qu'un alignement sur le délai de mise en œuvre du RGPD, à savoir un délai de 3 ans, apparait comme une option à privilégier car il prendrait en compte le principe de réalité opérationnelle. La définition d'une feuille de route avec un rétroplanning pour la mise en conformité pourrait sensiblement aider les entités à relever leur niveau de cybersécurité. Il sera sans doute nécessaire d'établir des étapes intermédiaires avec des délais spécifiques, en fonction de la nature et des moyens dont disposent les différentes catégories d'entités régulées, pour la mise en place des mesures de sécurité.

Pour la feuille de route, la CSNP préconise les 3 stades progressifs suivants :

1- Formation/sensibilisation
2- Évaluation/audit
3- Contrôle/sanction

<u>Recommandation n°3 :</u> Préciser dans la loi que les délais de mise en conformité sont fixés au 31 décembre 2027. Si les décrets et textes règlementaires étaient pris avec beaucoup de retard, comme cela avait été le cas dans le cadre de la transposition de la directive NIS1, le législateur serait en mesure de voter une loi rectificative.

➢ De la nécessité d'avoir une véritable étude d'impact

Lors des auditions, la CSNP a pu constater que l'absence d'une étude d'impact complète et détaillée à l'échelle européenne, en raison de la crise sanitaire puis de la modification du projet de

[5] Un décret en Conseil d'Etat doit préciser la liste des secteurs d'activité critiques et hautement critiques. Trois décrets simples seront pris pour préciser les seuils pour les entités essentielles, les entités importantes et les opérateurs du code des postes et des communications électroniques, les modalités de désignation unitaire de certaines entités par le Premier ministre et les modalités de communication des informations nécessaires à l'établissement de la liste des entités.

directive, avait largement participé à soulever des inquiétudes chez les entités potentiellement assujetties à la directive NIS 2, sans y apporter de réponses.

Le législateur pâtit également de cette étude d'impact incomplète laquelle doit de se pencher tout particulièrement sur les coûts humains, techniques et financiers pour les entités ainsi que sur les délais de mise en conformité.

<u>Recommandation n°4 :</u> Compléter l'étude d'impact sur les coûts humains, techniques et financiers pour les entités ainsi que sur les délais de mise en conformité.

- **Donner au législateur les bons outils**

Compte tenu de l'importance de ce texte, notamment au regard du nombre de secteurs concernés et d'entités, et des différentes commissions qui devraient être saisies au fond sur le projet de loi (commissions des lois, de la Défense nationale, des affaires économiques, etc…), la CSNP recommande vivement la création d'une commission spéciale pour son examen.

Par ailleurs, cela interroge sur le recours à des commissions spéciales pour l'examen des textes relatifs au numérique, comme cela a été le cas en 2023 avec l'examen du projet de loi *visant à sécuriser et réguler l'espace numérique*. Le numérique est un sujet transverse et n'a pas de commission permanente dédiée.

<u>Recommandation n°5 :</u> Créer une commission spéciale pour l'examen du projet de loi *relatif à la résilience des activités d'importance vitale, à la protection des infrastructures critiques, à la cybersécurité et à la résilience opérationnelle numérique du secteur financier.*

<u>Recommandation n°6 :</u> Créer une commission permanente en charge du numérique à l'occasion de la prochaine révision du règlement de l'Assemblée nationale et de celui du Sénat.

- **Un renvoi trop systématique à la voie règlementaire**

Sur les sujets du numérique tout particulièrement, les projets de loi renvoient beaucoup à des décrets, notamment pour pallier des études d'impact parfois approximatives et laisser le temps de la consultation avec l'écosystème.

Cependant, la grande majorité des textes relatifs au sujet du numérique débattus et adoptés ces dernières années sont des adaptations et des transpositions d'actes juridiques européens, tels que le *Digital Services Act* (DSA) ou encore le *Digital Markets Act* (DMA).

Or, comme le prévoit l'article 288 du traité sur le fonctionnement de l'Union européenne (TFUE), les actes juridiques contraignants, telles que les directives, doivent être transposés dans chacun des États-membres dans un délai fixé lors de leur adoption (généralement dans les deux ans), ce qui permet une possible anticipation de leur transposition.

Si la CSNP entend qu'il est parfois nécessaire de garder une certaine souplesse et ne pas être « trop disant » en inscrivant dans le marbre de la loi des critères et définitions trop précises ou des listes trop exhaustives, le renvoi trop fréquent aux décrets nuit à la clarté et à la lisibilité du texte pour les entités concernées et ceux qui les conseillent. En effet, lors des auditions menées dans le cadre du

présent rapport, nombreuses ont été les remarques sur ces nombreux renvois. Cela d'autant plus qu'ils ont tendance à se multiplier ces derniers temps et que les délais de parutions des décrets peuvent être assez longs, mettant à mal certaines mises en application.

Par ailleurs, ces renvois peuvent mettre à mal le rôle du législateur. Dans le projet de loi *relatif à la résilience des activités d'importance vitale, à la protection des infrastructures critiques, à la cybersécurité et à la résilience opérationnelle numérique du secteur financier* sur lequel la CSNP a été saisie pour avis en mai dernier, il est demandé au législateur de débattre et de voter des articles sans connaitre précisément le périmètre des entités concernées ainsi que le type d'incidents qu'il faudra déclarer puisque ces informations, pourtant essentielles, seront précisées par décret. Dès lors, comment savoir s'il n'y aura pas d'effet de bord ?

La CSNP tient à rappeler que le rôle des parlementaires n'est pas seulement de faire la loi mais également de contrôler l'action du Gouvernement. Alors que le contenu de la directive NIS 2 est connu depuis plusieurs années ainsi que son étude d'impact européenne, demander aux entités potentiellement concernées ainsi qu'au législateur de faire confiance au Gouvernement et au Conseil d'État sur des dispositions aussi importantes interroge.

A l'issue des auditions conduites par le groupe de travail, des interrogations subsistent sur la faculté pour certaines entités de savoir précisément si elles relèveront du champ d'application de la nouvelle loi.

C'est notamment le cas des collectivités locales. Le seuil de 30 000 habitants introduit par la directive NIS 2 et repris par l'article 6 du projet de loi paraît, en théorie, facilement applicable mais certaines collectivités locales qui ne sont pas concernées par ce seuil s'interrogent malgré tout sur leur possible entrée dans le champ d'application de la loi dès lors qu'elles fournissent un service qui relève de l'annexe I ou de l'annexe II de la directive NIS 2, notamment un service de gestion lié au traitement ou de gestion de fourniture d'énergie, d'eau potable, des eaux usées ou de déchets.

Ces interrogations sur le périmètre de la directive NIS 2 sont également partagées par certaines entreprises qui ne sont pas concernées en raison des critères de seuils mais dont l'activité relève des secteurs économiques critiques et hautement critiques.

La plateforme mise en place par l'ANSSI ne répondrait que partiellement aux préoccupations de ces entités.

La CSNP tient à souligner qu'un autre choix aurait été possible : le législateur belge, pour sa part, a choisi de confier à l'homologue belge de l'ANSSI la responsabilité de désigner les collectivités locales qui seraient soumises à la transposition de la directive NIS 2. Ce choix permet de clarifier la situation et place régulateur et régulés face à leurs responsabilités.

<u>Recommandation n°7 :</u> Limiter au maximum le renvoi à des décrets en Conseil d'État.

<u>Recommandation n°8 :</u> Réintégrer dans le projet de loi les seuils et critères précisés dans la directive NIS 2 et ses annexes.

<u>Recommandation n°9 :</u> Confier à l'ANSSI la responsabilité de désigner les collectivités locales soumises à NIS 2.

- **Des précisions attendues sur la notion de *« tout incident ayant un impact important »***

Les entités qui auront constaté un incident ayant un impact important auront l'obligation d'en informer l'ANSSI. Il ressort des auditions que l'obligation de notification *« sans retard injustifié »* à l'ANSSI de *« tout incident ayant un impact important »* (article 33 de la directive NIS 2) sur la fourniture de leurs services paraît insuffisamment précis.

En effet, il n'est pas rare qu'une cyberattaque ne soit pas immédiatement identifiée et que l'ampleur de son impact, important ou pas, puisse parfois être difficilement évaluable.

La notion d'incident important retenue par l'ANSSI est celle de la loi n° 2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense, dite loi de Programmation Militaire, et correspond à la jurisprudence construite de manière itérative dans le cadre de la transposition de la directive NIS 1.

Pour une entreprise ou une collectivité locale, cette notion peut évoluer et être appréciée différemment au fil du temps et de la découverte des conséquences d'un incident sur le fonctionnement des systèmes d'information.

Il est prévu qu'un décret en Conseil d'Etat précisera la procédure applicable et les critères d'appréciation des caractères importants et critiques des incidents et vulnérabilités ainsi que les délais de notification des incidents et des vulnérabilités.

Les membres de la CSNP sont confiants dans le fait que l'ANSSI appréciera avec une grille de lecture adaptée et contextualisée cette obligation mise en place par l'article 11 du projet de loi mais alertent sur les risques juridiques qui pourraient peser sur les entités essentielles et importantes en cas de contentieux avec leurs clients, leurs administrés, leurs fournisseurs ou leurs sous-traitants.

Le législateur belge a fait le choix de ne laisser libre court à aucune appréciation en inscrivant ces définitions dans la loi. Si certains acteurs auditionnés ont fait part de leur souhait de voir une définition inscrite dans la loi, d'autres ont souligné qu'il était davantage judicieux de laisser de la souplesse afin d'éviter des effets de bord, mais que des critères devaient toutefois être clairement écrits.

En effet, un « incident important » ne sera pas forcément perçu de la même manière selon les entités, ou entre un client et un fournisseur. Dans tous les cas, la CSNP recommande au législateur de ne pas inscrire une définition « incident important » dans la loi en partant de l'impact.

En tout état de cause, un guide de bonnes pratiques est souhaité et attendu par les entités interrogées.

<u>Recommandation n°10 :</u> Préciser dans le texte de loi la notion d'*« incident important »* en publiant une liste de critères objectivables par les entité essentielles et importantes.

<u>Recommandation n°11 :</u> Prévoir dans la loi des mécanismes explicites de protection des informations divulguées lors de signalement d'incidents, afin de garantir la confidentialité des données sensibles et stratégiques des entreprises qui pourraient être transmises dans le cadre d'une notification.

<u>Recommandation n°12 :</u> Prévoir dans la loi une clause d'adaptabilité aux évolutions technologiques liées notamment à l'usage de l'intelligence artificielle en matière de cybersécurité.

- **La difficulté de prouver la mise en conformité à NIS 2**

Lors des auditions, de très nombreux acteurs ont fait part de leur inquiétude quant à la manière dont ils pourraient prouver leur conformité à la directive NIS 2 à leurs clients. Comme proposé précédemment dans le présent avis, **la CSNP recommande la mise en place d'un système de labellisation.** Cette labellisation permettrait, en plus d'être incitative, d'être un gage de confiance entre les acteurs.

- **La question de la souveraineté**

Lors des auditions, menées au printemps 2024, le projet d'acte d'exécution de la Commission européenne n'était pas encore connu, aussi la CSNP n'a pu recueillir de remarques de la part des différents acteurs.

Toutefois, sur la base du projet d'acte d'exécution paru fin juin 2024, la CSNP constate que qu'il laisse entrevoir le fait que le champ d'action de l'ANSSI va désormais être élargi au contrôle du niveau de disponibilité et de qualité de service des fournisseurs de services numériques, et non plus seulement des incidents de cybersécurité. Cela fait craindre une multiplication d'incidents considérés comme « significatifs » et augmentera le nombre de notifications des différents acteurs auprès de l'ANSSI.

IV. UN IMPERATIF : PAS DE SURTRANSPOSITION QUI PORTERAIT ATTEINTE A UN CADRE EUROPEEN HARMONISE

Les membres de la CSNP sont très attentifs à ce que la transposition de la directive NIS 2 en France ne soit pas assortie de dispositions supplémentaires qui entraineraient une surtransposition susceptible de compromettre l'harmonisation des normes de cybersécurité à travers l'Union européenne.

Une surtransposition, en imposant des exigences supplémentaires et potentiellement plus strictes que celles prévues par la directive, créerait des divergences réglementaires entre les États membres. Cette situation placerait les entreprises françaises opérant à l'échelle européenne dans une situation défavorable. Les entreprises françaises seraient en effet confrontées à des exigences de conformité différentes et parfois contradictoires, générant des coûts administratifs et opérationnels et affectant *de facto* leur compétitivité face à des concurrents soumis à des régulations moins strictes.

Cette situation favoriserait l'apparition de "pavillons de complaisance" et pourrait conduire certaines entreprises à s'implanter dans des pays avec des exigences moins contraignantes pour réduire leurs coûts de mise en conformité, comme cela a été observé avec l'application du RGPD.

Il est donc essentiel que la directive NIS 2 ne fasse pas l'objet de surtransposition tant au niveau de la loi de transposition que de ses décrets d'application.

Il est également important que les options retenues pour transposer la directive NIS 2 soient proportionnées eu égards aux objectifs fixés par la directive NIS 2.

Dans cette perspective, les entités auditionnées par la CSNP recommandent d'impliquer davantage les collectivités territoriales et les acteurs du secteur privé dans le processus de transposition afin de s'assurer que les nouvelles exigences seront proportionnées et réalistes.

La CSNP salue le travail de consultation des parties prenantes mené par l'ANSSI à partir de l'automne 2023. Toutefois, la restitution de ces consultations organisée en avril 2024 n'a pas complètement dissipé les questionnements ou les craintes de l'ensemble de ces acteurs. Une approche collaborative est indispensable pour maintenir la compétitivité des entreprises françaises tout en garantissant un cadre de cybersécurité cohérent et efficace à l'échelle européenne.

Les membres de la CSNP considèrent que la loi de transposition de la directive NIS 2, en renvoyant certaines mesures de transposition au pouvoir réglementaire, ne permet pas au législateur de vérifier si *in fine* la directive NIS 2 ne sera pas surtransposée.

Recommandation n°13 : Respecter le principe de subsidiarité et promouvoir une approche harmonisée au niveau de l'Union européenne dans la transposition de la directive NIS 2 afin de faciliter la conformité pour les entreprises opérant à l'échelle européenne et d'éviter l'apparition de différentiels de régulation pouvant créer des effets de concurrence entre les législations européennes.

V. UN ACCOMPAGNEMENT NECESSAIRE DES NOUVELLES ENTITES

L'élargissement considérable du périmètre des entités qui seront soumises aux dispositions de la directive NIS 2 suppose un accompagnement approprié des entités potentiellement concernées.

En effet, jusqu'à présent les 600 entités couvertes par la directive NIS 1 disposaient de structures, d'équipes et de moyens dédiés nécessaires pour se conformer aux dispositions de la directive NIS 1.

Le profil des entités qui seront soumises aux dispositions de la directive NIS 2 sera sensiblement différent : certaines entités disposeront de moyens comparables tandis que d'autres seront bien moins préparées et dotées en ressources humaines, techniques et financières.

Au-delà des coûts, c'est la possibilité même de trouver des personnels suffisamment qualifiés pour mettre en œuvre ces dispositions qui est questionnée dans certaines régions où les ressources humaines sont rares et les contraintes salariales liées aux grilles indiciaires de la fonction publique territoriale inadaptées au marché de l'emploi.

L'ANSSI indique, dans le projet d'étude d'impact, qu'elle utilisera des relais, notamment sectoriels, qui faciliteront les échanges d'information avec les entités régulées. Les membres de la CSNP appellent l'ANSSI à ne pas sous-évaluer la disparité de situation et d'expertise selon les territoires.

En effet, certains territoires ne disposent tout simplement pas des ressources humaines ou des prestataires compétents en matière de cybersécurité pour accompagner les nouvelles entités essentielles ou importantes au sens de la directive NIS 2.

Il apparaît donc essentiel de prévoir un accompagnement de ces entités. Pour les membres de la CSNP, cet accompagnement passe par un renforcement de la présence de l'ANSSI en région, par la clarification du rôle des CSIRT régionaux dont plusieurs acteurs ont fait part des limites de leur efficacité quant à l'accompagnement des entités dans les territoires, et par la montée en puissance

du dispositif *cybermalveillance.gouv.fr*, mais aussi par la mise en place de procédures simplifiées et de guide de bonnes pratiques.

La CSNP attend un certain nombre de clarifications sur les moyens et l'organisation que mettra en œuvre l'ANSSI pour répondre à la charge supplémentaire significative à laquelle l'organisation va devoir faire face dès lors que la directive NIS 2 entrera en vigueur.

Enfin, la CSNP demande que les acteurs, relais opérationnels du terrain, soient rapidement et de manière transparente identifiés par l'ANSSI. Le réflexe de faire systématiquement appel au secteur privé ne doit en aucun cas être la règle unique dans les territoires.

- **Faciliter la déclaration des incidents**

Lors des auditions, de nombreux acteurs ont fait part de leurs inquiétudes quant à la surcharge administrative que pourrait représenter la déclaration d'un incident cyber. En effet, la majorité des entités qui seront concernées par NIS 2 doivent déjà déclarer un certain nombre d'incidents auprès de plusieurs acteurs tels que la CNIL. Aussi, la CSNP formule deux recommandations afin de simplifier ces démarches, dans un souci d'efficacité et de gain de temps.

<u>Recommandation n°14 :</u> Mettre en place un guichet unique pour déclarer les incidents en élargissant les fonctionnalités de la plateforme 17Cyber.

<u>Recommandation n°15 :</u> Uniformiser les formulaires de remontées d'incidents.

- **Maitriser les effets de bord et alerter sur les effets d'aubaine**

Il est nécessaire que le législateur prenne des dispositions afin d'alerter les entités nouvellement régulées par la directive NIS 2 et qui auraient un faible niveau de maturité et de connaissance en termes de cybersécurité sur les effets d'aubaine pour certains organismes, tels que les cabinets de conseil et assureurs car comme pour chaque nouvelle régulation des marchés peuvent s'ouvrir pour certains acteurs et des offres commerciales abusives et trompeuses peuvent émerger.

- **Accompagnement par l'ANSSI**

Passant de 600 entités concernées par la directive NIS 1 à 15 000 entités environ concernées par la directive NIS 2, l'ANSSI sollicite la création de 60 emplois temps plein.

L'ANSSI estime que son organisation actuelle est dimensionnée pour entretenir une relation de relative proximité avec les 600 OIV et les OSE mais que « *le changement d'échelle induit par les critères retenus dans la directive NIS 2 ne sera cependant pas répercuté dans les mêmes proportions au sein de l'autorité nationale. Les mécanismes de régulation retenus, et notamment celui consistant à demander aux entités assujetties de se déclarer elles-mêmes auprès de l'autorité nationale, permettront d'alléger la charge de travail administratif de l'autorité. Par ailleurs, l'expérience de plusieurs années d'accompagnement et d'évaluation permet à l'autorité nationale de développer des outils numériques afin d'automatiser une importante partie de la relation avec les assujettis, ce qui limitera également le besoin de renfort en effectif. ».*

Les membres de la CSNP ne sont pas pleinement convaincus par cette analyse et préconisent de renforcer la présence de l'ANSSI en région, limitée actuellement à deux seuls ETP par région.

<u>Recommandation n°16 :</u> Renforcer la présence de l'ANSSI en région.

- **La certification des prestataires privés**

La CSNP souhaite que l'ensemble des prestataires privés qui peuvent intervenir auprès d'une entité soumise à la directive NIS 2 fassent l'objet d'une certification par l'ANSSI selon les qualifications existantes : PACS, PASSI, PRIS, PDIS, PAMS[6]. La CSNP souhaite rappeler que, dans le respect naturellement des règles de concurrence, il est important de faire appel aux différentes entités existantes (tels que le GIP ACYMA cybermalveillance.gouv.fr, les gendarmes pour les actions de sensibilisation, les DSI, les chambres consulaires, etc…) et non uniquement aux seules entreprises privées.

<u>Recommandation n°17 :</u> Certifier par l'ANSSI les prestataires privés susceptibles d'intervenir auprès d'une entité soumise à la directive NIS 2.

- **Clarification du rôle joué par les CSIRT territoriaux**

Les Computer Security Incident Response Team (CSIRT) territoriaux pourraient être une réponse partielle à la présence régionale pour accompagner les entités concernées par la directive NIS 2, notamment celles de petites tailles dans la déclaration et la résolution d'incidents.

Issus d'un projet du plan France Relance en 2021, les CSIRT territoriaux (Computer Security Incident Response Team) sont des centres de réponse aux incidents cyber au plus près des entités implantées sur leurs territoires. Ils traitent les demandes d'assistance des acteurs de taille intermédiaire (ex : PME, ETI, collectivités territoriales et associations) et les mettent en relation avec des partenaires de proximité : prestataires de réponse à incident et partenaires étatiques.

Selon l'ANSSI, l'émergence de ces CSIRT doit permettre de fournir localement un service de réponse à incident de premier niveau gratuit, complémentaire de celui proposé par les prestataires, la plateforme Cybermalveillance.gouv.fr et les services du CERT-FR.

Ces équipes portent également des missions de prévention, sensibilisation et d'accompagnement dans la montée en maturité des acteurs de leurs territoires.

Le dispositif est à ce jour constitué de 13 CSIRT territoriaux, en métropole comme dans les Outre-mer. Toutefois, ce dispositif couvre encore inégalement notre territoire puis que la région Auvergne-Rhône-Alpes et la Corse ne disposent pas de CSIRT. De même, un seul CSIRT (CSIRT-ATLANTIC) couvre l'ensemble des territoires ultramarins.

Si lors des auditions, il en ressort que les CSIRT territoriaux ne seraient pas adaptés pour la remontée des incidents cyber, ils pourraient avoir un rôle à jouer dans la réponse aux incidents.

Aussi, pour les membres de la CSNP, il paraît important de préciser le positionnement des CSIRT régionaux et sectoriels dans le dispositif d'accompagnement du projet de loi. Les membres de la

[6] https://cyber.gouv.fr/referentiels-dexigences-pour-la-qualification

CSNP ne souhaitent pas une surtransposition de la directive NIS 2 mais considèrent que l'adoption de la loi pourrait être l'occasion de clarifier le rôle des CSIRT régionaux dans le dispositif français de la cybersécurité. Le financement national des CSIRT régionaux prendra fin en 2024, les régions prenant le relai : la question de la consolidation et de la pérennité des écosystèmes cyber régionaux se pose donc de manière urgente.

Recommandation n°18 : Clarifier le rôle des CSIRT territoriaux dans la transposition de NIS 2.

Recommandation n°19 : Créer une mission d'information parlementaire sur le rôle, le fonctionnement et le financement des CSIRT régionaux et sectoriels.

- **Montée en puissance du dispositif cybermalveillance.gouv.fr**

Le dispositif *cybermalveillance.gouv.fr* mis en place en 2017 avec le GIP ACYMA semble recueillir la confiance des usagers, des collectivités locales et des entreprises d'après nos auditions. Comme le préconise le rapport de la Cour des comptes de mars 2022, une montée en puissance et un renforcement des moyens du dispositif, à budget constant depuis des années alors que ses missions se renforcent et les sollicitations se multiplient, serait de nature à combler la « diagonale du vide » dont souffrent certains territoires.

Recommandation n°20 : Allouer des crédits supplémentaires au SGDSN dans le cadre du programme 129 lors du PLF pour 2025, crédits qui seront fléchés vers le GIP ACYMA.

Recommandation n°21 : Accompagner financièrement les entités ne disposant pas des moyens nécessaires à leur mise en conformité.

- **Nécessité d'un accompagnement spécifique des collectivités locales**

Les collectivités territoriales rencontrent des difficultés spécifiques dans la mise en œuvre de la directive NIS 2. Les petites communes, en particulier, sont moins préparées et ne disposent pas des ressources nécessaires pour se conformer aux exigences imposées aux entités essentielles.

Les associations d'élus ont été sensibilisées aux problèmes de cybersécurité par l'ANSSI, mais un écart significatif persiste entre les petites et grandes collectivités. La CSNP constate qu'un travail de pédagogie et de sensibilisation sera nécessaire vis-à-vis des collectivités dont la très large majorité se sent encore très éloignée des enjeux cyber alors qu'elles sont souvent la cible privilégiée de cyberattaques.

Les collectivités, et notamment les communautés de communes, s'inquiètent également de la mise en jeu de leurs responsabilités en cas de non-conformité des systèmes d'information des petites communes ou de leurs prestataires externes. En effet, il y a une incertitude sur la responsabilité en cas de non-conformité des prestataires aux exigences de la directive NIS 2. Elles demandent des clarifications sur les rôles et les responsabilités, et une meilleure collaboration avec les structures régionales.

La question des ressources humaines et financières est évidemment cruciale pour les collectivités. Les collectivités font face à une concurrence du secteur privé pour le recrutement de

talents en cybersécurité, compliquée par les grilles salariales de la fonction publique. La CSNP recommande de mettre l'accent sur les formations, y compris interne, et sur la reconversion.

S'agissant des formations en cybersécurité, un référentiel de formations en cybersécurité pour les entités publiques mais également privées pourrait être intégré au Répertoire national des compétences professionnelles. Ce référentiel des compétences minimales en matière de sécurité numérique pourrait être facilement constitué par l'ANSSI.

De manière générale, un débat sur le budget dotation pour les collectivités devra être engagé au Parlement puisque ces dernières ne cessent de voir leurs dotations baisser alors que la mise en œuvre de cette directive sera, à n'en point douter, très couteuse.

Par ailleurs, il nous faudra soutenir les actions des collectivités à inclure des clauses cyber face à des centrales d'achats pas toujours adaptées aux collectivités et face aux critères d'appels d'offres. La question des contrats en cours qui ne respecteraient pas les conformités cyber imposées par la directive NIS 2 se pose.

Les centrales d'achat comme l'UGAP peuvent jouer un rôle de levier important dans le relèvement du niveau de sécurité numérique des collectivités locales.

Évoquer le niveau de maturité cyber des collectivités à travers les choix effectués auprès des éditeurs de logiciels peut s'avérer une approche intéressante. En effet, la vulnérabilité de certaines collectivités peut varier selon qu'elles ont choisi une solution dite SaaS (« *Software as a Service* ») ou *on-premise* pour leurs logiciels. De nombreuses collectivités choisissent d'avoir leurs logiciels *on-premise,* à savoir hébergées et maintenus par le propre service informatique de la collectivité. Or, force est de constater que faute de temps ou de ressources humaines nécessaires, les mises à jour peuvent être effectuées dans un certain délai, voire pas du tout, exposant ainsi ces collectivités aux risques cyber. Le choix du mode dit SaaS présente à cet égard plusieurs avantages dont celui d'être hébergé dans le cloud et exploité en dehors de la collectivité par le fournisseur de service, permettant ainsi de conserver un meilleur niveau de cybersécurité même si l'actualité récente a démontré que cette solution ne présentait pas un niveau de sécurité absolu.

Reprenant l'esprit d'une recommandation de l'avis n°2023-06 du 12 septembre 2023 de la CSNP sur la souveraineté numérique, la CSNP pose à nouveau le rôle que les préfets pourraient jouer dans la mise en conformité à NIS 2 des collectivités.

<u>Recommandation n°22 :</u> Faire auditer par l'ANSSI le degré de maturité des collectivités locales qui seront soumises à la directive NIS 2 et en mesure de se conformer au calendrier de mise en œuvre. Un accompagnement spécifique, technique et financier sera prévu pour celles n'ayant pas les moyens nécessaires. La mobilisation des financements de la stratégie nationale d'accélération cyber vers des outils intégrés conformes aux exigences posées par l'ANSSI doit être étudiée.

<u>Recommandation n°23 :</u> Introduire plus de progressivité dans la mise en œuvre de la directive NIS 2 et réaliser une étude d'impact plus précise pour qualifier les risques, les menaces et les coûts financiers, administratifs, démocratiques des cyberattaques pesant sur les collectivités territoriales. Les membres de la CSNP appuient les demandes des collectivités territoriales exprimées en ce sens.

<u>Recommandation n°24 :</u> Inciter les collectivités, notamment celles qui n'ont pas les moyens humains nécessaires, à faire le choix d'une solution dite SaaS afin de maintenir le meilleur niveau de cybersécurité possible.

<u>Recommandation n°25 :</u> Renforcer le rôle des préfets dans l'accompagnement des collectivités à se conformer aux obligations de la directive NIS 2.

VI. DES ENJEUX SPECIFIQUES POUR CERTAINS SECTEURS ECONOMIQUES

Au cours des auditions qui ont été conduites, les membres de la CSNP ont pu observer des attentes particulières de certains acteurs économiques à l'égard de la transposition de la directive NIS 2.

- **Le secteur de la santé**

La mise en œuvre de la directive NIS 2 dans le secteur de la santé présente plusieurs enjeux majeurs. Tout d'abord, elle intervient après la transposition de la directive NIS 1, du RGPD et des modifications du code de santé publique. Les professionnels de santé appréhendent la création d'une couche de complexité supplémentaire aux exigences déjà multiples qui leur sont imposées. Le changement d'échelle de la directive NIS 2 passe notamment par le fait que tous les services d'information du secteur de la santé seront désormais concernés, nécessitant la mise en œuvre de moyens considérables.

Les établissements de santé ont des systèmes d'information autonomes et diversifiés : ils auront donc à harmoniser leurs pratiques. Ceci représente un défi d'autant plus grand que tous les établissements de santé ne disposent pas des ressources financières et humaines suffisantes.

La directive NIS 2 constitue sans nul doute un levier puissant pour encourager la mutualisation et renforcer la sécurisation de l'ensemble de la chaîne de valeur, des fournisseurs de médicaments aux systèmes internes.

S'agissant des délais de transposition, il apparait crucial d'aménager des délais de mise en conformité et de prévoir des dispositifs d'accompagnement, en particulier pour les petits établissements dépourvus de RSSI ou de DSI, afin de garantir une adoption efficace et pérenne de la directive NIS 2.

Les entreprises de dispositifs médicaux réunies au sein du SNITEM ont attiré l'attention de la CSNP sur la qualification d'entités essentielles de certaines entreprises de dispositifs médicaux en cas de crise sanitaire. En cas de crise sanitaire, il sera difficilement envisageable de passer, pour ces entreprises, du statut d'entité importante à celui d'entité essentielle et de relever immédiatement le niveau supplémentaire attendu pour une entité essentielle.

<u>Recommandation n°26 :</u> Prévoir un accompagnement financier des acteurs les plus fragiles afin que la mise en œuvre de la directive NIS 2 constitue un levier puissant pour encourager la mutualisation et renforcer la sécurisation des systèmes d'information des acteurs de la santé.

<u>Recommandation n°27 :</u> Renforcer la concertation entre l'ANSSI, le ministère de la Santé et les entités du secteur de la santé potentiellement concernées par un relèvement de leur statut d'entité importante à entité essentielle en cas de crise sanitaire sur les mesures adaptées et proportionnées à mettre en place.

- **Le secteur des assurances**

France Assureurs a souhaité attirer l'attention des membres de la CSNP sur l'articulation de la directive NIS 2 avec le règlement Digital Operational Resilience Act (DORA).

Le règlement DORA entrera en vigueur en janvier 2025 et a vocation à constituer le cadre légal en matière de cyberrésilience applicable au secteur financier dont fait partie le secteur de l'assurance. Ce règlement prévoit un cadre de gestion des risques cyber et la notification des incidents majeurs à l'ACPR, ainsi que la réalisation de programmes de tests de résilience.

France Assureurs craint que les assureurs ne soient à la fois soumis à la directive NIS 2 et au règlement DORA ce qui engendrerait une insécurité juridique alors qu'il est admis au niveau européen que DORA a un effet au moins équivalent à la directive NIS 2. Si certaines dispositions de la directive NIS 2 devaient s'appliquer aux assureurs, cela entrainerait *de facto* des coûts pour les assureurs français par rapport à leurs concurrents européens et les soumettraient à une double supervision : celle de l'ANSSI et de l'ACPR.

Recommandation n°28 : Préciser le régime applicable au secteur des assurances en application de la *lex specialis* pour lever les risques de double régulation entre la directive NIS 2 et le règlement DORA.

- **Le cas des sous-traitants et des éditeurs de logiciels**

Le projet de loi transposant la directive NIS 2 impose la protection des réseaux et systèmes d'information, y compris en cas de recours à la sous-traitance.

Cette extension aux sous-traitants interroge et inquiète. En effet, de nombreux représentants des entités essentielles ou importantes considèrent qu'ils ne disposent d'une vision ni partielle ni complète de leurs fournisseurs et sous-traitants.

Combinée au nouveau pouvoir de sanction qui est conféré à l'ANSSI, cette disposition fait craindre aux entités concernées qu'elles pourront être mises en cause pour des défaillances observées chez leurs sous-traitants. Pour anticiper et se prémunir ces défaillances, les entités essentielles et importantes vont devoir entamer un lourd et long travail de révision des contrats qui les lient à leurs fournisseurs et sous-traitants qui pourraient, selon certains juristes, prendre plus de deux ans à l'échelle nationale.

Les éditeurs de logiciels font face, quant à eux, à des défis particuliers, notamment en ce qui concerne la mise en œuvre des audits de conformité. La nécessité de réaliser ces audits par des sous-traitants représente une charge considérable pour les grandes entreprises et encore plus pour les petites entreprises qui pourraient être totalement dépassées par les coûts et les ressources nécessaires. Il leur parait essentiel de clarifier les rôles et les devoirs des éditeurs envers les entités qu'ils assistent, notamment les collectivités locales, et de distinguer les exigences selon les types de données protégées.

Recommandation n°29 : Intégrer dans le texte de transposition de la directive NIS 2 la nécessité pour les entités essentielles et importantes de modifier les obligations contractuelles qui les lient à leurs sous-traitants.

- **Le cas des noms de domaines**

Les noms de domaines (DNS) étaient déjà concernés par la directive NIS1, mais pas les bureaux d'enregistrement. Ces derniers sont toutefois désormais concernés par la directive NIS 2. Des clarifications sur le périmètre de l'article 28 de la directive semblent nécessaires afin de ne pas créer de ruptures d'égalité entre les bureaux d'enregistrement européens et extra européens.

Recommandation n°30 : Préciser dans la loi le périmètre de l'article 28 de la directive NIS 2 relatif à la base des données d'enregistrement des noms de domaine.

VII. UN DISPOSITIF DE SANCTIONS INEDIT

De manière inédite, la directive NIS 2 prévoit l'instauration de diverses sanctions administratives en cas de non-respect des dispositions qu'elle introduit. Ces sanctions prennent, selon les cas, la forme d'amendes administratives, d'astreintes, de suspensions de certaines activités ou d'interdictions temporaires d'exercice des responsabilités du dirigeant de l'entité concernée, de l'abrogation d'une certification, d'une qualification ou d'une autorisation.

La CSNP salue le choix retenu, parmi les trois options possibles pour l'établissement d'une autorité de sanctions évoquées lors de l'élaboration du projet de loi, de créer un collège *ad hoc* et indépendant. Composée de magistrats du Conseil d'État, de la Cour de cassation et de la Cour des comptes, ainsi que de personnalités qualifiées, cette instance est de nature à rassurer les professionnels du droit et les parties prenantes sur l'indépendance de cette commission vis-à-vis de l'ANSSI qui exerce les fonctions de conseil et de superviseur.

Le projet de loi précise les modalités de la supervision et de la constatation des manquements et confie à ladite commission des sanctions la faculté de décider dans chaque cas d'un montant individualisé, proportionné à la gravité des faits dans la limite du niveau maximum à savoir 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial hors taxes ou 7 millions d'euros ou 1,4 % du chiffre d'affaires annuel mondial hors taxes en fonction des entités concernées.

La création de cette commission indépendante permettra également de ne pas dénaturer le rôle de l'ANSSI qui est avant tout d'accompagner les entités françaises, répondant ainsi à de nombreuses inquiétudes soulevées par de nombreuses entités auditionnées.

Par ailleurs, ce dispositif permettra de pérenniser la confiance des entités en l'ANSSI. Si cette dernière devait se doter du pouvoir de sanction, il aurait été à craindre que certaines entités puissent être frileuses à l'idée de faire part à l'ANSSI de certaines failles de cybersécurité.

La CSNP tient cependant à appeler l'attention de la future commission des sanctions sur deux aspects :

- Premièrement, bien qu'il ne faille pas négliger l'effet dissuasif du risque de sanction, incitant fortement les entités concernées par la directive à s'y conformer, la CSNP abonde dans le sens de l'ANSSI qui ne souhaite pas voir les collectivités être soumises à des sanctions en cas de non-conformité. Comme évoqué précédemment, l'accompagnement des collectivités dans la mise en conformité sera un véritable enjeu de l'application de cette directive.

- Enfin, la CSNP recommande, compte tenu des délais de mise en conformité pour l'ensemble des entités concernées, une certaine souplesse dans l'appréciation des infractions aux obligations jusqu'au 31 décembre 2027.

<u>Recommandation n°31</u> *<u>(en cas d'évolution du projet de loi)</u>* : Faire le choix de déléguer à une commission *ad hoc* et indépendante le pouvoir de sanctions en cas de non-respect des obligations introduites par la directive.

<u>Recommandation n°32</u> : Accorder une certaine souplesse dans l'appréciation des infractions aux obligations et les sanctions relatives jusqu'au 31 décembre 2027.

LISTE DES PERSONNES AUDITIONNÉES

(par ordre alphabétique)

ADF (Assemblée des départements de France)

- M. Jean-Baptiste ESTACHY, conseiller sécurité

ADN Ouest

- M. Franz JARRY, délégué général

AFNIC (Association française pour le nommage Internet en coopération)

- M. Pierre BONIS, directeur général
- M. Régis MASSÉ, directeur des systèmes d'information et directeur technique

AFNUM (Alliance française des industries du numérique)

- Mme Stella MORABITO, déléguée générale
- M. Léo LAFARGE, chargé de mission politiques numériques

AMF (Association des Maires de France)

- M. Patrick MOLINOZ, co-président de la commission du numérique
- Mme Véronique PICARD, chargée de mission numérique

ANSSI (Agence nationale de la sécurité des systèmes d'information)

- M. Vincent STRUBEL, directeur général
- Mme Jennyfer CHRÉTIEN, directrice de cabinet

APSSIS (Association pour la sécurité des systèmes d'information de santé)

- M. Vincent TRELY, président fondateur

ARPEGE

- M. Grégoire BINET, directeur des systèmes d'information
- Mme Julie LE TRAON, déléguée à la protection des données, responsable équipe contrats et marchés publics
- M. Nathanaël VERON, responsable de la sécurité des systèmes d'information

AVICCA (Association des villes et collectivités pour les communications électroniques et l'audiovisuel)

- M. Ariel TURPIN, délégué général
- M. Guilhem DENIZOT, chargé de mission juridique et réglementaire

AWS

- M. Stephan HADINGER, directeur de la technologie chez AWS France
- M. Arnaud DAVID, directeur des Affaires publiques

BERGER LEVRAULT

- M. Jérôme BONNET, directeur de la technologie, membre du comité exécutif
- M. Alain DUWEZ, responsable de la sécurité des systèmes d'information
- Mme Valérie REINER, directrice des Affaires publiques

Centre pour la Cybersécurité Belgique :

- M. Dirk DE PAEPE, CCB Certification Service, Centre for Cybersecurity Belgium
- M. Stephan ANDRE, service juridique du CCB
- M. Nathanaël ACKERMAN, Head of AI4Belgium - Digital Minds Unit
- M. Taco MULDER, directeur général BOSA

CDSE (Club des directeurs de sécurité des entreprises)

- M. Émile PEREZ, vice-président, directeur de la sécurité et de l'intelligence économique du groupe EDF
- M. Florent JANSSEN, chargé de mission

Cigref (Club informatique des grandes entreprises françaises)

- M. Jean-Claude LAROCHE, président, directeur de mission auprès du Président d'ENEDIS
- M. Henri d'AGRAIN, délégué général

CLOUD TEMPLE

- M. Nicolas ABRIOUX, responsable Gouvernance de la Sécurité
- Mme Laure MARTIN-TERVONEN, directrice des Affaires publiques

Club des RSSI de Santé

- M. Jean-Sylvain CHAVANNE, secrétaire général

CPME (Confédération des petites et moyennes entreprises)

- M. Marc BOTHOREL, référent cybersécurité
- M. Jérôme NORMAND, économiste
- M. Adrien DUFOUR, responsable des Affaires publiques

Cybercercle

- M. Philippe LOUDENOT, senior advisor & cybersecurity strategist, délégué à la protection des données
- M. Christian DAVIOT, senior advisor

DOCAPOSTE

- M. Guillaume POUPARD, directeur général adjoint
- Mme Fanny LANNOY, responsable des Affaires publiques

EGERIE

- M. Jean LARROUMETS, président fondateur
- Mme Marie AUDREN, directrice des Affaires publiques

EY

- M. Marc AYADI, associé chargé des expertises cyber, technologiques et data pour la France
- M. Fabrice NAFTALSKI, avocat associé chargé du droit du numérique, de protection des données personnelles et de la propriété

FFTélécoms (Fédération française des télécoms)

- M. Patrick GUYONNEAU, président de la commission sécurité de la FFT et Directeur de la sécurité du groupe Orange
- M. Alexandre GALDIN, directeur délégué à la sécurité

FIEEC (Fédération des industries électriques, électroniques et de communication)

- Mme Aridge KHAYATI, chargée d'Affaires publiques

FNCCR (Fédération nationale des collectivités concédantes et régies)

- M. Jean-Luc SALLABERRY, chef du département numérique

France Assureurs

- Mme Mélodie LELOUP-VELAY, directrice Droit et Conformité
- Mme Olympia FEKETE, responsable d'études juridiques
- Mme Viviana MITRACHE, directrice des Affaires publiques France
- M. Arnaud GIROS, responsable Affaires parlementaires et gouvernementales
- Mme Anne-Marie PAPEIX, responsable RC Médicale, RC et Environnement

GOOGLE cloud

- M. Thiébaut MEYER, directeur des stratégies de cybersécurité
- M. Frédéric GIRAUD de LESCAZES, directeur des Affaires publiques

HEXATRUST

- M. Jean-Noël de GALZIN, président fondateur, président fondateur de Wallix
- Mme Dorothée DECROP, déléguée générale
- M. Armand NOURY, directeur conseil influence d'Agence Proches

HUAWEI

- M. Minggang ZHANG, directeur général adjoint de Huawei France
- Mme Myriam LAGARDE, directrice des Affaires institutionnelles de Huawei France

Intercommunalités de France

- Mme Marlène LE DIEU DE VILLE, vice-Présidente de la commission numérique
- M. Clément BAYLAC, conseiller économie et attractivité, numérique et commerce

Iteanu Associés

- Maître Alexandra ITEANU, avocate, responsable du pôle data et RGDP au cabinet Iteanu

MEDEF (Mouvement des entreprises de France)

- Mme Maxence DEMERLÉ, directrice du numérique
- M. Alexis KASBARIAN, responsable du pôle transition numérique et innovation
- Mme Mathilde BRIARD, chargée de mission économie numérique

MICROSOFT

- M. Lionel BENATIA, directeur senior des Affaires gouvernementales
- M. Marc GARDETTE, directeur technique adjoint

NUMEUM

- Mme Nolwenn LE STER, présidente de la commission cybersécurité, directrice des activités cybersécurité chez Capgémini
- M. Paul PASTOR, délégué aux Affaires publiques et cybersécurité
- M. Clément EMINE, délégué aux Affaires publiques

ONE POINT

- M. Alexis BOUIN, expert cybersécurité
- M. Vincent CHRIQUI, conseiller du président

OUTSCALE 3DS

- M. Grégory ABATE, secrétaire général de Dassault Systèmes
- M. David CHASSAN, directeur de la Stratégie

OVHCloud

- M. Julien LEVRARD, responsable de la sécurité informatique
- Mme Blandine EGGRICKX, responsable des Affaires publiques

Régions de France

- Mme Sinaa THABET, conseillère développement économique, recherche, innovation et numérique

Renaissance Numérique

- Mme Rayna STAMBOLIYSKA, présidente, RS Strategy
- M. Samuel LE GOFF, vice-président, consultant chez Commstrat

SCALEWAY

- Mme Ombeline BARTIN, directrice des Affaires publiques d'Iliad
- Mme Naphsica PAPANICOLAOU, chargée d'Affaires publiques d'Iliad

Service économique de Bruxelles

- M. Arnaud BELLANGER, chef du service
- M. Andri RABEHANTA, adjoint au chef du Service économique

WAVESTONE

- M. Pascal IMBERT, président directeur général et co-fondateur
- M. Gérôme BILLOIS, associé cybersécurité et confiance du numérique, chargé de la gestion des risques numériques, des situations de crises et d'innovation cyber

Contributions écrites

(par ordre alphabétique)

ACN (Alliance pour la confiance numérique)

CESIN (Club des experts de la sécurité de l'information et du numérique)

SNITEM (Syndicat national de l'industrie des technologies médicales)

Renaissance Numérique

BIOGRAPHIES

M. Damien MICHALLET

Elu Sénateur (Les Républicains) de l'Isère en septembre 2023, **M. Damien Michallet** est engagé depuis plusieurs années dans la stratégie et l'aménagement numérique de nos territoires au service de nos concitoyens et de nos entreprises, pendant 8 ans à la Communauté d'Agglomération de Porte de l'Isère en tant que Vice-Président en charge de la stratégie du numérique, et en tant que Vice-président du Département de l'Isère délégué à l'aménagement numérique et aux systèmes d'information. Membre de l'AVICCA, M. Damien Michallet, a rejoint le Groupe d'Etudes "Numérique" du Sénat présidé par M. Patrick Chaize, Sénateur de l'Ain et dont il a été élu Vice-président le 30 janvier dernier.

Mme Anne LE HENANFF

Mme Anne Le Hénanff, députée au Parlement français, a été élue pour la première fois députée en Juin 2022 et appartient au parti Horizons. Elle est membre de la Commission supérieure du numérique et des postes depuis 2022. Elle siège à la Commission de la défense et des forces armées à l'Assemblée nationale. Elle était également vice-présidente du groupe de travail sur l'économie numérique, la sécurité et la souveraineté. Elue à Vannes depuis 2008, elle a été première adjointe au maire en charge du Numérique et conseillère communautaire en charge du numérique à Golfe du Morbihan Vannes agglomération. Elle est l'auteure en 2023 d'un rapport sur les défis de la cyberdéfense et a été rapporteur sur le titre relatif au Cloud pour la loi Sécuriser et réguler l'espace numérique à l'Assemblée nationale.

CSNP
COMMISSION SUPÉRIEURE DU NUMÉRIQUE ET DES POSTES

100, rue Richelieu
75002 PARIS
Tel : 06.84.40.91.95.
contact@csnp.fr

@CSNUMPOST CSNP https://csnp.fr

COMMISSION SUPÉRIEURE DU NUMÉRIQUE ET DES POSTES

AVIS N° 2024-08 DU 28 NOVEMBRE 2024

« POUR UNE POLITIQUE NATIONALE D'INCLUSION NUMERIQUE

ADAPTEE AUX BESOINS DE NOS CONCITOYENS »

L'égalité de droits de nos concitoyens est un des principes fondamentaux de la République auquel les membres de la Commission supérieure du numérique et des postes sont particulièrement attachés. Le développement du numérique dans la société française et la numérisation des services publics et marchands constituent une évolution majeure, porteuse de nombreuses opportunités et à laquelle les français adhèrent massivement.

Pour autant, cette numérisation qui n'a fait que se renforcer après la crise du COVID, laisse sur le bord du chemin près d'un quart des français : le dernier Baromètre du numérique établi par le Credoc sur ce sujet estime que 25% des Français ne maîtrisent pas suffisamment les outils numériques pour les utiliser pleinement.

Cet éloignement du numérique d'une partie de nos concitoyens est une préoccupation constante de la CSNP qui avait formulé en décembre 2022 des recommandations pour renforcer la politique nationale d'inclusion numérique, recommandations qui avait été partiellement reprises en 2023 avec le lancement du dispositif Numérique Ensemble par M. Jean-Noël Barrot, alors ministre délégué en charge du numérique.

Fin septembre, les membres de la CSNP ont confié à M. Christian Redon-Sarrazy, Sénateur de la Haute-Vienne, et à Mme Jeanne Bretécher, personnalité qualifiée auprès de la CSNP, la mission d'évaluer le dispositif « Numérique ensemble » et, le cas échéant, de formuler des recommandations pour s'assurer que la politique d'inclusion numérique était adaptée aux publics les plus fragiles mais également pour que des solutions alternatives soient mises en place pour garantir l'accès aux droits de la totalité de nos concitoyens, notamment ceux qui ne peuvent ou ne souhaitent pas accéder aux services publics en ligne.

Dans le cadre de la mission qui lui a été confiée, le groupe de travail piloté par M. Christian Redon-Sarrazy et Mme Jeanne Bretécher a auditionné Mme Clara Chappaz, Secrétaire d'Etat pour l'intelligence artificielle et le numérique, des représentants de l'Etat et de l'Agence nationale de cohésion des territoire (ANCT), la défenseur des droits, des représentants des collectivités départementales et communales, de l'Association des maires de France et d'intercommunalités de France, de la Banque des territoires, de la MedNum, des représentants des centres sociaux et des missions locales pour l'emploi, des acteurs impliqués dans l'inclusion numérique (conseillers numériques, associations, entreprises).

Lorsque les membres de la CSNP leur ont confié cette mission, le projet de loi de finances 2025 n'avait pas encore été rendu public et la coupe budgétaire drastique des crédits alloués à l'inclusion numérique n'était pas encore connue : le gouvernement a en effet décidé de diminuer les crédits dédiés à l'inclusion numérique de 56% en n'allouant que 27 millions d'euros au dispositif des conseillers numériques contre 62 millions d'euros alloués en 2024.

Cette annonce a suscité, à juste titre, l'indignation des acteurs de l'inclusion numérique et des collectivités locales : alors que le dispositif des conseillers numérique a démontré son efficacité et que la feuille de route Numérique Ensemble n'est pas encore complètement mise en œuvre, cette coupe budgétaire va réduire à néant quatre ans d'investissements dont près de 200 millions d'euros mobilisés par l'Etat dans le cadre du plan de relance.

Ce sentiment de gâchis est partagé par l'ensemble des acteurs et les membres de la CSNP appellent au rétablissement des crédits dédiés à l'inclusion numérique à hauteur de 62 millions d'euros en 2025.

Les auditions conduites par M. Christian Redon-Sarrazy et Mme Jeanne Bretécher ont mis en lumière les avancées significatives du dispositif et notamment son appropriation par les acteurs et, surtout, la satisfaction des bénéficiaires du dispositif. Pour autant, le dispositif n'a pas encore atteint ses principaux objectifs, loin s'en faut. Les membres de la CSNP souhaitent donc formuler un certain nombre de recommandations pour améliorer et pérenniser le dispositif :

- **Simplifier et adapter aux usages du grand public la numérisation des services en ligne**

Recommandation n° 1 : Inscrire dans la loi l'obligation d'alternatives aux démarches dématérialisées, avec un accès à un point de contact physique et téléphonique pour accompagner nos concitoyens dans leurs démarches administratives **;**

Recommandation n°2 : Faire respecter le droit à ne pas recourir à une démarche dématérialisée, conformément à l'article L.112-8 du Code des relations entre usagers et administration ;

Recommandation n° 3 : Simplifier les procédures administratives et adapter l'ergonomie et le design des services en ligne des administrations publiques en mettant en place des groupes d'utilisateurs centrés sur les publics spécifiques et précaires pour tester et simplifier l'accès aux droits ;

Recommandation n° 4 : Faire appliquer la loi n° 2005-102 du 11 février 2005 pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées sur l'accès des personnes handicapées aux services en ligne;

Recommandation n° 5 : Former spécifiquement les conseillers numériques à l'accompagnement des personnes en situation de handicap intellectuel ou cognitif ;

Recommandation n° 6 : Mobiliser les nouvelles technologies pour inclure davantage les personnes souffrant de troubles cognitifs et proposer une alternative Facile à Lire et à Comprendre (FALC) pour les sites publics ;

- **Sur le financement du dispositif d'inclusion numérique**

Recommandation n°7 : Rétablir les crédits dédiés à l'inclusion numérique à hauteur de 62 millions d'euros dans la loi de finances 2025 ;

Recommandation n°8 : Anticiper un plan de financement de long terme pour assurer la continuité des initiatives et éviter les effets d'une politique de « stop and go » comme dans le cas des conseillers numériques ;

Recommandation n°9 : Créer le fonds national d'inclusion numérique qui permettra d'agréger les financements publics, les financements privés et les fonds européens encore insuffisamment mobilisés ;

Recommandation n°10 : Renforcer le rôle de la Banque des Territoires en ingénierie financière et dans la mobilisation de financements privés et européens pour l'inclusion numérique ;

Recommandation n°11 : Instituer une taxe "numériseur-payeur" ciblant les entreprises du numérique et les services marchands proposant des services dématérialisés **;**

Recommandation n°12 : Flécher des recettes issues des sanctions pécuniaires prélevées par l'ARCOM sur la non adaptation de l'accessibilité des sites web aux personnes en situation de handicap vers la politique d'inclusion numérique ;

Recommandation n° 13 : Instituer des conférences financières au niveau départemental ;

Recommandation n°14 : Expérimenter et, le cas échéant, généraliser la mise en place d'un Service d'intérêt économique général (SIEG) d'inclusion numérique par les régions, sur le modèle des Hauts-de-France ;

- **Sur la gouvernance du dispositif et le dispositif Aidants Connect**

Recommandation n°15 : Veiller à assurer une coordination efficace qui tienne compte des actions déjà engagées dans les territoires par l'ensemble des acteurs (conseillers départementaux, communes et intercommunalités, acteurs sociaux et associatifs) ;

Recommandation n°16 : Clarifier le statut Aidants Connect en précisant la responsabilité de l'Etat et en étudiant le statut de "bénévole aidant numérique » qui permettrait aux associations d'accompagner les personnes via Aidants Connect ;

- **Sur le développement d'une filière de reconditionnement économiquement viable**

Recommandation n°17 : Massifier les dons de matériel des administrations publiques, des entreprises et des particuliers aux associations et entreprises de reconditionnement ;

Recommandation n°18 : Renforcer les ressources du Fonds Reconditionnement pour développer une chaîne de valeur solidaire et durable au bénéfice des organisations de l'Économie sociale et solidaire ;

- **Sur la formation et la structuration d'une véritable filière de l'inclusion numérique**

Recommandation n°19 : Intégrer les enjeux de citoyenneté numérique et l'usage d'outils libres dans les parcours scolaires ;

Recommandation n° 20 : Sensibiliser les étudiants des cursus universitaires aux enjeux sociétaux, d'inclusion et de sécurité numérique ;

Recommandation n° 21 : Former les travailleurs sociaux en poste sur le rôle des algorithmes dans l'accès aux droits ;

Recommandation n° 22 : Former les intermédiaires du secteur médico-social, de l'action sociale, et de l'éducation populaire à l'accompagnement numérique des publics et veiller à ce que les formations aux compétences professionnelles spécifiques à l'inclusion numérique soient intégrées systématiquement dans les catalogues des 11 opérateurs de compétences (OPCO).

I. La fracture et l'éloignement numérique : un obstacle majeur à l'exercice des droits de nos concitoyens

La notion d'inclusion numérique comporte plusieurs dimensions et sans doute une part de subjectivité : la perception de chacun sur ses propres aptitudes à utiliser des instruments et des services numériques peut varier d'un individu à l'autre.

Le recensement des personnes éloignées du numérique est donc un exercice difficile et les résultats des différentes enquêtes menées sur ce sujet doivent sans doute être relativisés.

Au vu des études conduites sur ce sujet depuis plusieurs années, il est pourtant possible d'établir que 20 à 25% de nos concitoyens se considèrent éloignés des usages du numérique.

A l'occasion du Plan national pour un numérique inclusif lancé par Mounir Mahjoubi en 2018, le Baromètre du Numérique évaluait à 13 millions de français le nombre de nos concitoyens qui utilisaient peu ou pas Internet et se sentaient en difficulté avec les usages du numérique.

Au printemps 2024, le Baromètre du numérique du Crédoc[1] indique que 25% des Français ne maîtrisent pas suffisamment les outils numériques pour les utiliser pleinement.

Force est de constater que cette proportion de nos concitoyens qui ne maîtrisent peu ou pas les outils du numérique ne diminue pas sensiblement même si les français possèdent et utilisent massivement des outils numériques au premier rang desquels le téléphone portable :

- 87% des Français détiennent un smartphone,
- 80% des français utilisent une messagerie instantanée mobile
- 85% d'entre eux utilisent la navigation internet mobile.

Pour les membres de la CSNP, cette proportion importante des français confrontés à la fracture numérique nécessite de maintenir des points de contact physiques et téléphoniques pour permettre l'accès à l'ensemble des services publics en parallèle d'une politique d'inclusion numérique ambitieuse.

Il en va de l'égalité de nos concitoyens dans l'exercice de leurs droits.

Aujourd'hui, une très grande proportion des personnes éligibles aux minima sociaux ne les sollicite pas ou renonce à les solliciter:

- Un foyer éligible sur trois ne demande pas le revenu de solidarité active (RSA). Cela représente 600 000 personnes soit, environ, 3 milliards d'euros d'aides non versées chaque année.
- Une personne seule sur deux est éligible au minimum vieillesse sans le solliciter[2]

Les principales raisons de ce non recours aux droits sociaux sont la méconnaissance des dispositifs et la complexité des démarches administratives pour les obtenir. Le souhait de ne pas dépendre des aides sociales ne représenterait que 16% des personnes éligibles[3].

[1] Baromètre du numérique 2023 - Rapport

[2] Le non-recours au minimum vieillesse des personnes seules DRESS 2016

[3] MS2024.pdf Panorama de la DREES 2024 « Minima sociaux et prestations sociales - Ménages aux revenus modestes et redistribution »

Les membres de la CSNP, comme ils l'avaient déjà recommandé dans leur avis n°2022-08 du 14 décembre 2022[4], considèrent que le maintien d'une présence physique des services publics sur l'ensemble des territoires est essentiel.

Le déploiement des Maisons France Service et des bus France Service représente, de ce point de vue, un progrès important dans le maintien d'une présence physique des services publics dans les territoires.

Il est également essentiel que nos concitoyens puissent contacter les services publics par téléphone.

Sur ce point, en dépit des engagements pris au niveau ministériel et la mise en place du « Plan téléphone » en mai 2023, contacter directement des services publics par téléphone reste un parcours difficile, un objectif plus qu'une réalité ainsi que l'a démontré une étude réalisée par le défenseur des droits : au cours de l'expérience conduite dans le cadre de cette étude, 40 % des appels n'ont pas abouti sur l'ensemble des 4 plateformes testées (CPAM, CAF, Pôle emploi et Carsat) et la durée moyenne d'attente était supérieure à 9 minutes[5].

Une simplification des procédures administratives et une amélioration significative des sites en ligne des administrations publiques est une recommandation formulée depuis plusieurs années, pour ne pas dire plusieurs décennies, sans que les résultats soient atteints de manière satisfaisante.

Nos concitoyens ne peuvent que mesurer l'écart qui se creuse entre les sites en ligne des services marchands qu'ils peuvent utiliser avec une très grande facilité et les sites publics qui ne permettent pas de faire aboutir correctement leurs démarches.

Il s'agit d'un chantier important qui nécessite des moyens considérables alors que les coupes budgétaires se multiplient. La simplification des procédures administratives devrait être une des priorités du Ministre de la fonction publique.

Les membres de la CSNP constatent également qu'en dépit de la loi n° 2005-102 du 11 février 2005 pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées, l'accès des sites internet publics aux personnes handicapées n'est toujours pas appliquée près de vingt ans après l'adoption de la loi (cf. paragraphe VII).

II. Une politique d'inclusion numérique menacée par une coupe budgétaire massive.

Depuis 2020, la politique nationale d'inclusion numérique reposait sur le déploiement de 4000 conseillers numériques et bénéficiait d'un financement de 200 millions d'euros mobilisé dans le cadre du plan de relance décidé en 2020. La CSNP avait déjà eu l'occasion de questionner la pérennité du financement de cette politique et de formuler des recommandations pour améliorer le dispositif en décembre 2022.

Ces recommandations ont été partiellement prises en compte par M. Jean-Noël Barrot, alors ministre en charge de la souveraineté numérique lors de l'adoption de la feuille de route nationale France Numérique Ensemble à l'été 2023.

[4] Avis-n°2022-08-du-14-decembre-2022-sur-le-bilan-des-conseillers-numeriques.pdf
[5] Enquête - L'accueil téléphonique de 4 services publics | Défenseur des Droits

A. Les objectifs et les réalisations du plan “Numérique Ensemble”.

Ce plan a été co-signé par des associations d’élus (Départements de France, l’AMF, l’APVF, Intercommunalités de France, France Urbaine, Ville et Banlieue, Villes internet, Open Data France), le groupe La Poste, la Caisse des Dépôts et Consignations, la Mednum, Pix, France Travail, PIMMS, Familles rurales et Uniformation notamment.

La feuille de route Numérique Ensemble formule quatre objectifs à atteindre sur la période 2023-2027 :

- L’accompagnement de 8 millions de personnes,
- Un maillage de 25 000 lieux d’inclusion numérique,
- 20 000 aidants numériques formés,
- 2 millions d’équipements informatiques reconditionnés accessibles aux ménages les plus modestes.

Selon les données publiées par l’ANCT[6], la mise en œuvre de la feuille numérique ensemble est sur la bonne voie :

- **2 174 744 usagers auraient été accompagnés à 98% par des conseillers numériques** (39 446 usagers ont été accompagnés par des Aidants habilités à Aidants Connect)

- **20 349 lieux d'inclusion numérique sont recensés au niveau national** dont :
    - 10 124 lieux hébergés dans des services publics (5 871 lieux hébergés par les communes, 602 lieux hébergés par les EPCI, 272 lieux hébergés par les départements),
    - 2 729 lieux hébergés par des associations.

  Sur ces 20 349 lieux d’inclusion numérique, 7 050 lieux accueillent des conseillers numériques, 2 568 lieux sont des points d’accueil numérique labellisés France services et 4 876 lieux sont des points d’accueil habilités Aidants Connect.

- **19 617 aidants numériques sont identifiés par l’ANCT** dont :
    - 4 000 postes de Conseillers Numérique attribués,
    - 112 postes de Conseillers Coordinateurs attribués,
    - 15 617 aidants habilités à Aidant Connect.

L’ANCT ne dispose pas, à date, du nombre d’équipements informatiques reconditionnés et/ou distribués.

Pour sa part, l’Etat avait budgété 62 millions d’euros en 2024 pour le déploiement de cette feuille de route qui reposait sur une territorialisation de politique d’inclusion numérique et pour l’accompagnement des acteurs locaux. L’Etat s’était engagé au financement des actions d’inclusion numérique via le dispositif Conseiller numérique à hauteur de 60 millions d’euros par an (source : ANCT).

Cette territorialisation devait passer par la **création d’un fonds d’ingénierie dédié** qui devait permettre notamment le financement de formation en direction des aidants numériques à hauteur de 20 000 euros par département. Ce fonds n’a toujours pas été créé à ce jour.

[6] Données · National | Espace France Numérique Ensemble

B. L'Etat doit remplir ses engagements pour financer le plan "Numérique Ensemble"

En réduisant dans le PLF 2025 les crédits dédiés à l'inclusion numérique à 27 millions d'euros, la feuille de route Numérique Ensemble s'apparente désormais plus à une opération de défaisance territoriale en mettant à la charge des collectivités locales la quasi-totalité du financement de la politique publique d'inclusion numérique : l'Etat, non seulement, ne remplit pas ses engagements pris en 2023 mais il met également en péril le dispositif des conseillers numériques mis en place en 2020.

Le dispositif des conseillers numériques est pourtant la colonne vertébrale, certes fragile, de la politique d'inclusion numérique.

Lancé en 2020 dans la précipitation pour mobiliser 200 millions d'euros dans le cadre du plan de relance, le dispositif des 4000 conseillers numériques est considéré par l'ensemble des acteurs comme la colonne vertébrale de la politique publique d'inclusion numérique.

En 2022, le gouvernement avait annoncé le recrutement de 20 000 aidants numériques à l'horizon 2027 qui inclurait les 4000 conseillers numériques actuels dont le nombre devait être porté à 8000 d'ici la fin du quinquennat selon le Ministre de la transformation et de la fonction publiques, mais également 8300 agents France service déjà opérationnels qui seraient portés à 10 000, et 2000 titulaires d'un contrat de service civique. Il est vrai que le détail de ces annonces ne trouvait pas encore de traduction budgétaire dans la loi de finances 2023…

La formation initiale qui avait été jugée peu adaptée par la CSNP dans son avis de décembre 2022 a, semble-t-il, été améliorée pour répondre au plus près des besoins des personnes qui y ont recours.

C. La disparition des Conseillers numériques anéantira les efforts investis et les résultats obtenus en matière d'inclusion numérique

Alors que les besoins en accompagnement et formation de nos concitoyens vont s'accroître avec l'arrivée de l'intelligence artificielle, les conseillers numériques constituent la clé de voute de la politique publique d'inclusion numérique.

Selon l'ANCT, les conseillers numériques totalisent à eux seuls 98% des accompagnements réalisés. L'objectif des 8 millions de personnes accompagnées fixé par la feuille de route Numérique Ensemble ne pourra pas être atteint sans eux.

Le profil des personnes accompagnées par les conseillers numériques est relativement diversifié même si les plus de 60 ans représentent 47% du public accompagné (29% pour la tranche d'âge 35-60 ans et 10% pour les 18-35 ans)[7].

Le taux de satisfaction des personnes qui ont recours aux conseillers numériques est élevé :

- 97% des personnes accompagnées ont le sentiment d'avoir progressé,
- 83% des individus se sentent plus à l'aise avec le numérique après les accompagnements,
- 93% estiment réussir des tâches qu'elles n'arrivaient pas réaliser avant l'accompagnement,
- 60% estiment être moins stressées à l'idée de manipuler des outils numériques.

[7] Données · National | Espace France Numérique Ensemble

Le dispositif et son évolution a surtout permis de structurer la politique d'inclusion numérique dans les territoires.

Il convient de souligner que le vivier des conseillers numériques qui sont portés contractuellement et principalement par les collectivités territoriales connaît un turnover important du fait de la précarisation des contrats et parfois de leur non-renouvellement du fait des contraintes budgétaires des structures employeuses.

Les membres de la CSNP ont été frappés par la réduction du nombre de conseillers numériques employés par les associations depuis son avis publié en 2022. Or les conseillers numériques employés dans les structures telles que la Croix Rouge ou Emmaus Connect permettent d'aller vers des publics en très grande difficulté ou en très grande précarité pour qui il est difficile de franchir les portes d'une mairie, d'une maison France Service ou d'un service de l'Etat.

En réalité, entre les non renouvellement et les renouvellements de contrats en cours ainsi que le fort turnover des contrats de conseiller numérique, **ce n'est pas 4000 conseillers numériques qui sont déployés dans les territoires mais seulement 2 600 conseillers numériques (Source : ANCT).** L'ANCT a bon espoir que 3 800 conseillers numériques soient à nouveau présents sur le terrain en février 2025 à condition que les crédits budgétaires le permettent.

La dégressivité des financements de l'Etat explique en grande partie le non renouvellement de certains contrats et la réduction des crédits annoncée dans le PLF 2025 ne fera qu'aggraver cette hémorragie.

Pourtant cette fonction de conseiller numérique est essentielle et ne peut pas être compensée par le déploiement des seuls aidants numériques.

En effet, les conseillers numériques ont permis, après une période d'adaptation, de trouver et de mettre en place une formation adaptée aux personnes éloignées du numérique par des accompagnements individuels et collectifs.

Un conseiller numérique, contrairement aux aidants numériques, a vocation à animer une communauté et aller vers les publics les plus éloignés : en moyenne, un conseiller numérique exerce ses activités sur sept sites différents.

Les membres de la commission supérieure considèrent que le dispositif des conseillers numériques doit être pérennisé comme s'y étaient engagés les ministres successifs en charge du numérique. Cette pérennisation ne peut pas se faire par un désengagement financier unilatéral de l'Etat.

III. Elargir et pérenniser les financements de l'inclusion numérique

A. Mobilisation de l'Union européenne sur les enjeux d'inclusion numérique

L'Union européenne indique mobiliser 250 milliards d'euros dans le cadre de NextGenerationEU pour stimuler la numérisation dans l'espace de l'Union européenne.

A ce titre, l'Union européenne finance des formations en ligne afin « *que chacun, jeune ou âgé, puisse améliorer ses compétences numériques* ».

Il nous semble que les enjeux d'inclusion numérique, qui ne concerne pas que la France, exigent une implication plus large et claire de l'Union européenne sur les sujets de formation et d'inclusion

numérique. A ce stade, les fonds mobilisables au titre de l'inclusion numérique relèvent soit des fonds structurels FEDER ou FSE+, soit des fonds directs comme COSME pour les TPE PME ou Erasmus Plus en régie directe ou délégation nationale. Il manque - au niveau européen - un guichet unique et des interlocuteurs en responsabilité à la DG Connect et à la DG Emploi, affaires sociales et inclusion sur ces enjeux.

Les membres de la CSNP considèrent que le gouvernement français doit mettre à profit l'installation de la nouvelle commission pour placer les autorités européennes face à leurs responsabilités en demandant **la création d'une ligne de financement dédiée à l'inclusion numérique suffisamment abondée et dont la procédure de mobilisation soit adaptée à la typologie des acteurs de l'inclusion numérique (taille des structures, obligation de reporting).**

La généralisation des Service d'intérêt économique général (SIEG)[8] pour l'inclusion numérique pourrait utilement venir renforcer les financements des collectivités en la matière. A ce titre, la Région Hauts de France a mis en place un SIEG dédié entre 2020 et 2023, et cette expérimentation pourrait donner lieu à une capitalisation et un essaimage, déjà initié par la Région Grand Est[9]. La Banque des territoires pourrait mettre son expertise à disposition des collectivités dans cette perspective. Cette initiative permettrait de co-financer les acteurs de l'inclusion numérique en répartissant mieux l'effort en matière de dépense publique entre l'Etat et l'Union européenne.

L'identification d'une entité dédiée sur ce sujet au sein de la DG Connect et de la DG Emploi, Affaires sociales et inclusion de la Commission européenne serait une avancée car, à ce stade et selon nos recherches, aucune DG ne porte la responsabilité des questions d'inclusion numérique en propre.

B. Création d'un fonds national d'ingénierie piloté par la Banque des territoires

La feuille de route Numérique Ensemble proposait la création d'un fonds d'ingénierie pour agréger les contributions d'opérateurs privés. Ce fonds n'a pas été mis en œuvre à ce stade.

Les membres de la Commission supérieure considère qu'il y a **urgence à créer ce fonds le plus rapidement possible et qu'il convient d'en confier le pilotage ou le copilotage à la Banque des Territoires** qui, par ses attributions, son implication en matière d'inclusion numérique et son expertise en matière d'ingénierie financière est l'acteur institutionnel le plus à même de mobiliser et d'agréger les fonds privés mais surtout européens.

Pour des structures issues du milieux associatif, il est quasiment impossible de mobiliser des fonds européens tels que le FEDER ou le FSE. La Banque des Territoires a une expertise solide en la matière qu'il convient de valoriser et d'exploiter.

C. Mobiliser davantage le secteur privé pour financer l'inclusion numérique

Le Ministre Jean-Noël Barrot plaçait beaucoup d'espoirs dans la mobilisation du secteur privé pour abonder le fonds d'ingénierie prévu par la feuille de route. Les membres de la CSNP sont plus sceptiques sur la bonne volonté des acteurs économiques et des grandes entreprises du

[8] Guide SIEG du SGAE un SIEG est conçu pour répondre à une mission d'intérêt général en fournissant des services essentiels qui ne peuvent être assurés par le marché dans des conditions optimales de qualité, de sécurité ou d'accessibilité. Le cadre juridique spécifique des SIEG permet aux collectivités de déroger à certaines règles de concurrence, leur offrant une grande latitude pour adapter ces services aux spécificités locales. Ces dispositifs garantissent également un financement sécurisé et des protections sociales et environnementales accrues.

[9] Illettrisme - Dispositifs | C2RP Carif-Oref Hauts-de-France

numériques pour financer les actions d'inclusion numérique, qui viennent pourtant pallier les défauts de conception et de responsabilité sociétale dont ils sont à l'origine. dont ils sont pourtant *in fine* les principaux bénéficiaires.

La numérisation des services marchands permet des gains de productivité mais aussi des développements commerciaux exceptionnels pour l'ensemble des secteurs principalement concerné par les mouvements de dématérialisation et d'automatisation des services (banques, assurances, tourisme, santé, mobilités, etc.). De leur côté, les grandes entreprises du numériques (vente de produit et services) et les grands cabinets de conseil en accompagnement à la transition numérique sont les grands gagnants du nouveau système dématérialisé. Les économies et la valeur ajoutée réalisées par ces acteurs économiques pourraient être mieux redistribuées pour ne pas faire peser sur les seules finances publiques (à périmètre constant ou dégradé) les investissements en matière d'inclusion numériques.

Par ailleurs, force est de constater que cette numérisation à marche forcée des secteurs publics et privés ne s'est pas accompagnée d'une formation du grand public et que c'est finalement l'Etat et les collectivités locales qui financent les actions d'inclusion numérique qui vont permettre aux personnes exclues du numérique d'accéder à ces services.

Plusieurs options sont possibles pour mobiliser davantage les financements du secteur privé:

- Prévoir des mesures incitatives pour orienter les fonds du secteur privé vers le fonds d'ingénierie national proposé par la feuille de route "Numérique ensemble";
- Intégrer des formations à l'inclusion numérique dans le catalogue de formation des employés et salariés dans les 11 OPCO conce(cf. paragraphe X) ;
- Imposer une contribution obligatoire aux grands acteurs internationaux du numérique pour abonder le fonds d'ingénierie. Compte tenu du chiffre d'affaires réalisé en France par ces acteurs et ces plateformes numériques, un pourcentage très faible de leur chiffre d'affaires aurait un effet de levier majeur pour les actions d'inclusion numérique.

D. Instaurer des conférences des financeurs au niveau départemental pour identifier et coordonner les financements au secteur associatif

En matière d'efficacité des financements, la coordination des efforts est absolument primordiale. En matière de financement, ce manque de structuration se traduit par des associations qui vont individuellement solliciter les mêmes bailleurs (autorités locales, services de l'Etat, fondations d'entreprises ou reconnues d'utilité publique) pour des enveloppes annuelles voire des enveloppes de financement de projets. Ce temps de développement n'est pas financé et représente un risque majeur pour la pérennité et l'efficacité des opérateurs de l'inclusion numérique. Par ailleurs, la particularité du secteur de l'inclusion numérique réside notamment dans la multiplicité des acteurs (préfecture, collectivités territoriales, associations, entreprises….) et des rôles (financeur, opérateurs, bénéficiaires…) au niveau des territoires. Dans certains territoires comme la Drôme, des conférences de financeurs pilotés par le préfet se sont déjà installées. Elles permettent de coordonner les efforts de financement sur la base d'analyse de besoins collective.

Aussi, la proposition formulée par "Les Interconnectés" d'organiser au niveau départemental une conférence financière régulière pour fédérer et rationaliser le fléchage des financements dédiés à l'inclusion numérique est une recommandation que souhaite formuler la CSNP.

IV. La coordination de la politique d'inclusion numérique au niveau du département doit tenir compte des actions entreprises dans les territoires.

La CSNP se félicite de la signature des contrats de territorialisation qui associent les acteurs de terrains, institutionnels et associatifs, aux actions d'inclusion numérique déployées sur le territoire national.

Elle avait déjà exprimé son souhait de placer le département au cœur des politiques et des dispositifs d'inclusion numérique car le département est le mieux placé, avec les communes, pour jouer le rôle d'observatoire des besoins en matière d'inclusion numérique. Les politiques sociales et d'insertion sont placées sous sa responsabilité et il dispose d'une vision d'ensemble des besoins.

La désignation de coordonnateurs d'inclusion numérique au niveau départemental va dans ce sens. Les membres de la CSNP attirent cependant l'attention sur la nécessité de tenir compte des actions déjà entreprises dans les territoires par l'ensemble des acteurs : conseils départementaux, intercommunalités et communes, acteurs sociaux et associatifs.

La CSNP avait fait part de sa réserve au sujet des hubs régionaux qui cherchent encore leur modèle économique car tous n'offraient pas la même garantie en termes d'implantation et de solidité financière. De fait, plusieurs hubs pourtant dynamiques ont été déclarés en faillite depuis 2022.

V. Faciliter l'accès de tous aux réseaux et aux équipements numériques

Pour améliorer l'accès au numérique, les conditions préalables sont **la couverture du territoire national, métropolitain et ultramarin, en réseaux internet de qualité.**

Sur ce sujet, les membres de la CSNP ont alerté le gouvernement sur le risque que faisaient peser sur le Plan France Très Haut Débit les coupures budgétaires annoncées au début de l'année 2024[10].

La situation en zone rurale et dans les territoires ultramarins reste préoccupante. En dépit des progrès réalisés, nos concitoyens ont le sentiment de subir une double peine causée par l'éloignement des bassins de vie économique et de la mauvaise connexion qui les éloignent de l'économie et des services publics en ligne. Cette situation n'est pas acceptable.

L'inclusion numérique passe également par **l'accès aux équipements numériques** que ce soit des téléphones, des smartphones et des ordinateurs. La précarité et les facteurs économiques rendent difficile l'accès à ces équipements qui peuvent s'avérer très onéreux pour les foyers à faible revenus.

De nombreuses initiatives existent : certaines collectivités distribuent des ordinateurs ou proposent des formations gratuites. Des associations recyclent et redistribuent des équipements numériques. Emmaüs Connect a été en mesure de distribuer 13 500 équipements informatiques sur trois ans et anticipe une forte progression du nombre d'équipements au cours des prochaines années (en 2024, plus de 10000 équipements seront reconditionnés et redistribués).

Les entreprises du secteur technologique participent également à cet effort en faveur de l'inclusion numérique en proposant des programmes de dons de matériel ou des tarifs réduits pour les ménages défavorisés.

[10] Avis-n°2024-04-du-6-juin-2024-sur-les-consequences-des-coupes-budgetaires-sur-le-Plan-France-Tres-Haut-Debit-au-regard-des-enjeux-de-deploiement-de-resilience-et-de-la-fermeture-du-reseau-cuivre-1.pdf

La feuille de route Numérique Ensemble prévoit que 2 millions d'équipements informatiques reconditionnés seront accessibles aux ménages les plus modestes d'ici 2027.

Pour remplir cet objectif, il est essentiel de massifier les dons aux entreprises de reconditionnement et aux associations en mobilisant les particuliers, les administrations et les entreprises.

Selon une étude publiée par le Credoc[11], il y aurait 70 millions d'appareils susceptibles d'être reconditionnés ou recyclés. Le Baromètre du numérique révèle aussi que « chaque foyer dispose en 2023 en moyenne de 10 équipements numériques avec écrans, utilisés ou non utilisés, soit environ 300 millions d'équipements numériques en France métropolitaine. Sur l'ensemble des terminaux présents au sein d'un foyer, un quart sont conservés sans être utilisés : environ 70 millions d'appareils seraient donc susceptibles d'être reconditionnés ou recyclés ».

VI. L'inclusion numérique : structurer filières professionnelles de formation

Depuis la mise en place des politiques publiques d'inclusion numérique, la question de la formation des acteurs est au cœur des réflexions et des critiques. En effet, dans son dernier avis de 2022, la CSNP avait relevé que le déploiement "en urgence" des conseillers numériques pendant la crise sanitaire n'avait pas permis d'offrir à ces nouveaux professionnels de l'inclusion numérique une formation de qualité. En effet, les marchés publics, l'ingénierie pédagogique et la production des formations avaient dû être déployés en un temps très restreint. L'ANCT a depuis pris note du besoin de consolidation de la qualité des formations. Elle a mis en place un "commun de connaissances" (Les BAses) permettant à tous les acteurs de l'inclusion numérique de trouver les ressources utiles à la conduite de leurs actions, et veille à consolider la qualité des formations.

En France, la certification des formations passe désormais par France Compétences et son Registre national des compétences professionnelles (RNCP). A date, le seul titre professionnel correspondant au métier de conseiller numérique "Responsable d'espace de médiation numérique"[12] est daté, arrive à échéance en juillet 2025, et doit donc faire l'objet d'une mise à jour pour coller aux réalités des conseillers numériques sur le terrain.

C'est l'objet de l'Engagement pour le Développement des Compétences sur la médiation numérique en cours, co-piloté par l'ANCT et l'OPCO de la Cohésion sociale Uniformation[13]. Il a pour objet d'"appuyer la structuration de la filière professionnelle de l'aide et de la médiation numérique pour garantir aux citoyens et usagers une qualité d'accueil et d'accompagnement."

Au-delà, les compétences de l'inclusion numérique, souvent transverses et additionnelles aux métiers qui pré-existent, doivent faire l'objet d'inscription dans le Registre nationale des compétences spécifiques. C'est le cas, par exemple, des compétences mobilisées dans le cadre du programme Aidants connect. Elles doivent permettre "d'augmenter" les compétences de personnes qui accompagnent les publics en situation de fragilité numérique.

[11] https://www.banquedesterritoires.fr/barometre-du-numerique-2023-une-appropriation-elevee-mais-tres-heterogene

[12] https://www.francecompetences.fr/recherche/rncp/39181/

[13] https://www.societenumerique.gouv.fr/nos-missions/france-numerique-ensemble/axe-3

La CSNP recommande notamment de prioriser la formation des travailleurs sociaux, dont le travail quotidien est directement impacté par la dématérialisation des services publics comme le souligne le Haut Conseil au travail social dans son dernier Livre blanc[14], **mais aussi des éducateurs et accompagnateurs en insertion socio-professionnelle**, comme en ont témoigné les personnels de la Mission locale rurale rencontrés en Limousin. Plus largement, ces compétences transverses devraient être intégrées à l'ensemble des métiers d'accueil et d'accompagnement des publics, dans le secteur public (fonctionnaires) mais aussi dans le secteur privé (guichet des banques, assurances, etc.). Ce chantier - investissement central pour le déploiement d'une politique publique d'inclusion numérique à la hauteur des besoins- nécessite à la fois des financements mais aussi de l'accompagnement.

La CSNP recommande à ce titre que les formations aux compétences professionnelles et spécifiques de l'inclusion numérique soient intégrées systématiquement dans les catalogues des 11 OPCO et confiées aux acteurs de l'inclusion numérique, représentés par La Mednum et les Interconnectés.

A ce titre, les marchés pourraient être fléchés par des clauses d'accessibilité de marché public aux structures de l'Économie sociale et solidaire[15], majoritaire chez les acteurs de l'inclusion numérique. Cela aurait un double impact : renforcer les modèles économiques des seconds tout en garantissant une montée en compétences numériques de tous les salariés qui accompagnent des publics en fragilité numérique, pour une meilleure couverture des besoins des publics en situation de fragilité numérique, partout sur les territoires.

VII. Numérique et personnes souffrant de troubles cognitifs: une opportunité qui nous engage

Le numérique est un outil d'indépendance pour les personnes handicapées, facilitant l'accès à leurs droits et à des conditions de vie plus autonomes. Il peut également se transformer en un "surhandicap", en particulier pour les personnes en situation de handicap (PSH) cognitif ou intellectuel[16] .

Parmi les 7,7 millions de Français déclarant une limitation fonctionnelle sévère, environ 2 millions présentent des déficiences cognitives ou intellectuelles.[17] Une enquête menée par l'Association de gestion du fonds pour l'insertion professionnelle des personnes handicapées (Agefiph), l'ANCT, la Croix-Rouge française et Emmaüs Connect montre l'exclusion de cette population des services numériques en raison de leur inaccessibilité[18] .

En 2022, plus de 60% des démarches administratives étaient inaccessibles aux PSH [19] . Or, l'accès aux droits et à l'emploi des PSH intellectuel ou cognitif dépend aujourd'hui de cette accessibilité

[14] https://solidarites.gouv.fr/livre-blanc-du-travail-social-2023

[15] https://www.ess-france.org/system/files/inline-files/Chaire%20TerrESS_ESS-et-Commande-Publique.pdf

[16] https://shs.cairn.info/revue-pratique-en-sante-mentale-2023-1-page-21?lang=fr&tab=resume

[17] https://drees.solidarites-sante.gouv.fr/publications-communique-de-presse/panoramas-de-la-drees/le-handicap-en-chiffres-edition-2023

[18] https://lesbases.anct.gouv.fr/ressources/enquete-l-inclusion-numerique-des-personnes-en-situation-de-handicap-intellectuel-etou-cognitif

[19] https://www.defenseurdesdroits.fr/rapport-dematerialisation-des-services-publics-trois-ans-apres-ou-en-est-265

numérique. Sans un accompagnement adapté, la numérisation des services administratifs expose cette population à de nouveaux risques d'exclusion, d'isolement et d'abus de confiance.

Une véritable politique d'inclusion numérique nécessite un changement de paradigme, comme le montre l'initiative de la Fédération des Centres Sociaux et Socioculturels de France avec le projet "Dématérialiser sans déshumaniser", qui place les usagers vulnérables au cœur de l'amélioration des interfaces, les considérant comme des experts de leurs propres besoins [20]

A. Le dispositif des conseillers numériques et les lacunes en matière de formation spécifique

S'il a fait des progrès, la formation des conseillers numériques présente des lacunes significatives dans la prise en charge des PSH intellectuel ou cognitif. Les conseillers numériques manquent de ressources et de formation adaptées aux besoins spécifiques de ces populations.

Les modules de formation ne prévoient pas systématiquement de formations spécifiques sur les techniques de médiation numérique adaptées aux PSH qu'il soit physique, cognitif ou intellectuel. Un partenariat renforcé avec des organismes comme l'Agefiph pourrait faciliter le développement d'outils et de formations pour les conseillers numériques.

B. Accessibilité des sites web : état des lieux et perspectives

La loi du 11 février 2005[21] et le décret du 9 octobre 2023[22] garantissent l'accessibilité numérique en France, obligeant certains acteurs privés à rendre leurs sites accessibles aux PSH, conformément à la directive européenne sur l'accessibilité numérique. Toutefois, de nombreuses plateformes françaises restent inaccessibles, exacerbant les difficultés d'accès au travail, aux services publics et aux droits. **Le Défenseur des droits a souligné les défis de conformité avec le référentiel général d'amélioration de l'accessibilité (RGAA) liés à l'absence de financement et de temps pour les structures concernées.**

En effet, une PSH sur cinq renonce à effectuer des démarches en ligne en raison de la difficulté d'utilisation des sites, compromettant ainsi leur accès aux droits sociaux, à l'emploi et à l'autonomie [23.] En 2022, seules 76 des 241 démarches administratives les plus fréquemment utilisées étaient partiellement accessibles [24] . Les sanctions pour non-conformité étant rares, la CSNP soutient la recommandation de la Défenseure des droits d'instaurer un contrôle de conformité sur les sites web publics et privés.

C. Vers des solutions innovantes : des partenariats au service de l'inclusion

Face à la vulnérabilité accrue des PSH cognitif ou intellectuel, certaines initiatives émergent pour répondre à leurs besoins. L'Agefiph, en partenariat avec Diversidays et France Immersive Learning, développe des programmes de formation aux métiers du numérique, en utilisant des outils immersifs pour faciliter l'apprentissage de ce public.

---

[20] https://www.centres-sociaux.fr/une-coalition-dacteurs-pour-dematerialiser-sans-deshumaniser/

[21] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000809647

[22] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000048178349

[23] https://lesbases.anct.gouv.fr/ressources/enquete-l-inclusion-numerique-des-personnes-en-situation-de-handicap-intellectuel-etou-cognitif

[24] https://www.defenseurdesdroits.fr/rapport-dematerialisation-des-services-publics-trois-ans-apres-ou-en-est-265

Dans ce cadre, l'intelligence artificielle, en personnalisant les interfaces et parcours numériques, est perçue par les acteurs auditionnés comme essentielle pour améliorer l'accessibilité, bien qu'elle présente des risques de biais et manque de transparence.

Des solutions technologiques françaises existent : l'entreprise FACIL'ITI propose la personnalisation de l'affichage des sites sans en modifier le contenu d'origine. Leur outil MYdys, qui adapte l'affichage des textes aux personnes dyslexiques en partie grâce à l'IA, a été testé auprès de plus de 14 000 personnes handicapées. Les risques liés à l'utilisation de grands modèles de langage (LLM) sont mitigés par un agrégateur de modèle français permettant de vérifier les informations proposées.

Pour garantir une politique d'inclusion numérique efficace pour les PSH intellectuel ou cognitif, il est essentiel d'adopter une approche collaborative, impliquant à la fois les acteurs publics, privés et les nouvelles technologies.

VIII. Des clarifications à apporter sur le statut Aidants Connect

Au cours de ses auditions, le groupe de travail a pu constater des **flottements sur la notion d'Aidants Connect,** parfois confondus avec les Conseillers numériques ou les « anciens » conseillers numériques France Service.

Il paraît donc opportun d'entreprendre un travail de clarification et de communication sur l'utilité et la promotion du dispositif Aidants Connect qui répond à un besoin réel de la population.

La clarification pourrait notamment porter sur le statut des Aidants Connect et sur la responsabilité engagée en cas d'erreur ou de fraude des Aidants Connect.

Pour les membres de la CSNP, la responsabilité de l'Etat en cas d'erreur ou de fraude d'un Aidant Connect serait de nature à dissiper les craintes de certaines structures employeuses, qui comme Le groupe La Poste ne souhaite pas engager sa responsabilité et a fait le choix de ne pas habiliter ses postiers à la procédure Aidants Connect.

La possible mise en jeu de la responsabilité de l'Etat pourrait également permettre un recrutement plus massif auprès des associations et le développement d'un statut de "bénévole aidant numérique » qui permettrait aux associations d'accompagner les personnes via Aidants Connect.

Une étude conduite par des juristes associant les structures employeuses apporterait ces clarifications tout en veillant à ne pas complexifier la procédure d'habilitation des Aidants Connect.

LISTE DES PERSONNES AUDITIONNÉES

(par ordre alphabétique)

Agence nationale de la cohésion des territoires (ANCT)

- M. Laurent ROJEY, Directeur général délégué numérique
- Mme Léa GISLAIS, Co-Directrice Programme Société numérique

Association pour la gestion des fonds pour l'insertion professionnelle des personnes handicapées (Agefiph)

- Mme Véronique BUSTREEL, Directrice de l'innovation, de l'évaluation et de la stratégie

Association des maires de France (AMF)

- M. Michel SAUVADE, Maire de Marsac en Livradois, Vice-président du Conseil départemental du Puy de Dôme, Co-président de la commission numérique de l'Association des maires de France

Banque des territoires

- M. Christophe GENTER, Directeur du Département Cohésion Sociale et Territoriale
- M. François BLOUVAC, Responsable Éducation, inclusion numérique et services au public
- Mme Emmanuelle BORRELLY, Responsable du pôle Inclusion numérique et services au public
- Mme Sacha DESMARIS, Responsable du pôle Conseillers numériques France Services
- Mme Julie STEIN, Chargée de projets éducation au sein du département cohésion sociale et territoriale

Conseil départemental de la Haute-Vienne

- Mme Gulsen YILDIRIM, 3ème Vice-Présidente en charge de l'enfance, de la famille et de la démocratie sanitaire
- Mme Sylvie TUYERAS, 5ème Vice-Présidente en charge de l'insertion et du logement
- Mme Charlotte LOISEAU, Directrice générale adjointe en charge des Solidarités Humaines
- Mme Nathalie SARDENNE, Directrice de l'insertion, de l'emploi et l'action sociale

Croix-Rouge française

- Mme Pauline BLANC-PATIN, Directrice de l'innovation
- Mme Irène ROSSETTI, Coordinatrice régionale Ile-de-France Inclusion Numérique

Défenseur des droits

- Mme Claire HÉDON, Défenseure des droits
- Mme Sarah BENICHOU, Directrice de la promotion de l'égalité et de l'accès aux droits
- M. Victor MANCIET, Chef de cabinet

Emmaüs Connect

- M. Victor ESTIENNEY, Responsable national des opérations
- M. Victor BAYSANG-MICHELIN, Chargé de plaidoyer

FACIL'ITI

- M. Frédéric SUDRAUD, Président
- Mme Audrey JAYET, Chargée de communication

Fédération des Centres Sociaux et socioculturels de France

- Mme Isabelle ZELLER, Membre du bureau

Groupe La Poste

- Mme Isabelle LHERBIER, Directrice des relations opérateurs publics et privés et Présidente du réseau PIMMS Médiation
- Mme Rebecca PÉRÈS, Déléguée aux affaires territoriales et parlementaires

Interconnectés

- Mme Céline COLUCCI, Déléguée générale d'Interconnectés, 1er réseau national de transformation numérique des collectivités

Mairie de Rilhac-Rancon

- M. Paul ANGLERAUD, Directeur général des services
- Mme Maryange POMMIER, Conseillère numérique

Mednum

- Mme Mélusine BLONDEL, Co-Directrice générale
- M. Jan BUSCHER, Directeur général

Le Park numérique

- M. Gregory GUILLOU, Co-fondateur
- M. Pascal PIERRE-LOUIS, Co-fondateur et Président

Préfecture de la Haute-Vienne

- Mme Anne-Sophie MARCON, Sous-Préfète en charge du numérique

Restos du cœur

- Mme Estelle TOVOLI, Chargée des relations Institutionnelles
- M. Vincent BOURGEOIS, Bénévole au pôle insertion et accompagnement des Restos sur les sujets d'inclusion numérique

Secrétariat d'État auprès du ministre de l'Enseignement supérieur et de la Recherche, chargé de l'Intelligence artificielle et du Numérique

- Mme Clara CHAPPAZ, Secrétaire d'État auprès du ministre de l'Enseignement supérieur et de la Recherche, chargée de l'Intelligence artificielle et du Numérique
- M. Pierre BOUILLON, Directeur du cabinet
- Mme Mélodie AMBROISE, Conseillère parlementaire, Inclusion numérique et Protection de l'enfance en ligne
- M. Vincent RAPP, Conseiller spécial chargé de l'Intelligence artificielle

- M. Maxime DONADILLE, Conseiller Régulation et protection de l'espace numérique
- Mme Amélie PINGEOT, Conseillère Écosystème startup et Financement

CONTRIBUTIONS ÉCRITES

(par ordre alphabétique)

- **Agence Nationale de la Cohésion des Térritoires**
- **Banque des territoires**
- **Emmaus Connect**
- **Fédération des Centres Sociaux de France**
- **MedNum**

BIBLIOGRAPHIE

(par ordre alphabétique)

- ANCT, CREDOC, Université Rennes 2 CREAD-M@rsouin (2023). *La société numérique française : définir et mesurer l'éloignement numérique.*
- ANCT, Croix-rouge, AGEFIPH & Emmaüs Connect (2024). *L'inclusion numérique des personnes en situation de handicap.*
- ANCT, Mazet P. & Stefan J. (2023). *Déploiement du dispositif conseiller numérique France Services : résultats d'étape de l'enquête quantitative du programme national de recherche.*
- ANCT (2022). *Société numérique : rapport d'activités 2017-2022*
- Banque des territoires (2022). *L'inclusion numérique, un marché comme les autres ? Étude de marché.*
- Commission supérieure du numérique et des postes & FILLEUL, M. (2022). *Avis N°2022-08 sur le bilan du dispositif des conseillers numériques.*
- Cour des comptes (2024). *Programme France Services (2020-2023).*
- Demas, P. (2022). *Renforcer la cohésion numérique dans les territoires : 20 mesures pragmatiques et de bon sens, rapport d'information 588.* Commission de l'aménagement du territoire et du développement durable. Rapport au Sénat
- France Assos Santé, La Mednum (2023). *Inclusion numérique. Représentants des usagers, comprendre et participer à l'inclusion numérique.*
- Gelot, D. (2019). *Dématérialisation des actes administratifs : quel impact sur les publics les plus fragiles ?* Note sur le rapport 2019 du Défenseur des droits », Vie sociale, vol. 28, n°4, pp. 189-193.
- Impact Tank, Mbanza E. & Archias P. (2024). *Faire numérique ensemble.*
- La Mednum, *Observatoire de l'inclusion numérique*, 2024.
- La Mednum, ANCT, *CNR Numérique – Volet Inclusion numérique*, 21 avril 2023
- Ministère chargé de la Transition numérique et des Télécommunications (2023). *France numérique ensemble. Proposition de feuille de route issue des travaux du Conseil national de la refondation 2023-2027.*
- Sénat & VALL, R. (2020). *Rapport d'information (. . .) sur la lutte contre l'illectronisme et pour l'inclusion numérique.*

AVIS N°2024-09 DU 11 DECEMBRE 2024

SUR LE PROJET DE RAPPORT AU GOUVERNEMENT ET AU PARLEMENT SUR LE COÛT NET EN 2023 DE LA MISSION D'AMENAGEMENT DU TERRITOIRE ASSUREE PAR LA POSTE

Conformément aux termes du point IV de l'article 6 de la loi n°90-568 du 2 juillet 1990, modifiée par la loi n°2010-123 du 9 février 2010, la Commission Supérieure du Numérique et des Postes (CSNP) a été saisie le 5 novembre 2024 pour avis par l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep) sur le projet de rapport au Gouvernement et au Parlement déterminant le coût net en 2023 de la mission d'aménagement du territoire assurée par La Poste.

Vu la loi n° 90-568 du 2 juillet 1990, modifiée par les lois 2005-516 du 20 mai et 2010-123 du 9 février 2010 ;

Vu le décret 2007-09 du 5 janvier 2007 relatif au service postal universel et aux droits et obligations de La Poste ;

Vu le décret 2011-849 du 18 juillet 2011 précisant la méthode de calcul du coût net du maillage complémentaire permettant à La Poste d'assurer sa mission d'aménagement du territoire ;

Vu le contrat de présence postale territoriale 2023/2025 signé entre l'Etat, l'Association des Maires de France et des Présidents d'intercommunalité, et La Poste ;

Vu les réunions techniques préparatoires :

- du 18 novembre 2024 avec les représentants du Groupe La Poste :
    - M. Vincent MOULLE, directeur de la Régulation, de la Concurrence et des Relations Institutionnelles ;
    - Mme Rebecca PERES, déléguée aux Affaires Territoriales et Parlementaires ;
    - M. Denis JORAM, directeur de la régulation et des études ;
    - Mme Lorraine AEBERHARDT, cheffe de projet ;
    - M. Théophile CUQ, économiste.

- du 21 novembre 2024 avec les représentants de l'Arcep :
    - M. Jules BELEY, Adjoint au chef d'Unité DEN/UPA ;
    - Mme Estelle CHAUVEAU, Chargée de mission unité Coûts et tarifs, Poste, Presse et Audiovisuel.

Ces deux réunions techniques ont été menées pour la CSNP par M. Patrick GUILLEMOT, personnalité qualifiée sur les questions postales et membre de la CSNP, Mme Valérie MONTANE, secrétaire générale, M. Marc SIFFERT-SIRVENT, secrétaire général adjoint.

Vu les auditions :

- du 28 novembre 2024 pour le Groupe La Poste :
    - M. Nicolas ROUTIER, directeur général adjoint, en charge du Service Public et de la Régulation ;
    - Mme Rebecca PERES, déléguée aux Affaires Territoriales et Parlementaires ;
    - Mme Lorraine AEBERHARDT, cheffe de projet ;
    - M. Théophile CUQ, économiste.

- du 3 décembre 2024 pour l'Arcep :
    - Mme Anne YVRANDE-BILLON, Directrice Economie, Marchés et Numérique ;
    - M. Jules BELEY, Adjoint au chef d'Unité DEN/UPA .

Ces auditions ont été menées dans le cadre d'une séance de la CSNP, sous la présidence de M. Stéphane TRAVERT, Député de la Manche et Président de l'Observatoire national de la présence postale (ONPP).

Ont participé à la procédure de consultation : M. Damien Michallet, sénateur de l'Isère, M. Christian Redon-Sarrazy, sénateur de la Haute-Vienne, M. Bernard Delcros, sénateur du Cantal, Mme Patricia Demas, sénatrice des Alpes Maritimes, Mme Audrey Linkenheld, sénatrice du Nord, M. Jean-Yves Roux, Sénateur des Alpes de Haute Provence, Mme Denise Saint-Pé, sénatrice des Pyrénées-Atlantiques, M. Stéphane Travert, député de la Manche, M. Henri d'Agrain, personnalité qualifiée, Mme Jeanne Bretécher, personnalité qualifiée, M. Patrick Guillemot, personnalité qualifiée.

N'ont pas participé à la procédure de consultation : Mme Lisa Belluco, députée de la Vienne, Mme Anne Le Hénanff, députée du Morbihan, M. Aurélien Lopez-Liguori, député de l'Hérault, M. Jacques Oberti, député de Haute-Garonne, Mme Marie Pochon, députée de la Vienne, M. Stéphane Vojetta, député de la 5ème circonscription des français de l'étranger.

I. ELEMENTS DE CONTEXTE

L'article 6 de la loi n°90-568 du 2 juillet 1990 prévoit qu'en complément de ses obligations de service universel, La Poste contribue à l'aménagement du territoire par son réseau de points de contact.

Un fonds postal national de péréquation territoriale est constitué pour financer le coût du maillage territorial complémentaire : Les ressources du fonds proviennent notamment de l'allègement de fiscalité locale à hauteur de 59 millions d'euros en 2023 dont bénéficie La Poste en contrepartie de sa mission d'aménagement du territoire, complété d'une dotation budgétaire à hauteur de 105 millions d'euros en 2023.

Le présent avis porte donc sur le projet de rapport au Gouvernement et au Parlement déterminant le coût net en 2023 de la mission d'aménagement et de développement du territoire assurée par La Poste. Il est établi par l'Autorité de régulation des communications électroniques, des postes et de la distribution de la Presse (Arcep). Il s'agit de la 15ème évaluation du coût net de cette mission.

1. Place du réseau de La Poste dans le Groupe. Le Groupe La Poste est structuré en quatre branches : « Services-Courrier-Colis », « GeoPost », « La Banque Postale » et « Grand Public et Numérique ». Pour mener à bien ces différentes activités et en assurer la commercialisation, le groupe dispose d'un réseau de distribution géré par la direction du Réseau qui est rattachée à la branche « Grand Public et Numérique ». Celle-ci met à disposition des différents métiers une structure commerciale permettant d'accueillir et de servir les clients particuliers et professionnels du groupe en assurant des prestations au nom et pour le compte de chaque métier.

D'autres canaux de vente, comme les buralistes, la grande distribution, les agences postales communales, ou encore les points relais assurent la commercialisation de prestations de La Poste. L'offre disponible dans ces points demeure toutefois plus restreinte que celle mise à disposition dans les bureaux de poste.

Au total, le réseau est constitué d'environ 17 000 points de contact répartis sur l'ensemble du territoire français.

2. Rappels méthodologiques.

Pour évaluer le coût net de la mission d'aménagement du territoire, trois réseaux théoriques sont identifiés :
- le réseau commercial défini comme le réseau qui maximise la rentabilité des services sans contrainte de présence territoriale,
- le réseau d'accessibilité du service universel (dit aussi « réseau accessible »), réseau avec lequel 99% de la population nationale et 95% de la population de chaque département est à moins de 10 km d'un point de contact, et qui compte au moins un point de contact par tranche de 20 000 habitants dans les communes de plus de 10 000 habitants,
- le réseau complémentaire qui permet, en complément du réseau d'accessibilité du service universel, que pas plus de 10% de la population d'un département ne se trouve éloignée de plus de 5 kilomètres et de plus de 20 minutes du trajet automobile des plus proches points de contact de la Poste.

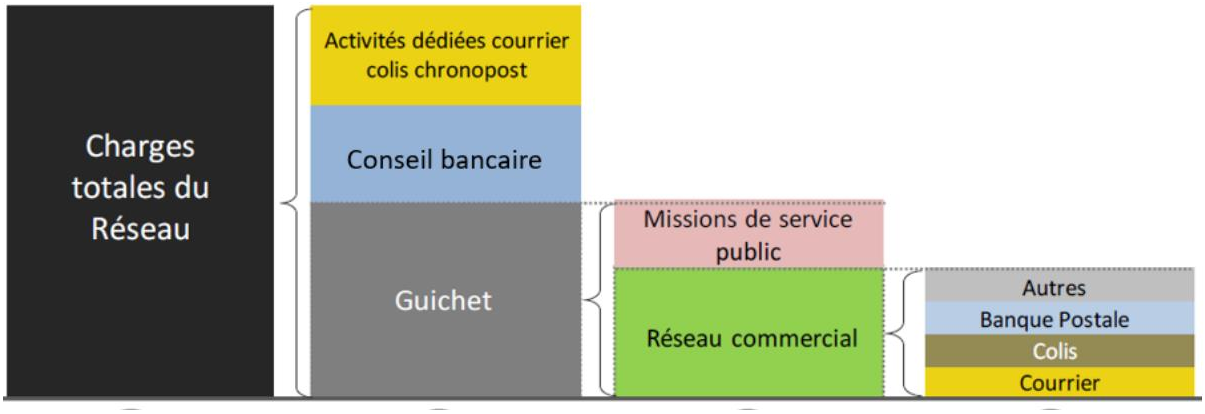
Au total, le réseau de La Poste compte au moins 17 000 points de contacts répartis sur l'ensemble du territoire.

L'évaluation du coût net de la mission d'aménagement du territoire pour La Poste repose sur les éléments suivants :

- estimation des coûts dans un scénario hypothétique sans réseau complémentaire ;
- report intégral de la demande vers le réseau accessible (pas de pertes de recettes et surcroit d'activité aux coûts du réseau accessible) ;
- prise en compte de l'avantage immatériel que retire La Poste de la présence de son logo sur les points du réseau complémentaire.

Les recettes totales du réseau sont composées principalement des recettes générées par la vente de produits Courrier, Colis et autres, auxquelles s'ajoute la part du produit net bancaire (ci-après « PNB ») réalisé dans le réseau.

Les charges du Réseau se décomposent comme suit :



Par une modélisation, les charges du guichet sont séparées entre celles relatives aux missions de service public de présence territoriale (correspondant au réseau accessible et au réseau complémentaire) et celles relatives au réseau commercial de La Poste, c'est-à-dire le réseau que La Poste développerait en l'absence d'obligations de présence territoriale.

II. RESULTATS DE L'EVALUATION 2023

1. Evolution du Réseau

Le nombre de points de contact de La Poste est en légère diminution pour l'année 2023 : la progression du nombre de points partenaires (points « La Postes Agences Communales » et points « La Poste Relais Commerçants ») ne compense pas la diminution du nombre des bureaux de poste en propre.

2. Activité

En 2023, l'activité totale du réseau affiche une baisse sensible, quasiment de même ampleur que celle enregistrée en 2022 et qui confirme la tendance observée depuis plusieurs années (hormis la hausse atypique notée entre 2020 et 2021 liée à la reprise post COVID). Cette baisse d'activité concerne aussi bien les opérations guichets que les opérations sur automates. Le temps moyen d'une opération reste quant à lui relativement stable. L'activité du Réseau de La Poste reste fortement concentrée dans un nombre restreint de points de contact.

3. Charges

Contrairement aux années précédentes, les charges sont en légère augmentation en 2023. Les efforts continus de La Poste en matière d'adaptation de ses organisations et de poursuite de la transformation du Réseau ont de même permis de contrebalancer en grande partie les effets de la forte augmentation de l'inflation sur la fin de l'année 2022 et sur toute l'année 2023.

4. Coût net de la mission d'aménagement du territoire.

En 2023, l'Arcep évalue ce coût net à **322 millions** € soit une diminution de 26 millions € par rapport à 2022 (348 millions €).
L'estimation par La Poste qui résulte d'un modèle légèrement différent de celui de l'Arcep et n'a qu'un usage interne s'élève à 333 millions €, également en diminution par rapport à 2022 (350 millions €)

L'écart entre l'évaluation de l'Arcep et l'évaluation de La Poste est donc de 11 millions € en 2023. Cet écart est dû à quelques différences dans le détail de la méthode utilisée par La Poste.

III. POSITION DE LA COMMISSION SUPERIEURE DU NUMERIQUE ET DES POSTES

La Commission supérieure note avec satisfaction la convergence constante entre l'évaluation du coût net de la mission d'aménagement du territoire confiée au Groupe La Poste de l'Arcep (322 M€) et celle produite par La Poste (333 M€). Pour mémoire, cet écart représentait 33 millions € en 2020. Cette convergence des données offre un socle clair aux débats sur le service rendu et sa compensation.

La Commission supérieure relève que, comme en 2022, les tendances observées avant la crise COVID, à savoir une baisse sensible et constante de la fréquentation des points de contact et donc de l'activité se confirment.

La Commission supérieure observe qu'en matière de coûts, comme elle en avait émis la crainte lors de son avis sur le coût net 2022, les niveaux d'inflation de fin 2022 et de 2023 ont pesé sur les charges du réseau de La Poste. Ces charges ont toutefois évolué sensiblement moins vite que l'inflation grâce aux efforts de réorganisation.

Alors que la compensation de l'Etat de la mission d'aménagement du territoire s'est établie à 164 M€ en 2023, la Commission supérieure constate donc que la mission d'aménagement du territoire est très largement sous-compensée au regard de son coût net évalué à 322 M€ par l'Arcep.

La Commission supérieure rappelle sa position concernant le financement des missions de service public confiées au Groupe La Poste : une juste compensation des coûts générés par la mise en œuvre de ces missions est essentielle pour garantir dans le temps le maintien non seulement de la présence postale mais aussi de la qualité de service due à nos concitoyens.

Les effets de l'inflation ont durement affecté le niveau des charges du Réseau de La Poste. Les membres de la Commission supérieure attirent l'attention de l'Etat sur la nécessité de maintenir sa dotation au Fonds postal national de péréquation territoriale pour maintenir les moyens d'intervention des Commission Départementales de Présence Postale Territoriale qui sont grevés par l'augmentation des charges et par l'indexation contractuelle et annuelle des rémunérations des partenariats.

Une baisse des moyens fait peser un risque sur la qualité et la disponibilité du service mais aussi fragilise la situation économique de La Poste.

La compensation de la mission d'aménagement du territoire n'est qu'une partie de la problématique de la compensation des missions de service public confiées à La Poste. La Commission supérieure souhaite, qu'au-delà des méthodes d'évaluation retenues par type de mission, puisse être présenté un modèle économique permettant de compenser au plus près les coûts du service public postal intégrant des indicateurs de qualité de service reflétant la perception des utilisateurs des services en question.

La Commission supérieure plaide pour une juste et complète compensation des coûts de la mission d'aménagement du territoire confiée à La Poste, tout en encourageant celle-ci à poursuivre résolument son adaptation et la transformation de son réseau dans le cadre des négociations et principes précisées dans le contrat de présence postale territoriale. Sur ce point de l'adaptation de ses formes de présence, la Commission supérieure souligne son intérêt pour de nouvelle formes de présence comme la mutualisation de services. Plusieurs exemples de réalisation semblent prometteurs tant sur la capacité à garantir une présence étendue qu'à offrir un service intégré, efficient pour la population.

Conclusion

La Commission supérieure rappelle son attachement au principe de compensation des missions de service public assurées par La Poste au plus près des coûts réels. Les services de La Poste sont indispensables pour contribuer à la cohésion sociale et pour garantir un développement équilibré dans tous les territoires.

La Commission supérieure souhaite également alerter les pouvoirs publics sur un modèle fragilisé par les effets de la baisse constante de la fréquentation et de l'activité dans les points de contact de La Poste ainsi que sur les éléments conjoncturels tels que l'inflation qui font peser un risque de dégradation du service sur le territoire.

Dans ce contexte, la Commission supérieure appelle l'Etat à respecter les engagements pris lors de la signature du contrat de présence postale 2023-2025 et à abonder le fonds national de péréquation territoriale à hauteur de 174 M€ par an. Elle rappelle que la compensation au plus juste des coûts réels engagés sur la Poste devrait représenter une compensation de l'ordre de 322 millions d'euros en 2023.

Sous réserve des observations formulées dans le présent avis, la Commission supérieure émet un avis favorable sur le projet de rapport de l'Arcep destiné au Gouvernement et au Parlement sur le coût net 2023 de la mission d'aménagement du territoire assurée par La Poste.

Commission Supérieure du Numérique et des Postes
100, rue de Richelieu
75002 Paris

@CSNUMPOST

@Commission Supérieure du Numérique et des Postes