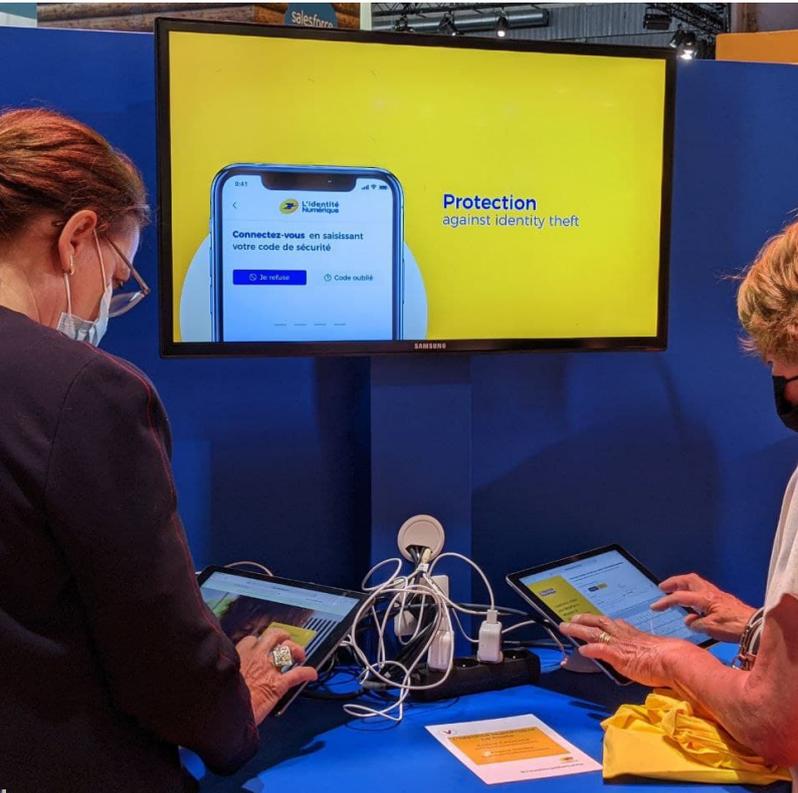


RAPPORT D'ACTIVITÉ



2021

SOMMAIRE

Editorial de la Présidente	p. 01
Composition et mouvements.....	p. 03
Les missions.....	p. 07
Les activités de la CSNP en quelques chiffres.....	p. 09
Les moyens.....	p. 10
Les priorités de la CSNP en 2021.....	p. 12
• Entretien avec Mme Mireille Clapot.....	p. 14
• Entretien avec M. Patrick Chaize.....	p. 15
• Entretien avec Mme Martine Filleul.....	p. 17
• Entretien avec M. Hervé Saulignac.....	p. 19
L'agenda en 2021.....	p. 21
Avis rendus en 2021.....	p. 27



EDITORIAL DE LA PRÉSIDENTE

Mireille Clapot, députée de la Drôme,
Présidente de la Commission Supérieure
du Numérique et des Postes,
Membre de la Commission des Affaires étrangères

Pour la Commission supérieure du numérique et des postes, l'année 2021 a été synonyme de renouvellement : renouvellement partiel de ses membres issus du Sénat, renouvellement de sa présidence et de son bureau et renouvellement de ses méthodes de travail.

Dans le prolongement des élections sénatoriales du 27 septembre 2020, la Commission a eu le plaisir d'accueillir en janvier 2021 Mme Toine Bourrat, sénatrice des Yvelines, M. Jean-Pierre Corbizez, sénateur du Pas-de-Calais et M. Franck Montaugé, sénateur du Gers, remplacé en juillet 2021 par M. Christian Redon-Sarrazy, sénateur de la Haute-Vienne.

Cette reconstitution a permis l'organisation des élections de la présidence de la Commission supérieure et celle du bureau le 11 février 2021. Elue à l'unanimité, je remercie l'ensemble des membres de la Commission supérieure pour la confiance qu'ils m'ont témoignée et remercie mon prédécesseur, M. Yvon Collin, sénateur du Tarn-et-Garonne, pour son engagement sans faille au service de la Commission supérieure tout au long de son mandat et pendant la période d'intérim.

Fort logiquement, le bureau de la CSNP a également été renouvelé : Mme Toine Bourrat a été élue première vice-présidente, M. Bernard Delcros, deuxième vice-président et M. Hervé Saulignac, secrétaire.

Parce que nous souhaitons impulser une nouvelle dynamique et structurer nos travaux en impliquant davantage nos membres de manière collective, une nouvelle organisation s'est mise en place par la création de groupes de travail thématiques sur les sujets suivants : sécurité numérique, souveraineté numérique, missions de service public de La Poste, feuille de route technologique de la France, inclusion numérique, médiation et citoyenneté numérique, numérique responsable et communs numériques et sujets sociétaux et réglementaires.

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

Cette nouvelle organisation s'est traduite par moins de séances plénières mais plus de réunions thématiques.

En 2021, les travaux de la Commission supérieure ont porté sur la transposition du code européen des télécommunications, le renforcement des dispositifs publics en matière de souveraineté et de sécurité numérique, les missions de service public confiées à La Poste, la modernisation et les apports du numérique au processus électoral ainsi que le renforcement de l'inclusion numérique.

S'agissant de la transposition du code européen des télécommunications, nous avons déjà eu l'occasion d'émettre plusieurs recommandations sur ces travaux de transposition dont certaines ont été prises en compte par le gouvernement. Les membres de la CSNP resteront vigilants sur la mise en œuvre de plusieurs nouvelles mesures introduites dans le code des télécommunications notamment sur les mesures portant sur le service universel.

Compte tenu de la progression exponentielle des cyberattaques observée ces dernières années, la Commission supérieure a étudié avec beaucoup d'attention le plan d'accélération cyber présenté par le Président de la République en février 2021. Après avoir auditionné plusieurs experts dans ce domaine, nous avons adopté des recommandations afin de compléter certains angles morts qui nous semblaient insuffisamment couverts.

Avec la crise COVID, le phénomène d'attrition du courrier observé depuis plusieurs années s'est accéléré, mettant désormais en péril l'équilibre financier de la mission du service public universel : les avis de la CSNP et notre participation au comité de suivi de haut niveau organisé par le Premier ministre en juillet 2021 ont permis de dresser des perspectives sur l'évolution des missions de service public confiées à La Poste. Les membres de la Commission seront particulièrement attentifs au cours des prochains mois aux termes du renouvellement du contrat d'entreprise conclu entre l'Etat et La Poste et du contrat de présence territoriale.

Les membres de la Commission supérieure ont conscience que le phénomène d'abstention massive observé lors des dernières élections régionales a des causes multifactorielles. En restant dans son champ de compétence, la Commission supérieure a souhaité expertiser les leviers qui pouvaient être mobilisés pour réduire la mal inscription, favoriser la pratique des procurations et réduire le taux d'abstention. Certaines recommandations ont été reprises dans les travaux conduits par nos collègues parlementaires et nous nous en réjouissons.

Enfin, la lutte contre la fracture numérique est un motif de préoccupation constant. La Commission supérieure s'est interrogée sur la gouvernance locale la plus adaptée des dispositifs d'inclusion numérique existant sur le territoire.

L'année 2022 sera marquée par des échéances électorales importantes. Le prochain gouvernement sera placé face à des choix stratégiques en matière d'infrastructures numériques et de télécommunication. Les missions de service public de La Poste doivent être définies pour s'adapter aux évolutions de notre société. La Commission supérieure du numérique et des postes prendra toute sa part en contribuant aux réflexions et débats sur ces sujets importants pour nos concitoyens.

Mireille Clapot

COMPOSITION ET MOUVEMENTS

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 la suite des élections sénatoriales de septembre 2020, le mandat de M. Yvon Collin, sénateur du Tarn-et-Garonne et Président de la Commission supérieure du numérique et des Postes, de M. Christian Manable, sénateur de la Somme, et de Mme Patricia Morhet-Richaud, sénatrice des Hautes-Alpes ont pris fin.

M. Gérard Larcher, Président du Sénat, a désigné leurs successeurs à la Commission supérieure le 27 janvier 2021 : Mme Toine Bourrat, sénatrice des Yvelines, M. Jean-Pierre Corbisez, sénateur du Pas-de-Calais et M. Franck Montaugé, sénateur du Gers.

Conformément au règlement intérieur de la Commission supérieure, M. Yvon Collin a assuré la présidence par intérim de la Commission supérieure jusqu'à l'élection du nouveau bureau le 11 février 2021.

Au cours de la séance d'installation du 11 février 2021, les membres de la Commission supérieure ont élu Mme Mireille Clapot, Présidente de la CSNP et un nouveau bureau :

- Mme. Toine Bourrat, sénatrice des Yvelines, première vice-présidente ;
- M. Bernard Delcros, sénateur du Cantal, deuxième vice-président ;
- M. Hervé Saulignac, député de l'Ardèche, secrétaire.

Pour convenance personnelle, M. Franck Montaugé a souhaité mettre fin à ses fonctions au sein de la Commission supérieure. Le Président du Sénat a désigné M. Christian Redon-Sarrazy, sénateur de la Haute-Vienne pour lui succéder le 28 juillet 2021.

Après le départ de Mme Anne-Marie Jean, secrétaire générale de la CSNP depuis janvier 2019, Mme Valérie Montané a été nommée secrétaire générale le 2 avril 2021.

M. Valentin Mugnié a pris ses fonctions de secrétaire général adjoint le 1er septembre 2021.

MEMBRES DE LA CSNP

Députés :

Mireille CLAPOT (La République en Marche), députée de la Drôme ; Présidente de la CSNP depuis le 11 février 2021 ; Membre de la Commission des Affaires étrangères ; Présidente du Groupe d'amitié France-Albanie ; Vice-Présidente du Groupe d'amitié France-Russie ;

Dominique DAVID (La République en Marche), députée de la Gironde ; Membre de la Commission des Finances de l'économie générale et du contrôle budgétaire.

Virginie DUBY-MULLER (Les Républicains), députée de la Haute-Savoie ; Membre de la Commission des Affaires culturelles et de l'éducation ; Présidente du Groupe de travail sur le statut des députés et leurs moyens de travail ; Présidente du Groupe d'amitié France-Ethiopie.

Jean-Paul DUFRÈGNE (Gauche Démocrate et Républicaine), député de l'Allier ; Membre de la Commission des Finances, de l'économie générale et du contrôle budgétaire ; Ancien Président du Conseil départemental de l'Allier ; Vice-Président du Groupe d'amitié France-Vietnam.

Christine HENNION (La République en Marche), députée des Hauts-de-Seine ; Vice-présidente de la CSNP jusqu'au 11 février 2021 ; Membre de la Commission des Affaires économiques ; Vice-Présidente du Groupe d'Amitié France-Japon.

Jean-Michel MIS (La République en Marche), député de la Loire ; Membre de Commission des lois constitutionnelles, de la législation et de l'administration générale de la République ; Vice-Président des Groupes Cybersécurité et souveraineté numérique et Santé et numérique.

Hervé SAULIGNAC (Nouvelle Gauche), député de l'Ardèche ; Membre de la Commission du développement durable et de l'aménagement du territoire ; Secrétaire du Groupe d'amitié France-Chine ; Ancien Président du Conseil départemental de l'Ardèche.

Sénateurs :

Toine BOURRAT, (Les Républicains), sénatrice des Yvelines, Première Vice-présidente de la CSNP depuis le 11 février 2021 ; Membre de la Commission de la culture, de l'éducation et de la communication, Membre de la Mission d'information sur le harcèlement scolaire et le cyberharcèlement.

Patrick CHAIZE (Les Républicains), sénateur de l'Ain ; Vice-Président de la Commission de l'aménagement du territoire et du développement durable ; Président du Groupe d'études Numérique ; Président de l'AVICCA.

Jean-Pierre CORBISEZ, (Rassemblement Démocratique et Social Européen), sénateur du Pas-de-Calais ; Membre de la Commission supérieure du numérique et des postes depuis le 11 février 2021 ; Vice-Président de la commission de l'aménagement du territoire et du développement durable ; Vice-Président de la délégation sénatoriale aux collectivités territoriales et à la décentralisation ; Membre de la délégation aux droits des femmes et à l'égalité des chances entre les hommes et les femmes.

Bernard DELCROS (Union Centriste), sénateur du Cantal ; Vice-Président de la Commission des finances, Secrétaire de la délégation sénatoriale aux collectivités territoriales et à la décentralisation

Martine FILLEUL (Socialiste et républicain), sénatrice du Nord ; Membre de la Commission de l'aménagement du territoire et du développement durable ; Présidente déléguée du Groupe d'amitié France-Afrique Centrale

Christian REDON-SARRAZY (Socialiste, Écologiste et Républicain), sénateur de la Haute-Vienne ; Membre de la commission des affaires économiques ; Membre de la délégation sénatoriale aux entreprises ; Vice-Président de la mission d'information sur le thème : « les influences étatiques extra-européennes dans le monde universitaire et académique français et leurs incidences » ; Président de la mission d'information sur le thème « Excellence de la recherche/innovation, pénurie de champions industriels : cherchez l'erreur française »

Denise SAINT-PÉ (Union Centriste), sénatrice des Pyrénées-Atlantiques ; Membre de la Commission des affaires économiques.

Personnalités qualifiées :

Henri d'AGRAIN, Délégué général du CIGREF

Jeanne BRETECHER, Dirigeante de Génération 2 et Présidente de Social Good Accelerator

Françoise SOKOLOWSKI, ancienne Secrétaire générale de l'Observatoire National de la Présence Postale

Secrétaire Générale :

Anne-Marie JEAN, jusqu'au 15 mars 2021

Valérie MONTANE, depuis le 2 avril 2021



Mireille CLAPOT
Députée de la Drôme



Toine BOURRAT
Sénatrice des Yvelines



Bernard DELCROS
Sénateur du Cantal



Hervé SAULIGNAC
Député de l'Ardèche



Patrick CHAIZE
Sénateur de l'Ain



Jean-Pierre CORBISEZ
Sénateur du Pas-de-Calais



Dominique DAVID
Députée de la Gironde



Virginie DUBY-MULLER
Députée de la Haute-Savoie



Jean-Paul DUFRÈGNE
Députée de l'Allier



Martine FILLEUL
Sénatrice du Nord



Christine HENNION
Députée des Hauts-de-Seine



Jean-Michel MIS
Député de la Loire



Christian REDON-SARRAZY
Sénateur de la haute-Vienne



Denise SAINT-PÉ
Sénatrice des Pyrénées-Atlantiques



Henri d'AGRAIN
Délégué général du CIGREF



Jeanne BRETECHER
Dirigeante de Génération 2 et
Présidente de Social Good
accelerator



Françoise SOKOLOWSKI
Ancienne Secrétaire générale de
l'Observatoire National de la
Présence Postale

LES MISSIONS

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.

Compte tenu de la nouvelle organisation instaurée en février 2021 par la nouvelle gouvernance, plusieurs groupes de travail ont été mis en place sur les sujets suivants :

- Sécurité numérique,
- Souveraineté numérique,
- Missions de services publics de La Poste,
- Feuille de route technologique de la France,
- Inclusion numérique, médiation et citoyenneté numérique,
- Numérique responsable et communs numériques,
- Sujets sociétaux et réglementaires.

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

En quelques chiffres, l'activité de la CSNP en 2021, c'est :

- 6 avis rendus,
- 13 séances plénières,
- 67 auditions et réunions en groupes de travail,
- 12 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 auditionnent ponctuellement des experts sur des sujets très précis et associent à leurs auditions et à leurs travaux un groupe d'experts associés aux profils différents : Henri d'Agrain, Délégué général du CIGREF, Jeanne Bretecher, Dirigeante de Génération 2 et Présidente de Social Good Accelerator et Françoise Sokolowski, ancienne Secrétaire générale de l'Observatoire National de la Présence Postale.

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

Les domaines d'intervention



Sécurité numérique



Souveraineté numérique



Feuille de route technologique
de la France



LA POSTE

Missions de services publics
de la Poste



Numérique responsable
et communs numériques



Inclusion numérique,
médiation et
citoyenneté numérique



Sujets sociétaux et
réglementaires

Les activités en quelques chiffres



6 avis rendus



13 séances plénières



67 auditions et réunions
en groupes de travail



12 participations et interventions
lors de colloques

LES MOYENS

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.

Au titre de l'année fiscale 2021, les crédits de fonctionnement consommés se sont élevés à 4 948 euros contre 6 149 euros en 2020 (Source : Ministère de l'économie, des finances et de la relance).

Compte tenu des contraintes liées au COVID, la CSNP n'a pas consommé intégralement ses plafonds de crédit qui étaient fixés à 15 000 euros et ont été reconduits au même niveau en 2022.

Conformément au décret n°2001-478 du 30 mai 2001, l'indemnisation des personnalités qualifiées a représenté une enveloppe annuelle de 17 949,60 euros en 2021.

Les personnels du Secrétariat général de la CSNP sont mis à disposition par le Ministère de l'Economie, des Finances et de la Relance. Les arbitrages pris par le Ministère de l'Economie, des Finances et de la Relance ont conduit à la réduction de la moitié des effectifs de la CSNP en 2020 qui sont passés de quatre ETP (Emplois Temps Plein) en janvier 2020 (une Secrétaire générale, une chargée de mission, une assistante, un chauffeur-assistant) à deux ETP en novembre 2020 (une secrétaire générale et une secrétaire générale adjointe).

Au 31 décembre 2021, les effectifs de la CSNP étaient composés de deux ETP (une secrétaire générale et un secrétaire général adjoint). Pour mémoire, à sa création, la CSNP comptait six emplois temps plein.

Ainsi que cela a été exprimé à plusieurs reprises, les membres de la CSNP sont favorables à une prise en charge des frais de personnels et de fonctionnement par l'Assemblée nationale et le Sénat mais, à ce stade, aucun accord n'a pu être trouvé par les deux assemblées.

LES PRIORITÉS DE LA CSNP

PRIORITÉS DE LA CSNP EN 2021

Entretien avec Mme Mireille Clapot, députée de la Drôme, Présidente de la CSNP



© Europe 1

Mireille Clapot, vous avez pris la présidence de la CSNP le 11 février 2021. Quelles ont été vos priorités pour la CSNP?

En prenant la présidence de la CSNP, j'ai souhaité, avec les membres du bureau et l'ensemble des membres, poursuivre l'engagement de la Commission supérieure sur les sujets prioritaires de l'accès de tous nos concitoyens aux services numériques et des télécommunications (téléphonie fixe, accès à internet, déploiement de la fibre et du très haut débit dans l'ensemble des territoires) et de la qualité des missions de service public confiées au groupe La Poste sur l'ensemble du territoire. Ces dossiers constituent le « socle » de compétence de la CSNP. Elue du département de la Drôme, je suis particulièrement sensibilisée aux problèmes d'entretien du réseau cuivre qui laissent certains usagers sans accès téléphonique pendant plusieurs jours voire plusieurs semaines. Cette situation est inacceptable et il y a urgence à agir. La CSNP participe depuis sa création à l'automne 2021 aux réunions du comité national Qualité de service cuivre piloté par le Secrétaire d'Etat chargé de la Transition numérique et des Communications électroniques. D'une manière générale, la Commission supérieure est très attachée à la qualité du service rendu aux usagers et nous alertons régulièrement les pouvoirs publics et l'Arcep sur les dysfonctionnements qui persistent notamment sur les problèmes de raccordement liés au mode « STOC ».

En tant que parlementaires, il nous paraît également important d'avoir une vision à long

terme des enjeux stratégiques pour notre pays et nous avons souhaité travailler de manière plus prospective en lançant un groupe de travail sur la « Feuille de route technologique de la France ».

Par ailleurs, depuis plusieurs années, les membres de la CSNP s'alarment de la progression exponentielle des cyberattaques. Nous attendions le plan d'accélération cyber présenté par le Président de la République en février 2021 avec impatience. C'est un plan essentiel qui met en place des moyens considérables, 1 milliard d'euros dont 720 millions de financements publics, pour améliorer le niveau de cybersécurité de l'écosystème.

Avec les membres de la Commission supérieure, nous avons cependant souhaité formuler plusieurs recommandations sur des sujets qui ne nous paraissent pas complètement ou pas encore couverts par ce plan.

« La Commission supérieure du numérique est très attachée à la qualité du service rendu aux usagers et nous alertons régulièrement les pouvoirs publics et l'Arcep sur les dysfonctionnements qui persistent notamment sur les problèmes de raccordement liés au mode « STOC ». »



© MC

Pouvez-vous préciser les recommandations de la CSNP dans le domaine de la sécurité numérique ?

Compte tenu de la gravité d'une situation sécuritaire qui ne cesse de se dégrader dans l'espace numérique, la CSNP a formulé un certain nombre de recommandations concrètes sur le renforcement de la lutte contre la cybercriminalité, les points d'amélioration du plan cyber, la stratégie de cyberdéfense de l'Etat français, la sécurité des produits et services numériques, le développement d'un cloud de confiance et la conduite des politiques publiques en faveur de la sécurité dans l'espace numérique.

Nous avons formulé 27 recommandations et je vous invite à en prendre connaissance.

Parmi ces recommandations, je citerai le renforcement des moyens judiciaires et une meilleure coopération au niveau européen et international : aujourd'hui, trois magistrats seulement traitent les dossiers de cybercriminalité en France alors que le nombre d'attaques augmente à un rythme exponentiel depuis deux ans. Les moyens dont dispose l'institution judiciaire pour traiter cette cyberdélinquance mondialisée et industrialisée est un sujet de préoccupation majeur pour les parlementaires membres de notre Commission. La CSNP recommande de renforcer la coopération judiciaire européenne et internationale et encourage une initiative française en vue de la création d'un véritable parquet européen spécialisé dans la cybercriminalité, dans la perspective de la Présidence française de l'Union européenne.

Une des recommandations de la CSNP porte sur le déploiement dans chaque région d'un CSIRT (Computer Security Incident Response Team - équipe de réponse aux incidents informatiques) incubé avec le soutien de l'ANSSI. La CSNP recommande que la création des CSIRT en région se fasse en étroite concertation avec les collectivités territoriales à l'échelle régionale.

Elle recommande notamment la création dans chaque région d'un campus régional de la sécurité numérique capable de fédérer localement les acteurs de la sécurité numérique, de les faire travailler en réseau, et

de sensibiliser l'écosystème public et privé à ces problématiques.

Les sujets de souveraineté numérique et de notre stratégie de cyberdéfense font également partie de nos recommandations : le conflit entre l'Ukraine et la Russie ne fait que confirmer l'absolue nécessité d'adapter notre dispositif national à la réalité évolutive et croissante de la cybermenace.

« La CSNP a formulé un certain nombre de recommandations concrètes sur le renforcement de la lutte contre la cybercriminalité, les points d'amélioration du plan cyber, la stratégie de cyberdéfense de l'Etat français, la sécurité des produits et services numériques, le développement d'un cloud de confiance et la conduite des politiques publiques en faveur de la sécurité dans l'espace numérique. »

Quelles sont les priorités de la CSNP pour 2022 ?

Dans le domaine postal, la CSNP aura à se prononcer sur le contrat d'entreprise qui sera renégocié cette année entre l'Etat et La Poste ainsi que sur le nouveau contrat de présence territoriale. Nous souhaitons que ces échéances soient l'opportunité de repenser les missions de service public confiées au groupe La Poste afin de mieux les adapter aux besoins des usagers.

Sur le volet numérique et télécommunication, nous souhaitons qu'un débat soit ouvert et que des solutions pérennes soient trouvées pour garantir aux français des infrastructures qui fonctionnent et soient entretenues pour que la notion de service universel ne soit pas un concept mais une réalité.

Enfin, nous devons nous projeter à long terme et identifier dès aujourd'hui les enjeux de souveraineté que posent les évolutions majeures du numérique.

ÉVOLUTION DES MISSIONS DE SERVICE PUBLIC DE LA POSTE

Entretien avec M. Patrick Chaize, sénateur de l'Ain, pilote du GT sur les sujets postaux



© La Gazette des communes

Vous pilotez au sein de la CSNP le groupe de travail sur les sujets postaux. En mars 2021, vous avez rendu un rapport sur l'avenir de La Poste, fait au nom de la commission des affaires économiques du Sénat présidée par Sophie Primas. Quels ont été les sujets marquants pour les missions de service publics de la Poste en 2021?

L'année 2021 a été une année décisive pour le financement de la mission du service universel postal. En raison de la baisse tendancielle du volume du courrier collecté et distribué, le service universel postal affichait depuis 2018 un déficit qui n'était pas compensé par l'Etat. Pour donner un ordre de grandeur, le volume du courrier a diminué de 39% entre 2010 et 2020. En 2020, la crise du COVID et ses effets sur l'activité économique ont accéléré la baisse du volume du courrier creusant le déficit à un niveau record de 1,3 milliard d'euros pour l'année 2020. Face à l'ampleur de ce déficit, l'Etat n'avait d'autre choix que de réagir.

Le Ministre de l'économie, des finances et de la relance a confié à M. Jean Launay, ancien député du Lot et ancien président de la CSNP, une mission en vue d'identifier des propositions concrètes pour adapter le service universel postal et identifier des solutions et des pistes de réforme.

Avec mes collègues sénateurs, Pierre Louault et Rémi Cardon, j'ai remis un rapport le 31 mars 2021 sur l'avenir de La Poste au nom de la commission des affaires économiques du Sénat appelant à compenser la mission de service universel postal. Nous avons proposé un mécanisme de compensation mixte, associant un levier fiscal, jusqu'à 270M€, et un levier budgétaire complémentaire, jusqu'à 730M€.

Dans son avis n°2021-02 du 8 mars 2021, les membres de la CSNP ont rappelé leur position : il est essentiel que l'Etat assume la juste compensation des coûts générés par la mise en œuvre des missions de service public. Les membres de la CSNP ne se sont pas prononcés sur la nature fiscale ou budgétaire de la compensation mais ont demandé que cette compensation soit claire et lisible pour les différents acteurs concernés (entreprise publique, collectivités et citoyens).

Sur la base de ces rapports et recommandations, le Premier ministre, en présence du ministre de l'économie, des finances et de la relance et de la ministre de la Cohésion des territoires et des Relations avec les collectivités locales, a présidé, le 22 juillet 2021, le comité de suivi de haut niveau du contrat d'entreprise entre l'Etat et La Poste.

L'année 2021 a été une année décisive pour le financement de la mission du service universel postal. (...) le volume du courrier a diminué de 39% entre 2010 et 2020. En 2020, la crise du COVID et ses effets sur l'activité économique ont accéléré la baisse du volume du courrier creusant le déficit à un niveau record de 1,3 milliard d'euros pour l'année 2020

Le Premier ministre a réaffirmé l'attachement de l'Etat aux missions de service public et aux actions d'intérêt général accomplies par La Poste et s'est prononcé en faveur d'une évolution du service universel postal avec la mise en œuvre d'ici à 2023 d'une nouvelle gamme centrée sur une offre à J+3.



© SIG - Service d'Information du Gouvernement

Sur le plan financier, le Premier ministre a annoncé le versement d'une dotation budgétaire annuelle, modulée en fonction des résultats de qualité de service, entre 500 et 520 millions d'euros.

Quelles sont les conséquences concrètes de cette décision pour nos concitoyens ?

En demandant à La Poste de centrer sa nouvelle gamme d'offre de distribution de courrier sur une offre à J+3 et non plus sur le J+1 ou le J+2, les autorités publiques s'adaptent à la réalité : en 2020, chaque ménage a envoyé en moyenne cinq courriers J+1, contre 45 en 2008.

La Commission supérieure n'était pas opposée à un tel aménagement qui correspond à l'évolution de notre société.

Pour autant, le facteur continuera de faire sa tournée six jours sur sept.

La Commission s'était prononcée en faveur du maintien de la distribution six jours sur sept, pour assurer non seulement au quotidien les services postaux traditionnels mais également en se plaçant dans la perspective d'une évolution des missions du Groupe La Poste qui intégrerait d'avantage de nouveaux services de proximité (services auprès d'une population isolée, services liés au vieillissement de la population, services à domicile, médiation numérique).

Quels sont les enjeux à venir sur les sujets postaux ?

Dans un avenir très proche, le contrat d'entreprise conclu entre l'Etat et le groupe La Poste pour la période 2018-2022 arrive à échéance. Un nouveau contrat devra être élaboré après les échéances électorales législa-



Depuis plusieurs années, la CSNP appelle de ses vœux une évolution des missions de service public telles qu'elles avaient été définies par la loi du 2 juillet 1990 en renforçant les missions de service à la personne et le rôle de la poste dans le domaine de l'inclusion numérique.»

tives. En tout état de cause, les membres de la CSNP étudieront de très près les nouveaux équilibres de ce contrat et se montreront extrêmement vigilants sur la qualité de service dans sa mise en œuvre.

S'agissant plus particulièrement de la mission d'aménagement du territoire confiée à La Poste, le Premier ministre avait annoncé en juillet 2021 que le Gouvernement était prêt à maintenir le niveau de son soutien financier à cette mission.

La négociation du prochain contrat de présence postale territoriale conclu entre La Poste, l'Association des maires de France et des présidents d'intercommunalités (AMF) et l'Etat pour la période 2023 - 2025 sera déterminante.

Depuis plusieurs années, la CSNP appelle de ses vœux une évolution des missions de service public telles qu'elles avaient été définies par la loi du 2 juillet 1990 en renforçant les missions de service à la personne et le rôle de la poste dans le domaine de l'inclusion numérique.



POLITIQUE D'INCLUSION NUMÉRIQUE : LES DÉPARTEMENTS AUX AVANT-POSTES

Entretien avec Mme Martine Filleul, sénatrice du Nord , pilote du GT Inclusion numérique



© Les Bons Clics

Pour quelles raisons avez-vous souhaité organiser l'atelier « Politique d'inclusion numérique : les départements aux avant-postes » le 25 novembre 2021?

Nous souhaitons faire la preuve avec le groupe de travail sur l'inclusion numérique de la Commission Supérieure du Numérique et des Postes que les départements étaient très impliqués dans la lutte contre l'illectronisme. De ce point de vue, cet atelier est véritablement une réussite : 5 conseillers départementaux ont participé à cet atelier ainsi que des représentants de l'Association des départements de France et Département Solidaire. Ces acteurs de terrain nous ont rendu compte des expériences et des innovations qu'ils menaient. Ils nous ont expliqué comment ils posaient les diagnostics et les constats en matière de fracture numérique et ont partagé avec nous les problèmes de cohérence, de pilotage et de coordination des politiques publiques en matière d'inclusion numérique.

Les élus départementaux présents ont tous fait état des mêmes difficultés rencontrées par leurs administrés, quelles que soient la géographie et la diversité de la population de leur territoire.

Ils s'accordent tous pour dire que l'échelon départemental permet de donner une cohérence et une ambition aux actions menées en matière de lutte contre l'illectronisme, notamment en capitalisant sur les actions déployées par les communes et les partenaires. Cette transversalité de l'échelon départemental se concrétise par la signature de partenariats

avec des acteurs publics et privés, actifs dans l'inclusion numérique.

Les départements, à travers l'accompagnement social qu'ils assurent, possèdent une source de données incomparable sur l'état des populations en fragilité, qu'il s'agisse de difficultés géographiques mais aussi économiques, sanitaires, familiales et sociales. Ces données permettent d'être plus efficace et de mieux cibler les publics et les besoins en matière de lutte contre l'exclusion numérique car, en la matière, il faut une connaissance presque personnelle des usagers.



L'échelon départemental permet de donner une cohérence et une ambition aux actions menées en matière de lutte contre l'illectronisme, notamment en capitalisant sur les actions déployées par les communes et les partenaires. »

Précisément, quels sont les obstacles qui persistent dans le déploiement des actions d'inclusion numérique au niveau des départements?

Tout d'abord, je pense que les acteurs départementaux sont confrontés à une question de moyens: leurs moyens sont contraints par leur budget et le niveau des dotations qui leur sont affectées pour lutter contre les inégalités territoriales et les inégalités sociales. Les départements sont également contraints par le manque de reconnaissance de cette collectivité



pour piloter la politique d'inclusion numérique.

D'une manière générale, les départements font le constat que l'Etat a mis en œuvre un certain nombre de moyens dont font partie les conseillers numériques. Pourtant, ils sont parfois utilisés à d'autres missions que l'inclusion numérique. Aussi, ils ne sont pas immédiatement opérationnels, car ils ne disposent pas toujours des éléments d'information sur leurs missions ou sur leur localisation territoriale.

Quelles sont les conclusions de cet atelier en matière de pilotage des politiques d'inclusion numérique ?

L'inclusion numérique est à la croisée des compétences et des acteurs. De très nombreux acteurs interviennent dans la lutte contre l'illectronisme. La gouvernance est donc un sujet essentiel. Une clarification des rôles est nécessaire.

Par ailleurs, pour reprendre les propos de Madame Christine Gonzato-Roque, vice-présidente du département Lot-et-Garonne, « s'il n'y a pas de pilotage de l'inclusion numérique, il n'y a qu'un saupoudrage ».

Tous les élus présents s'accordent à dire qu'il faut que la compétence de lutte contre l'exclusion numérique soit clairement dévolue aux départements, et souhaitent obtenir les moyens humains et financiers correspondants.

L'ANCT et la Banque des territoires appellent de leurs vœux la mise en place d'une gouvernance ouverte en donnant au département un rôle de coordination.

De fait, le département joue déjà le rôle de coordinateur du déploiement mais aussi de l'animation du réseau de conseillers numériques mis en place par l'ANCT.

La Poste, très engagée sur la lutte contre l'illectronisme, s'est également montrée intéressée sur la coordination départementale.



« L'inclusion numérique est à la croisée des compétences et des acteurs. De très nombreux acteurs interviennent dans la lutte contre l'illectronisme. La gouvernance est donc un sujet essentiel. Une clarification des rôles est nécessaire. »

MODERNISATION ET APPORT DU NUMÉRIQUE AUX PROCESSUS ÉLECTORAUX

Entretien avec M. Hervé Saulignac, député de l'Ardèche



© Compte Twitter @hsaulignac

Pour quelle raison la CSNP a-t-elle souhaité travailler sur l'amélioration et sur les apports du numérique aux processus électoraux ?

Cette réflexion de la Commission part d'un constat : les élections régionales et départementales de juin 2021 ont été marquées par une abstention record puisque deux électeurs sur trois ont fait le choix de ne pas se rendre aux urnes.

Les raisons de l'abstention sont multifactorielles mais plusieurs obstacles pratiques ou techniques pourraient être levés et de nouvelles initiatives devraient être expérimentées.

Le numérique peut être un moyen d'y parvenir. C'est en ce sens que nous avons formulé dix recommandations visant à favoriser la participation dans l'avis n°2021-05 du 10 novembre 2021.

L'une de vos recommandations porte sur la procédure d'inscription sur les listes électorales. Comment les démarches peuvent-elles être facilitées ?

15 % des inscrits sur les listes électorales, soit plus de 7 millions d'électeurs, sont mal inscrits car enregistrés sur les listes électorales à une autre adresse que celle de leur résidence principale. Ceci a une incidence directe sur les chiffres de la participation électorale. Il est donc essentiel de simplifier les procédures d'inscription sur les listes électorales et de réduire de manière significative les démarches

pour nos concitoyens. Elles imposent une démarche volontaire qui peut leur paraître trop lourde ou chronophage. Cette situation, qui empêche une part très importante de l'électorat de voter près de son lieu de résidence, n'est pas tenable.

La CSNP propose donc que les citoyens français soient inscrits automatiquement sur les listes électorales à l'occasion de l'accomplissement de démarches administratives telles que la déclaration d'impôts ou le versement de prestations sociales.

« Il est essentiel de simplifier les procédures d'inscription sur les listes électorales et de réduire de manière significative les démarches pour nos concitoyens. »

Le vote par internet est régulièrement cité dans le débat public en tant que moyen de lutte contre l'abstention. Quelle est la position de la CSNP sur un recours possible à cette modalité de vote ?

Les auditions conduites dans le cadre de nos travaux ont mis l'accent sur les difficultés substantielles que soulèverait une généralisation du vote par internet en termes de sécurisation du scrutin, d'identification et d'authentification des électeurs ainsi que de vérifiabilité et de secret du vote.

Les tentatives d'ingérence dans des élections nationales ces dernières années, visant à créer du trouble pour mettre en tension des pays démocratiques comme la France, plaident pour une approche prudente sur ce sujet.

Les membres de la CSNP souhaitent que la recherche de solutions technologiques adaptées aux exigences de la vie démocratique soit encouragée. L'accélération du déploiement d'une identité numérique fiable et sécurisée pour l'ensemble du corps électoral constitue, de notre point de vue, une condition préalable à la sécurisation des processus d'identification et d'authentification dans le cadre du parcours votant.



© Wikipedia Commons

Quelle est la position de la CSNP sur les machines à voter ?

S'agissant des machines à voter qui existent déjà dans certains bureaux de vote, nous proposons de lever le moratoire décidé en 2008 qui rend impossible le recours aux machines de vote dans les communes non équipées et entraîne l'obsolescence des machines déjà installées.

Les membres de la CSNP sont favorables à l'expérimentation afin de tendre vers des machines plus fiables et sécurisées, en lien étroit avec les services de l'Agence nationale de la sécurité des systèmes d'information.

Si l'abstention aux échéances électorales traditionnelles est massive, nous observons également une très forte mobilisation de nos concitoyens pour contribuer à une démocratie plus participative sur les sujets ou projets locaux: ces machines électroniques pourraient à l'avenir être plus et mieux utilisées à condition bien sûr d'être modernisées et sécurisées.



© Adobe Stock

« Les auditions conduites dans le cadre de nos travaux ont mis l'accent sur les difficultés substantielles que soulèverait une généralisation du vote par internet en termes de sécurisation du scrutin, d'identification et d'authentification des électeurs ainsi que de vérifiabilité et de secret du vote. »

AGENDA 2021

JANVIER

11 janvier

- Réunion de travail sur les sujets postaux

13 janvier

- Audition de la Fédération française des télécoms
- Audition de l'Association des Maires de France
- Audition de l'Arcep

14 janvier

- Audition de l'Avicca
- Audition de la DGCCRF

15 janvier

- Audition d'Alternative Telecom

25 janvier

- Réunion de travail sur l'inclusion numérique

26 janvier

- Audition d'Infranum

28 janvier

- Participation à l'ONPP

29 janvier

- Audition de la Direction générale des entreprises

FÉVRIER

3 février

- Réunion de travail avec l'APTIC
- Réunion de travail sur le gouvernement ouvert

11 février

- Séance plénière
- Election du nouveau bureau de la CSNP

16 février

- Publication de l'avis n°2021-01 sur la transposition de la Directive (UE) 2018/1972 établissant le code des communications électroniques européen

17 février

- Réunion du bureau de la CSNP

25 février

- Réunion de travail sur les sujets postaux



MARS

2 mars

- Réunion de travail avec Le groupe La Poste
- Réunion du bureau de la CSNP

3 mars

- Séance plénière

4 mars

- Réunion avec le cabinet du Secrétaire d'Etat sur le plan d'accélération cyber

8 mars

- Publication de l'avis n° 2021-02 sur l'évolution des missions de service public de La Poste
- Réunion de travail avec Free

9 mars

- Réunion de travail avec le CIGREF

15 mars

- Réunion de travail avec les représentants de l'OCDE sur la sécurité numérique

16 mars

- Participation à l'Orange Business Summit
- Réunion du bureau

17 mars

- Audition de l'OCDE et du CIGREF sur la sécurité numérique

23 mars

- Réunion de travail

24 mars

- Entretien avec la DGE
- Audition de Myriam Quemener sur le volet judiciaire de la sécurité numérique

29 mars

- Réunion de travail avec l'AMF

30 mars

- Audition de Gerome Billois sur la sécurité numérique

31 mars

- Séance plénière
- Auditions de l'ARCEP et de l'ANSSI

AVRIL

1er avril

- Réunion de travail avec Aromates

7 avril

- Réunion de travail sur la sécurité numérique

9 avril

- Audition du département cybersécurité au Commissariat à l'Energie Atomique

15 avril

- Séance plénière
- Audition du Pôle d'Expertise de la Régulation Numérique

21 avril

- Réunion de travail sur la sécurité numérique

28 avril

- Réunion de travail sur la sécurité numérique

29 avril

- Publication de l'avis n°2021-03 portant recommandations dans le domaine de la sécurité numérique



MAI

4 mai

- Réunion de travail avec la FFT

6 mai

- **Séance plénière**

- Audition du Health Data Hub

11 mai

- Réunion avec l'AVICCA

18 mai

- Réunion de bureau

19 mai

- Audition de Free

20 mai

- **Séance plénière**

- Auditions de la FFT

et de la Médiatrice des communications électroniques

25 mai

- Réunion de travail avec La Poste

26 mai

- Réunion de travail sur les 3èmes Assises de la Cohésion numérique et territoriale

JUIN

3 juin

- Participation de la CSNP aux 3èmes Assises de la Cohésion numérique et territoriale

9 juin

- Réunion avec le cabinet du Ministre de l'Économie, des Finances et de la Relance sur la compensation du déficit de la mission du service universel postal et sur les principales recommandations de l'avis de la CSNP sur la sécurité numérique.

10 juin

- Publication de l'avis n°2020-04 portant contribution de la CSNP sur les nouvelles technologies dans le domaine de la sécurité

15 juin

- Contribution à la mission relative aux nouvelles technologies dans le domaine de la sécurité

16 juin

- Participation de la CSNP au salon Vivatech 2021

17 juin

- Entretien avec le Directeur général du Campus Cyber

- Participation à l'ONPP

22 juin

- Réunion de travail avec La Poste

23 juin

- Participation de la CSNP aux 15èmes assises du Très Haut Débit

24 juin

- Entretien avec le Conseiller numérique du Président de la République

29 juin

- Réunion du bureau



JUILLET

1er juillet

- Audition de Mme Marion Lenne, députée de la Haute-Savoie et M. Alain David, Député de la Gironde co-rapporteurs du rapport d'information n° 4213 sur les Géants du numérique

12 juillet

- Réunion de travail sur les sujets postaux

16 juillet

- Réunion de travail sur les sujets postaux

19 juillet

- Audition du Président-Directeur Général du Groupe La Poste

26 juillet

- Réunion du Comité de suivi de haut niveau à Matignon

22 juillet

- Petit-déjeuner avec des représentants du Cybercercle

29 juillet

- Audition de M. Eric Lombard, Directeur général du Groupe Caisse des Dépôts

30 juillet

- Audition de M. Thomas Courbe, Directeur général des entreprises



SEPTEMBRE

6 septembre

- Réunion de travail avec La Poste

7, 8 et 9 septembre

- Participation de la CSNP au Forum International de la cybersécurité à Lille

13 septembre

- Réunion de travail avec le MEAE

14 septembre

- Rencontre avec les représentants du groupe ALTICE-SFR

15 septembre

- Audition de Mme Véronique Cortier, directrice de recherche au Centre national de la recherche scientifique (CNRS), spécialiste des protocoles de sécurité informatique

20 septembre

- Réunion de travail avec la DGE

21 septembre

- Réunion de travail feuille de route technologique de la France

22 septembre

- Auditions de M. Romain Rambaud, professeur des universités, agrégé de droit public, Université Grenoble-Alpes et de Mme Céline Braconnier, directrice de Sciences Po Saint-Germain-en-Laye, professeure de sciences politiques, chercheuse au centre de recherches sociologiques sur le droit et les institutions pénales (CESDIP)

28 septembre

- Audition de la CNIL

29 septembre

- Audition de l'ANSSI

OCTOBRE

1er octobre

- Séance plénière

5 octobre

- Participation de la CSNP à l'Observatoire national de la présence postale

6 octobre

- Participation de la CSNP à la 21ème Rencontre des Présidents de CDPPT

7 octobre

- Rencontre avec Scaleway

13 octobre

- Audition de la Direction des français de l'étranger et de l'administration consulaire
- Réunion de travail sur la modernisation et les apports du numérique au processus électoral
19 octobre - réunion de travail avec la DGE

21 octobre

- Participation de la CSNP à la réunion du comité national Cuivre
- Séance plénière

28 octobre

- Intervention de la Présidente de la CSNP à la Matinale du Cybercercle
- Auditions du Groupe La Poste et de Docaposte

29 octobre

- Réunion avec le cabinet du Garde des sceaux



NOVEMBRE

3 novembre

- Réunion de travail avec le groupe La Poste sur le coût net de la mission d'aménagement du territoire

5 novembre

- Réunion de travail avec Free

9 novembre

- Réunion de travail avec la FFT

10 novembre

- Réunion de travail avec l'Arcep
- Publication de l'avis n° 2021-05 sur la modernisation et les apports du numérique aux processus électoraux

15 novembre

- Réunion de travail sur les sujets postaux

18 novembre

- Participation au congrès de l'Association des Maires de France

19 novembre

- Auditions de l'Arcep et du groupe La Poste sur le coût net de la mission d'aménagement du territoire

20 novembre

- Réunion de travail avec l'Arcep sur le coût net de la mission d'aménagement du territoire

24 novembre

- Séance plénière

25 novembre

- Atelier « Inclusion numérique : les départements aux avant-postes » organisé par Mme Martine Filleul, Sénatrice du Nord et pilote du GT Inclusion numérique de la CSNP

DÉCEMBRE

1er décembre

- Participation à l'inauguration de l'INRIA à Lyon

8 décembre

- Séance plénière
- Audition du groupe Free-Iliad
- Publication de l'avis n°2021-06 sur le projet de rapport sur le coût net en 2020 de la mission d'aménagement du territoire assurée par La Poste

16 décembre

- Entretien avec Tehtris



AVIS RENDUS EN 2021

SOMMAIRE DES AVIS RENDUS EN 2021

Avis 2021-01 du 16 février 2021 portant sur la transposition du Code des communications électroniques européen.....	p. 29
Avis 2021-02 du 8 mars 2021 sur l'évolution des missions de service public de La Poste.....	p. 34
Avis 2021-03 du 29 avril 2021 portant recommandations sur la sécurité numérique.....	p. 39
Avis 2021-04 du 10 juin 2021 portant contribution à la mission relative aux nouvelles technologies dans le domaine de la sécurité.....	p. 51
Avis 2021-05 du 10 novembre 2021 sur la modernisation et les apports du numérique aux processus électoraux.....	p.59
Avis 2021-06 du 8 décembre 2021 sur l'évaluation du coût net de la mission d'aménagement du territoire 2020.....	p. 70



COMMISSION SUPERIEURE DU NUMERIQUE ET DES POSTES

**AVIS N°2021-01 DU 16 FEVRIER 2021
PORTANT SUR LA TRANSPOSITION DE LA DIRECTIVE (UE) 2018/1972
DU PARLEMENT EUROPEEN ET DU CONSEIL DU 11 DECEMBRE 2018
ETABLISSANT LE CODE DES COMMUNICATIONS ELECTRONIQUES
EUROPEEN ET ADAPTANT CERTAINS POUVOIRS DE L'ARCEP**

Vu la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen ;

Vu la loi n° 2020-1508 du 3 décembre 2020 portant diverses dispositions d'adaptation au droit de l'Union européenne en matière économique et financière ;

Vu l'article L.43 du Code des postes et des communications électroniques modifiant l'arrêté du 17 décembre 2007 pris en application de l'article R. 20-44-11 du code des postes et des communications électroniques et relatif aux conditions d'implantation de certaines installations et stations radioélectriques ;

Vu la saisine du 19 décembre 2020 du Directeur général des entreprises ;

Lancées en 2016, les négociations sur le nouveau code européen des communications électroniques ont abouti à l'adoption de la Directive (UE) 2018/1972 du Parlement européen et du Conseil de l'Union européenne du 11 décembre 2018 établissant le Code des communications électroniques européen¹. Les Etats membres avaient jusqu'au 21 décembre 2020 pour adopter et publier les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la directive.

Après avoir envisagé de transposer la totalité des dispositions du nouveau Code européen des communications électroniques par ordonnance, le gouvernement a proposé au Parlement la transposition d'une partie des dispositions de ce Code, notamment celles qui relèvent du service universel et du déploiement de la 5G, dans le cadre des débats parlementaires relatifs à la loi Ddadue et a choisi de transposer par ordonnance, par décrets et par arrêté les dispositions jugées plus techniques. Ce sont ces derniers textes qui sont soumis pour avis à la Commission supérieure.

Le présent avis de la Commission supérieure du numérique et des postes est donc relatif :

- au projet d'ordonnance portant transposition de la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen et relative aux mesures d'adaptation des pouvoirs de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse,
- au projet de décret portant diverses mesures de transposition de la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen,
- au projet de décret modifiant les obligations des opérateurs de communications électroniques conformément au code des communications électroniques européen,
- au projet d'arrêté pris en application de l'article L.43 du code des postes et des communications électroniques modifiant l'arrêté du 17 décembre 2007 pris en application de l'article R. 20-44-11 du code des postes et des communications électroniques et relatif aux conditions d'implantation de certaines installations et stations radioélectriques.

¹ <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32018L1972&from=EN>

En vue de rendre le présent avis, la Commission supérieure a auditionné Thomas Courbe, Directeur général des entreprises, et organisé plusieurs auditions avec les autorités, administrations et entités concernées par cette transposition :

- Les représentants de l'ARCEP et de l'administration :
 - l'ARCEP, Autorité de régulation des communications électroniques, des postes et de la distribution de la presse ;
 - la Direction générale de la Concurrence, de la Consommation et de la Répression des Fraudes ;
 - les représentants des opérateurs de communications électroniques et des industries d'infrastructure:
 - la Fédération Française des Télécommunications ;
 - Alternative Telecom, association qui défend les intérêts des opérateurs alternatifs de télécommunications fixes et mobiles ;
 - la Fédération InfraNum qui regroupe les partenaires industriels des territoires connectés et de l'aménagement numérique des territoires ;
 - Les représentants des collectivités locales :
 - l'Association des Maires de France et des présidents d'intercommunalités ;
 - l'AVICCA, qui regroupe les collectivités territoriales engagées dans le numérique pour faciliter l'échange des pratiques dans le domaine des infrastructures et des réseaux, le numérique éducatif, les SIG, les territoires intelligents, la communication territoriale sur les déploiements, l'audiovisuel.
1. La CSNP se félicite que le gouvernement ait suivi la recommandation formulée dans son avis du 3 mars 2020 en portant devant le Parlement, et non par ordonnance comme initialement prévu, les aspects les plus politiques de la transposition du Code européen des communications électroniques, notamment l'extension du service universel à la fourniture du très haut débit ou la mise en œuvre de communications électroniques à un tarif abordable. Il était en effet essentiel que les parlementaires puissent débattre des dispositions portant sur la transposition des articles 39 et 40 de la loi Ddadue. La définition retenue par le projet de décret sur le service universel est également conforme à l'avis rendu par la Commission supérieure le 3 mars 2020.
 2. Les membres de la Commission supérieure notent une frustration certaine de la plupart des acteurs entendus dans le cadre des auditions. En effet, le processus d'élaboration de la directive et d'instruction de la transposition s'est avéré particulièrement long et complexe pour, *in fine*, ne pas modifier grand-chose aux dispositions actuelles. Face à ce constat, la Commission supérieure exprime sa satisfaction, qu'au cours de ce long processus, les positions françaises aient pu prévaloir la plupart du temps, en minimisant l'impact de la transposition sur les pratiques nationales dans le secteur des télécommunications électroniques. En revanche, les membres de la Commission supérieure estiment que la directive et sa transposition constituent **une occasion manquée pour mettre en place une véritable politique industrielle garantissant la**

souveraineté française et européenne dans le domaine des communications électroniques.

Les membres de la Commission supérieure relèvent une étape encore timide vers une supervision renforcée à l'égard des opérateurs de service par contournement (en anglais *Over-The-Top service* OTT). Si les membres de la Commission supérieure se félicitent que les opérateurs de service par contournement entrent désormais dans le champ d'application du Code des communications électroniques, ils regrettent que ces acteurs ne soient pas soumis à des règles aussi contraignantes que celles applicables aux opérateurs de télécommunications historiques.

3. Pour la Commission supérieure, il est essentiel que les discussions en cours dans le cadre du Digital Services Act et du Digital Markets Act abordent **la régulation des opérateurs de service par contournement** de manière plus efficiente, en adoptant une approche moins timorée et plus adaptée à la complexité posée par la régulation des GAFAM qui pourront être définis comme des plateformes structurantes ou contrôleurs d'accès (*gatekeepers*).
4. **S'agissant de la mise en œuvre effective du service universel dans les territoires**, il est apparu à l'occasion des auditions conduites par la Commission supérieure que les débats parlementaires engagés au titre de la loi Ddadue n'avaient pas complètement répondu aux interrogations et aux craintes des parties prenantes (usagers, opérateurs de télécommunications, élus) sur **les modalités du désengagement d'Orange en tant qu'opérateur historique du service universel et plus généralement sur les aspects concurrentiels de l'écosystème des communications électroniques**.

Dans ces conditions, le plan d'action annoncé pour la mi-mars 2021 par le Secrétaire d'Etat chargé de la Transition numérique et des Communications électroniques en réponse aux propositions formulées par Mme Celia de Lavergne, Députée de la Drôme, chargée d'une "mission flash" sur le réseau cuivre (prolongation de cinq ans la mission d'Orange sur le service universel du téléphone notamment) sera examiné attentivement par les membres de la Commission supérieure. En tout état de cause, les membres de la Commission supérieure préconisent que l'ARCEP, en liaison avec la Direction générale des entreprises, puisse apporter aux opérateurs de télécommunication et aux collectivités locales les précisions attendues.

Pour garantir la qualité du service universel proposé aux usagers, les membres de la Commission supérieure proposent que les textes précisent que **le service universel soit apporté avec la meilleure technologie disponible localement, notamment la fibre lorsque la commune est fibrée**.

S'agissant du volet tarifaire du service universel, les membres de la Commission supérieure approuvent les mesures mises en œuvre pour **garantir à nos concitoyens les plus fragiles un accès aux services de communications électroniques à un tarif abordable**. Si le niveau actuel de tarification de ces services pratiqué par les opérateurs français est plutôt dans la fourchette basse des prix pratiqués dans l'Union européenne, les membres de la Commission supérieure entendent rester vigilants sur l'équité des tarifs applicables aux consommateurs et usagers français sur l'ensemble du territoire pour accéder aux services numériques de base: la baisse des prix des services de téléphone mobile est absorbée par la part croissante des biens et services des TCSI dans le budget des ménages

français en raison de la hausse des dépenses pré-engagées dans les services de télécommunication (abonnements téléphoniques, aux chaînes de radio et de télévision par câble ou satellite, Internet).

5. **L'extension des mesures protectrices du consommateur aux micro-entreprises et aux TPE** est introduite par l'article 45 du projet d'ordonnance, qui précise que toute micro-entreprise ou petite entreprise au sens de la recommandation 2003/361/CE pourra bénéficier des dispositions des articles L. 224-27, L. 224-28 (I°, L. 224-29, L. 224-30, L. 224.-42 et L.224-42 (I et III) du Code de la Consommation. **Les membres de la Commission supérieure saluent cette avancée et veilleront à ce que, dans la pratique, les prestataires de services aux TPE n'imposent pas à celles-ci de renoncer à tout ou partie de ces dispositions protectrices.**

Par ailleurs, l'extension en droit de la concurrence de la notion « d'utilisateur final » aux utilisateurs des entreprises de taille intermédiaire et des grandes entreprises laisse perplexes les membres de la Commission et inquiète les organisations représentatives des opérateurs de télécommunication.

6. Les membres de la Commission supérieure sont attentifs aux préoccupations des élus locaux qui leur ont fait part de leur **inquiétude vis-à-vis du nouveau champ des autorisations mis en place par les articles 7 et 12 de l'ordonnance** et par l'arrêté relatif aux points d'accès sans fil à portée limitée ou *small cells*. Ces élus de terrain craignent, en effet, un déficit d'information relatif aux travaux ou aux installations effectués par les opérateurs dans leur territoire et de ne pas disposer d'éléments suffisants pour répondre aux interrogations de leurs administrés sur ces installations, alors qu'ils sont pourtant parfois les seuls interlocuteurs présents sur le terrain.

Pour répondre à ces préoccupations légitimes des élus locaux, sans entraver la simplification de procédures et ralentir le déploiement des infrastructures, les membres de la Commission supérieure préconisent qu'une information systématique des élus soit mise en place par le biais d'une plateforme d'information alimentée par les opérateurs et accessible aux élus. Ce dispositif pourrait être piloté dans un mode conventionnel par l'Agence Nationale des Fréquences.

Sous réserve de ces observations, la Commission supérieure du numérique et des postes émet un avis positif sur les textes portant transposition de la Directive (UE) 2018/1972 du Parlement du Parlement européen et du conseil du 11 décembre 2018 établissant le Code des communications électroniques européen et adaptant certains pouvoirs de l'ARCEP.

sur l'évolution des missions de service public de la Poste



Depuis plusieurs années, la Commission Supérieure du Numérique et des Postes souhaite que les missions de service public confiées au Groupe La Poste soient repensées et évoluent. Avec l'évolution des usages et de la société française, le contenu des missions de service public confiées au groupe La Poste et définies par la loi n°90-568 du 2 juillet 1990 (service postal universel, aménagement du territoire, accessibilité bancaire et distribution de la presse) répond imparfaitement aux besoins des usagers.

La crise économique et sanitaire de 2020 n'a fait qu'accélérer ces tendances et les questions de financement posées par l'effondrement du volume du courrier appellent à une redéfinition des missions et des moyens des missions de service public confiées au groupe La Poste.

La CSNP souhaite donc formuler plusieurs recommandations :

1/ Redéfinition des missions de service public confiées au groupe La Poste

- Intégrer le facteur comme un acteur essentiel de la mission d'aménagement du territoire notamment dans les territoires ruraux et non, comme c'est le cas aujourd'hui, considérer son rôle uniquement dans le cadre du service universel postal
- Inclure le service à la personne (ou services de proximité aux personnes fragiles) et l'inclusion numérique, dont les bonnes pratiques de cybersécurité, dans le périmètre des missions de service public confiées à La Poste
- Améliorer la formation et l'accompagnement des postiers dans l'évolution de leurs métiers

2/ Financement des missions de service public confiées à La Poste

- Repenser l'examen des coûts des missions de service public
- Prise en compte de l'évaluation des coûts dus à la non-qualité
- Compenser les coûts des missions de service public confiées à La Poste par l'Etat (compensation de nature fiscale ou de nature budgétaire)
- Améliorer la clarté et la lisibilité de la compensation financière pour les différents acteurs concernés (entreprise publique, collectivités locales et citoyens)
- Prévoir ou maintenir un engagement pluriannuel pour permettre à l'ensemble des parties prenantes d'inscrire efficacement leur action dans la durée (déploiement des effectifs, dotations)

3/ Gouvernance effective des missions de service public sur le modèle de l'Observatoire National de la Présence Postale

4/ Maintien d'une distribution six jours sur sept sur l'ensemble du territoire pour la presse, le courrier et les colis

5/ Réflexion sur l'obligation d'acheminement à J+1 du courrier prioritaire (timbre rouge)

- Disposer de toutes les données pertinentes (simulation financière, réorganisation industrielle...) sur les conséquences de la levée de cette obligation

L'intégralité de l'avis est consultable sur www.csnp.fr/avis/





COMMISSION SUPERIEURE DU NUMERIQUE ET DES POSTES

AVIS N°2021-03 DU 29 AVRIL 2021

PORTANT RECOMMANDATIONS

DANS LE DOMAINE DE LA SECURITE NUMERIQUE

Les attaques dans l'espace numérique se sont multipliées à un rythme quasi-exponentiel ces deux dernières années, partout dans le monde. Tous les experts auditionnés par notre Commission nous ont fait part de leurs inquiétudes. Ils ont confirmé que la situation sécuritaire dans l'espace numérique est désormais particulièrement préoccupante et qu'elle devrait continuer à se dégrader dans les années qui viennent. La capacité des cybercriminels à commettre leurs forfaits s'est professionnalisée, mondialisée et industrialisée, et croît plus rapidement que celle de leurs victimes à se protéger. Les principales puissances numériques elles-mêmes, à commencer par les Etats-Unis, la Chine et la Russie, sont au bord du cyber-affrontement. A ce rythme, si la France et l'Europe ne prennent pas rapidement la mesure du défi sécuritaire auquel nous sommes collectivement confrontés, et n'adoptent pas des mesures vigoureuses permettant de changer les paradigmes de la sécurité dans l'espace numérique, nos Etats, notre économie, nos concitoyens, le fonctionnement même de nos démocraties pourraient être confrontés au chaos numérique à l'horizon de la prochaine décennie. Cette sombre perspective n'est hélas pas qu'une simple hypothèse ou une vue de l'esprit, mais un scénario plausible qui prolonge le caractère exponentiel de la croissance des cybermenaces observée au cours de ces dernières années.

La stratégie nationale pour la cybersécurité, présentée par le Président de la République le 18 février dernier, et pilotée par le Secrétaire d'Etat chargé de la Transition numérique et des communications électroniques, est un plan ambitieux. Elle apporte un certain nombre de réponses à des besoins identifiés en mobilisant des financements importants - 1 milliard d'euros dont 720 millions de financements publics – qui devraient permettre de réduire les vulnérabilités des systèmes informatiques de nombreuses infrastructures publiques et privées.

Pour autant, une stratégie nationale pour la sécurité dans l'espace numérique ne peut se limiter à un tel plan, aussi nécessaire soit-il. La cybersécurité ne constitue qu'un volet des mesures qui permettront, à terme, de renforcer le niveau global de la sécurité dans l'espace numérique dont l'Etat français, les services publics nationaux, les collectivités territoriales, les entreprises et nos concitoyens ont désormais une absolue nécessité. C'est en articulant l'ensemble de ces volets que l'Etat sera en mesure d'assurer l'ordre public et la sécurité des biens et des personnes dans l'espace numérique au même titre que dans l'espace physique. A cet égard, les mesures de renforcement des capacités de lutte contre la cybercriminalité apparaissent comme prioritaires.

Enfin, il est essentiel que la sécurité numérique soit mieux comprise par nos concitoyens. Ils doivent être instruits des menaces auxquelles ils peuvent être confrontés dans leurs usages du numérique, que ce soit dans leurs usages numériques du quotidien, en utilisant des objets connectés ou dans le cadre du télétravail qu'ils sont de plus en plus nombreux à pratiquer, et qui peuvent mettre en cause la protection de leurs données personnelles.

Au terme de ses auditions, la CSNP a souhaité émettre dans les meilleurs délais, compte tenu de la gravité d'une situation sécuritaire qui ne cesse de se dégrader dans l'espace numérique, un certain nombre de recommandations concrètes portant sur les cinq champs de progrès suivants que notre commission a identifié :

- Le renforcement de la lutte contre la cybercriminalité ;
- Les points d'amélioration du plan cyber ;
- La stratégie de cyberdéfense de l'Etat français ;
- La sécurité des produits et services numériques, et le développement du *cloud* de confiance ;
- La conduite des politiques publiques en faveur de la sécurité dans l'espace numérique.

I. Sur les moyens judiciaires et policiers pour combattre la cybercriminalité

La CSNP a bien noté que la stratégie nationale pour la cybersécurité n'aborde pas le volet du traitement policier et judiciaire de la cybercriminalité. Notre commission estime que ce champ de progrès doit faire l'objet d'une priorité gouvernementale dans un contexte de croissance quasi exponentielle de cette criminalité nouvelle.

• Sur le volet judiciaire

Les membres de la CSNP observent une véritable carence de l'Etat dans les moyens dédiés à la lutte contre la cybercriminalité. Aujourd'hui, trois magistrats seulement traitent les dossiers de cybercriminalité en France alors que le nombre d'attaques augmente à un rythme exponentiel depuis deux ans. La qualité et l'engagement de ces magistrats doivent être salués mais cet effectif est clairement insuffisant. Le décalage croissant entre la réalité de la criminalité dans l'espace numérique et les moyens dont dispose l'institution judiciaire pour traiter cette cyber-délinquance mondialisée et industrialisée, est un sujet de préoccupation majeur pour les parlementaires membres de notre Commission.

Recommandation n°1 : La CSNP engage le Gouvernement à étudier la création d'un parquet national cyber, disposant des ressources et des expertises suffisantes pour instruire les dossiers liés aux affaires de cyber-délinquance les plus complexes.

Recommandation n°2 : La CSNP recommande au Gouvernement de consolider le dispositif des référents cybercriminalité, auprès de chaque Cour d'appel, en renforçant notamment leur formation à ces enjeux.

Recommandation n°3 : La CSNP recommande une formation spécifique des magistrats sur les enjeux du numérique, la sécurité dans l'espace numérique, et le traitement judiciaire de la cybercriminalité, dès leur formation initiale et au cœur des dispositifs de leur formation continue.

Recommandation n°4 : La CSNP recommande de renforcer la coopération judiciaire européenne et internationale et encourage une initiative française en vue de la création d'un véritable parquet européen spécialisé dans la cybercriminalité, dans la perspective de la Présidence française de l'Union européenne.

- **Sur le volet organisationnel de la police et de la gendarmerie nationale**

L'arrêté du 25 février 2021 portant création du commandement de la gendarmerie dans le cyberspace est une disposition nécessaire pour structurer l'action des forces de gendarmerie dans la lutte contre la cybercriminalité. Cependant, les membres de la CSNP estiment que le Ministère de l'Intérieur ne dispose pas des moyens suffisants, en nombre et en qualité, pour assurer le maintien de l'ordre public dans l'espace numérique, et pour lutter contre et enquêter sur la grande délinquance numérique. L'Etat doit pouvoir assurer la sécurité des citoyens et le maintien de l'ordre public dans l'espace numérique, y compris dans ses dimensions les moins régulés comme le *darkweb*.

Recommandation n°5 : La CSNP recommande un renforcement significatif des moyens des services d'enquête pour lutter contre la grande cyberdélinquance, dans le cadre d'un plan ambitieux d'adaptation des ressources relevant du Ministère de l'Intérieur à ces nouvelles formes de délinquance.

- **Sur l'adaptation du corpus législatif**

La CSNP n'appelle pas à l'adoption d'une nouvelle loi sur la cybersécurité mais propose des aménagements aux textes actuels en étendant les pouvoirs de l'ANSSI dans le cadre de la loi n°2018-607 relative à la programmation militaire pour les années 2019 - 2025 du 13 juillet 2018.

La cybercriminalité est devenue une nouvelle forme d'atteinte aux intérêts vitaux de la nation, au même titre que le terrorisme. Il convient de s'interroger sur l'adaptation des mesures permettant de lever le secret des enquêtes judiciaires pour renforcer le champ d'action de l'ANSSI à l'instar des mesures qui ont été prises pour renforcer l'action de nos services de renseignement en matière de lutte contre le terrorisme.

Recommandation n°6 : La CSNP suggère :

- De modifier l'article 34 de la loi n°2018-607 relative à la programmation militaire pour les années 2019 - 2025 du 13 juillet 2018 afin de d'étendre les capacités d'investigation technique de l'ANSSI aux contenus des équipements informatiques ;
- De permettre à la Justice de transmettre à l'ANSSI des informations couvertes par le secret de l'instruction mais utiles à l'accomplissement de ses missions.

- **Sur le paiement des rançons par les entreprises**

Environ 20% des entreprises subissant une attaque par rançongiciel paieraient la rançon qui leur est réclamée par les attaquants, souvent incitées à le faire par les sociétés d'assurance auprès desquelles elles ont souscrit une police d'assurance contre les cyber-risques. Cette situation n'est pas acceptable car elle entretient et renforce l'activité des cybercriminels, dont il est absolument indispensable de tarir les ressources.

Recommandation n°7 : La CSNP recommande au Gouvernement de développer un dispositif de régulation du paiement des rançons par les entreprises françaises, soit pour l'interdire, soit pour rendre obligatoire, sous le couvert d'une protection du type « secret des affaires », la déclaration aux autorités françaises, d'une demande de rançon et de son traitement.

II. Recommandations visant à renforcer et compléter les mesures annoncées dans le cadre de la stratégie nationale pour la cybersécurité

La CSNP reconnaît l'ambition et la pertinence des mesures annoncées dans le cadre du plan d'accélération de la cybersécurité aux besoins identifiés de l'écosystème français (renforcer la filière française de la cybersécurité, en doublant les emplois passant de 37 000 à 75 000), destiné prioritairement à stimuler la recherche française en cybersécurité et l'innovation industrielle.

• **Sur le dispositif national de cybersécurité**

Un effort particulier a été porté sur les moyens budgétaires de l'ANSSI qui va bénéficier d'un budget de 136 millions d'euros sur 2021/2022 pour financer des projets structurants. De l'avis unanime des parties prenantes, l'ANSSI effectue un travail remarquable et remplit sa mission avec efficacité. L'Etat a su dégager des moyens pour permettre le recrutement de 600 experts en cybersécurité (contre 200 experts à sa création en 2009). L'Agence connaît cependant un turn-over relativement élevé, et ses experts sont très recherchés sur un marché des compétences en cybersécurité particulièrement en tension.

Recommandation n°8 : La CSNP recommande au Gouvernement de mobiliser les moyens qui permettront à l'ANSSI de fidéliser ses agents en leur offrant des conditions plus attractives.

Initié par le Président de la République en 2019, le Campus Cyber a vocation à être, dès cette année, un lieu emblématique qui rassemblera les principaux acteurs du domaine de la cybersécurité afin de développer des synergies entre grands groupes, PME, startups, services de l'État, organismes de formation, acteurs de la recherche et associations. Le Campus Cyber a également pour mission de développer des partenariats avec des pôles de cybersécurité en région.

Par ailleurs, le plan d'accélération cyber prévoit le déploiement dans chaque région d'un CSIRT (*Computer Security Incident Response Team* - équipe de réponse aux incidents informatiques) incubé avec le soutien de l'ANSSI. Ces CSIRT doivent permettre de réagir plus rapidement et efficacement aux incidents cybers qui peuvent frapper les collectivités territoriales, les structures du tissu sanitaire (hôpitaux, cliniques) et les structures du tissu économique local.

Recommandation n°9 : La CSNP recommande que la création des CSIRT en région se fasse en étroite concertation avec les collectivités territoriales à l'échelle régionale. Elle recommande notamment la création dans chaque région d'un campus régional de la sécurité numérique capable de fédérer localement les acteurs de la sécurité numérique, de les faire travailler en réseau, et de sensibiliser l'écosystème public et privé à ces problématiques. Ce campus hébergerait le CSIRT incubé par l'ANSSI et serait notamment un véritable relais de gouvernance régionale pour l'ANSSI, au service de tous les départements d'une même région pour un maillage territorial efficace. La création de ces campus régionaux pourrait s'appuyer sur l'article L4251-13 du Code général des collectivités territoriales portant nouvelle organisation territoriale de la République, et être inscrite dans les schémas régionaux de développement économique, d'innovation et d'internationalisation.

- **Sur la sensibilisation et la formation à la sécurité numérique**

Recommandation n°10 : La CSNP recommande aux pouvoirs publics de développer une politique massive d'information et de sensibilisation de la population sur les risques encourus dans l'espace numérique, tant à titre privé que professionnel, et sur les mesures et dispositions permettant de s'en prémunir.

La formation est la condition sine qua non de la mise en œuvre opérationnelle du plan d'accélération cyber en raison de la pénurie de compétences : 500 000 emplois déficitaires en Europe dans le numérique en général, notamment la cybersécurité, la science des données et l'intelligence artificielle, sont annoncés d'ici 2025 par la Commission européenne.

Le plan d'accélération cyber propose de renforcer la formation initiale et continue aux métiers de la cybersécurité, afin de résorber les déficits de compétences dans ce domaine en établissant un diagnostic des formations et des métiers existants pour répondre à la demande et aux enjeux de la cybersécurité de manière transversale. La sécurité numérique doit être plus systématiquement intégrée dans l'ensemble des formations pour changer le paradigme de la sécurité dans l'espace numérique. La sensibilisation à ces sujets doit s'effectuer dès le collège, grâce aux stages de troisième.

Recommandation n°11 : La CSNP recommande que des enseignements portant sur la sécurité numérique et la cybersécurité soient intégrés systématiquement et rapidement dans tous les cursus de formation aux métiers du numérique. Les principes de « sécurité par conception », « d'architecture sécurisée » et de « sécurité d'exploitation » doivent s'imposer dans les formations de tous niveaux aux métiers du numérique. Cette recommandation est formulée tant pour la formation initiale que pour la formation continue.

Recommandation n°12 : La CSNP recommande qu'un effort tout particulier soit engagé en faveur de la sensibilisation et la formation aux enjeux de la sécurité numérique et de la cybersécurité au profit des agents publics, notamment ceux qui sont employés dans les plus petites structures, particulièrement vulnérables.

Nous faisons le constat de la faible féminisation de ces métiers (à peine 15%) et particulièrement des métiers de la cybersécurité, dans lesquels les femmes représentent à peine 11% des effectifs, selon la plupart des études.

Recommandation n°13 : La CSNP suggère de renforcer de manière très substantielle les actions en faveur de la féminisation des métiers du secteur numérique. Dans un contexte de déficit de compétences, nous demandons que soit mis un terme à ce phénomène d'éviction croissante des femmes de ces métiers. A ce titre, nous appelons les pouvoirs publics à renforcer leurs soutiens à la fondation Femmes@Numérique présidée par notre collègue Christine Hennion, députée des Hauts de Seine, et membre de la CSNP, fondation qui œuvre en faveur de la féminisation des métiers du numérique.

- **Sur la consolidation de la filière cybersécurité**

Aujourd'hui la filière française de l'industrie de la cybersécurité est morcelée entre de nombreuses PME et quelques grands industriels très spécialisés. Elle ne propose pas dans son offre, contrairement à ses concurrents américains, de dispositifs de sécurité intégrés (firewall, antivirus, EDR etc.). Un des axes de renforcement de la filière pourrait passer par des objectifs de consolidation de ces dispositifs afin que l'offre française en matière de cybersécurité puisse proposer des offres intégrées plus facilement commercialisables auprès des acteurs de taille modeste ou intermédiaire. Le plan propose de structurer la filière et de repositionner la France par rapport à la concurrence internationale en nombre d'entreprises.

Recommandation n°14 : La CSNP recommande au Gouvernement de développer une politique industrielle active de consolidation de la filière industrielle française des produits et services de cybersécurité afin de favoriser la création d'entreprises *leaders* de la cybersécurité, disposant d'une taille critique de classe mondiale et capables de développer des gammes de produits de sécurité répondant aux attentes du marché mondial. Le contrat de la filière des industries de sécurité 2020 /2022 peut permettre à l'écosystème numérique français d'être moins compartimenté grâce à ses projets structurants sur la cybersécurité et le numérique de confiance, tout en s'ouvrant à la dimension européenne.

Recommandation n°15 : La CSNP recommande que l'Etat prenne une part plus active à la consolidation de la filière cybersécurité en mobilisant d'avantage le levier de la commande publique au niveau national et européen. Il convient par ailleurs d'étudier si la directive 2014/25/UE du 26 février 2014 relative à la commande publique des opérateurs de réseaux doit être modifiée, notamment pour permettre aux opérateurs de réseaux, dont les achats de produits et services de cybersécurité sont généralement soumis à cette directive, d'orienter leurs achats en la matière auprès de fournisseurs nationaux et européens. A minima, il conviendrait de définir que la cybersécurité entre dans le champ d'exclusion de l'application de la directive au profit des OIV (Opérateurs d'Importance Vitale) et OSE (Opérateurs de Services Essentiels) afin de leur permettre d'accéder à des solutions de confiance.

- **Sur les mesures incitatives pour renforcer les budgets sécurité numérique du secteur privé**

Le plan d'accélération cyber incite les entreprises à porter leurs investissements dans les produits et services de sécurité numérique à hauteur de 5 à 10% du montant de leur budget informatique.

Recommandation n°16 : La CSNP suggère d'accompagner le plan d'accélération cyber par des mesures d'incitation fiscale afin que les entreprises puissent dédier plus facilement et rapidement des moyens supplémentaires à leur budget cybersécurité. Cela peut prendre la forme de suramortissement des investissements en sécurité numérique ou d'un crédit d'impôt sur les dépenses et investissements engagés dans ce secteur auprès de fournisseurs nationaux et européens.

- **Sur le pilotage de la mise en œuvre du plan d'accélération cyber**

Le plan d'accélération cyber est inédit par son ambition et l'ampleur des ressources financières qui lui sont consacrées. Ce sont désormais la qualité de sa mise en œuvre et la rapidité de son exécution qui seront déterminantes, notamment parce que la dégradation de la situation actuelle appelle des mesures urgentes.

Recommandation n°17 : La CSNP attire l'attention du Gouvernement sur la nécessité de garantir la disponibilité des moyens humains et financiers dédiés à la mise en œuvre du plan d'accélération cyber, sous la direction de son coordinateur. L'exécution de ce plan d'accélération cyber nécessite un effort de gouvernance très substantiel, inscrit dans la durée.

Recommandation n°18 : La CSNP demande au Gouvernement de déterminer les indicateurs pertinents de pilotage de ce plan et d'établir un tableau de bord qui sera présenté semestriellement à notre Commission.

- **Sur l'identité numérique régalienn**

Dans un contexte de dématérialisation croissante de tous types de démarches, tant administratives que privées, l'accès aux ressources numériques devient un enjeu de sécurité pour l'ensemble de nos concitoyens. Plus de 200 000 Français par an sont victimes d'usurpation de leur identité dans l'espace numérique. L'identité numérique est la capacité à utiliser de façon sécurisée les attributs de son identité pour accéder à un ensemble de ressources numériques. Le projet d'identité numérique porté par le programme France Identité Numérique vise à répondre à ce besoin. Après la mise en place de FranceConnect, en 2016, fédérateur d'identité, et l'expérimentation d'Alicem en 2019, le déploiement de la carte nationale d'identité électronique (CNIe), prévu à partir de 2021, devrait permettre de proposer une solution d'identité numérique régalienn à l'ensemble des français.

Recommandation n°19 : La CSNP demande au Gouvernement d'accélérer le déploiement de l'identité numérique régalienn afin que nos concitoyens disposent dans les meilleurs délais de cet instrument essentiel pour la sécurité des accès aux ressources numériques. Cette accélération est également nécessaire pour que la France ne prenne pas de retard supplémentaire par rapport à ses voisins européens.

III. Sur la dimension géopolitique de la lutte contre les cybermenaces

- **Sur une mise en œuvre plus rapide de l'Appel de Paris pour la confiance et la sécurité dans le cyberspace**

Le 12 novembre 2018, à l'occasion de la réunion à l'UNESCO du Forum sur la gouvernance de l'internet (FGI) et du premier Forum de Paris sur la paix, le Président de la République, Emmanuel Macron, a lancé l'Appel de Paris pour la confiance et la sécurité dans le cyberspace, une déclaration de haut niveau articulée autour de neuf principes et de valeurs communes pour faire du cyberspace un espace libre, sûr et ouvert.

Aujourd'hui soutenu par 79 Etats, 35 organismes publics, 387 organisations et membres de la société civile ainsi que par 702 entreprises, l'Appel de Paris permet à l'ensemble de ces acteurs d'agir de

concert afin de faire respecter dans le cyberspace les mêmes droits fondamentaux et principes qui s'appliquent dans le monde physique. En novembre 2020, le ministre de l'Europe et des Affaires étrangères a annoncé la création de six groupes de travail issus de secteurs et pays différents qui rendront des travaux et résultats préliminaires en novembre 2021.

Pour les membres de la CSNP, la France doit se saisir de cet Appel pour amorcer un véritable changement de paradigme dans la gestion de la sécurité dans l'espace numérique. Il s'agit d'une opportunité à développer au profit du caractère opératoire et législatif de cet Appel afin qu'il soit en mesure de fournir des cadres concrets de lutte contre les nouvelles menaces : cybercriminalité, espionnage, vols de données personnelles ou d'informations confidentielles, attaques contre des individus ou des infrastructures...

Recommandation n°20 : La CSNP recommande que les ambitions de l'Appel de Paris, et leur traduction en mesures opératoires par les groupes de travail, soient portées par le gouvernement auprès de l'Union européenne dans le cadre de la Présidence française de l'UE de 2022.

Dans une perspective d'amélioration de la coopération européenne et internationale en matière de lutte contre la cybercriminalité, il apparaît essentiel de réguler les activités de dévoilement des failles de sécurité et de vulnérabilité. Certains chercheurs agissent de manière irresponsable en documentant publiquement des vulnérabilités, laissant ainsi le champ libre aux cybercriminels pour les exploiter avant qu'elles aient fait l'objet de la publication de correctifs.

Recommandation n° 21 : La CSNP recommande le développement d'une politique publique de régulation des démarches de divulgation des vulnérabilités afin que les propriétaires de vulnérabilités et les chercheurs coopèrent pour réduire les risques associés à une divulgation inappropriée dans l'espace public. La CSNP appelle le Gouvernement à se saisir des recommandations du rapport de l'OCDE "*Encouraging vulnerability treatment*" publié le 11 février 2021, et à les porter au niveau européen dans le cadre de la PFUE 2022, et à l'international à l'ONU, dans le cadre de l'Appel de Paris, du G7 et du G20.

- **Sur la stratégie de cyberdéfense française**

La cyberdéfense est un pilier essentiel de la stratégie de défense et de sécurité nationale. L'ANSSI déploie des compétences remarquables au profit de la cyberprotection des services de l'État, des opérateurs d'importance vitale et de services essentiels, ainsi que de l'ensemble des organismes publics et privés. Cependant, à la lumière des dernières attaques, l'on constate que ces capacités nationales interviennent essentiellement en "pompiers" pour accompagner les victimes des cyber-agressions. Confrontée à ce qui s'apparente à une guerre permanente, menée par des cybercriminels qui agissent bien souvent en proximité avec des agences étatiques ou des officines paraétatiques, la défense dans la profondeur de la collectivité nationale est désormais une priorité au service de la résilience de la société et de son économie. La capacité des services de l'Etat concernés (ANSSI, Ministère de l'Intérieur, Ministère des Armées) doit être développée de manière très substantielle afin qu'ils soient en mesure de détecter et d'identifier les attaquants partout sur la planète, et engager les instruments de la force légitimes pour neutraliser les cybercriminels, avant qu'ils ne commettent leurs méfaits.

Recommandation n°22 : La CSNP invite les commissions compétentes du Parlement à s’informer auprès du Gouvernement et des services chargés, à divers titres, des missions de cyberdéfense dans le détail, et à vérifier l’adéquation du dispositif national à la réalité évolutive et croissante de la cybermenace. La CSNP se tient à leur disposition pour compléter leur information sur le diagnostic porté par ses membres.

- **Sur les priorités de la présidence française de l’Union Européenne en 2022**

La France présidera le Conseil de l’Union européenne au cours du premier semestre 2022. Il paraît hautement souhaitable aux membres de la CSNP que les autorités françaises inscrivent à l’agenda de ses travaux, le sujet de la coopération européenne en matière de politique numérique et de sécurité dans l’espace numérique.

Il apparaît à notre Commission qu’un véritable changement de paradigme doit s’opérer en Europe pour envisager un niveau acceptable de cyber-risque dans l’espace numérique. Dans un secteur largement dominé par les Etats-Unis, et demain par la Chine, l’Europe doit trouver les voies et moyens de son autonomie afin de maîtriser ses dépendances à des technologies et des opérateurs extra-européens. La présidence française de l’Union Européenne en 2022 constitue une opportunité que la France doit saisir pour initier ce changement de paradigme et mobiliser dans cette démarche ses partenaires européens, ainsi que les acteurs clés du secteur du numérique.

Recommandation n°23 : La CSNP recommande que la PFUE 2022 soit mise à profit pour porter différents sujets auprès des Etats membres et des institutions, afin de renforcer la sécurité et la protection de l’espace numérique européen :

- Le parquet européen doit acquérir des compétences dans le traitement et l’application de peines en matière de cybersécurité sans toutefois empiéter sur les compétences qui relèvent du droit national. (Cf. recommandation n°4)
- Les recommandations des groupes de travail de l’Appel de Paris devront être endossées par les institutions européennes afin d’orienter les futures politiques publiques sur l’espace numérique et sa protection. (Cf. recommandation n°20)
- La France doit engager les institutions européennes dans la promotion d’une régulation internationale du dévoilement des vulnérabilités des produits et services numériques. (Cf. recommandation n°21)
- La France doit promouvoir l’échelle européenne pour imposer des normes minimales de sécurité par conception sur l’ensemble des produits et services numériques mis en service sur le marché européen. (Cf. recommandation n°24)

IV. Sur les enjeux liés à la sécurité des produits numériques et connectés et un cloud de confiance

- **Sur la sécurité des produits et des services numériques**

L’espace numérique recouvre un ensemble d’acteurs, de technologies et de chaînes de valeurs complexes et souvent mondialisés (hardware, middlewares, softwares, datas...). Bien souvent les produits et services numériques sont considérés à tort comme « suffisamment sûrs » or, ils reposent

sur un code informatique par nature vulnérable aux cyberattaques. Ces failles de sécurité n'apparaissent pas seulement lors de la phase d'exploitation d'un produit ou d'un service numérique mais bien tout au long de son cycle de vie, et notamment lors de sa conception.

En s'appuyant sur deux études comparatives sur le cycle de vie et la chaîne de valeur des produits et services numérique, l'OCDE a mis en évidence le rôle des facteurs économiques, des pouvoirs publics et des acteurs finaux dans les dynamiques de création et d'établissement des normes de sécurité de ces produits et services. L'Organisation met en évidence les nombreuses défaillances de marchés qui ne permettent pas aux acteurs industriels de fournir des normes de sécurité optimales sur le marché du numérique. Contrairement à la plupart des autres secteurs industriels, l'industrie du numérique n'est pas encore soumise à des normes minimales de sécurité. La sécurité numérique étant un domaine dynamique en constante évolution, les acteurs industriels doivent être encouragés à traiter ces vulnérabilités de façon plus efficace sur le temps long.

Recommandation n° 24 : Les membres de la CSNP appellent à l'adoption de normes minimales de sécurité sur tous les produits et services numériques avant leur mise sur le marché, en cohérence avec les préconisations formulées par l'OCDE dans son rapport « *Enhancing the digital security of products* » publié le 9 février 2021. Afin de favoriser l'adoption de principes de haut niveau de sécurité numérique par conception, les pouvoirs publics nationaux et européens pourraient décliner des mécanismes d'incitations pour le développement de normes communes et des instruments règlementaires contraignants. A cet égard, la France et l'Europe doivent renforcer leur présence dans les instances de normalisation internationales.

- **Sur le *cloud* de confiance**

Le *cloud* n'est plus un simple sous-domaine du secteur numérique. Il est désormais celui qui commande tous les autres. Comme la crise sanitaire l'a amplement montré, de façon extrêmement concrète, les données sont au cœur de la transformation numérique, et le *cloud* est à présent le socle incontournable du système d'information des entreprises et administrations publiques. De plus, quasiment tous les champs de l'innovation numérique (intelligence artificielle, objets connectés, *edge computing*, industrie 4.0, 5G et 6G, calcul intensif, *quantum computing*, pour ne citer que ces quelques exemples) se cultivent aujourd'hui dans les environnements mis à disposition par le *cloud*.

Le concept de cloud de confiance repose sur trois piliers : la garantie de sécurité, à laquelle le label SecNumCloud serait susceptible de répondre, l'immunité aux législations extra-européennes, la maîtrise de leurs dépendances par les utilisateurs, notamment en termes de portabilité des données et des traitements associés, de réversibilité des offres, d'interopérabilité des solutions, de transparence des contrats. Le cloud de confiance va progressivement devenir une condition indispensable de la sécurité dans l'espace numérique des entreprises et administrations publiques de toutes tailles et de toutes natures.

Recommandation n°25 : La CSNP incite le Gouvernement à développer et renforcer les liens entre les acteurs politiques et industriels du numérique afin de faire émerger des solutions de cloud de confiance, notamment au profit des applications les plus sensibles pour nos concitoyens comme celles traitant des données de santé. La CSNP appuie par ailleurs la mise en cohérence du projet GAIA-X avec les enjeux nationaux du cloud de confiance. Enfin, la CSNP demande au Gouvernement de l'informer régulièrement de la mise en œuvre de sa feuille de route d'accélération du cloud de confiance.

V. L'élaboration et la conduite des politiques publiques en faveur de la sécurité dans l'espace numérique.

Depuis plusieurs années, les sujets numériques sont désormais présents à tous les niveaux, et dans tous les départements ministériels. Ils nécessitent un pilotage à la fois transversal et centralisé permettant de renforcer la cohérence des actions engagées. La plupart des recommandations émises plus haut dans cet avis relèvent du champ de compétence des Ministères de l'Economie, des Finances et de la Relance, des Armées, de la Justice, de l'Intérieur, de l'Europe et des Affaires étrangères, de l'Enseignement supérieur de la Recherche et de l'Innovation, de la Cohésion des territoires et des Relations avec les collectivités territoriales, voire directement de l'action du Premier ministre.

Recommandation n°26 : Suivant en cela une appréciation constante de notre commission, la CSNP recommande au Gouvernement d'incarner au meilleur niveau, auprès du Premier ministre, une autorité politique interministérielle chargée d'élaborer, de fédérer et de conduire les politiques publiques en matière de numérique, et dont la sécurité serait une priorité.

La France, son économie, et l'ensemble de nos concitoyens doivent pouvoir compter, pour adapter le pays aux enjeux du vingt-et-unième siècle, dans la durée et le temps long, sur une puissante organisation en mesure d'éclairer l'avenir numérique par la recherche, et de le préparer par l'investissement. C'est à cette condition que la France, et avec elle le continent européen, retrouveront leur autonomie et leur capacité à développer un numérique sûr, éthique, durable et de confiance.

L'histoire du Commissariat à l'énergie atomique et aux énergies alternatives peut nous inspirer en la matière. Il a été l'instrument de l'autonomie de la France dans le domaine de l'énergie atomique civile et militaire, laquelle permet à notre pays de disposer d'un siège permanent au Conseil de sécurité de l'ONU et d'être un Etat parmi les plus vertueux en matière de rejet de CO2 pour sa production électrique.

Recommandation n°27 : La CSNP suggère au Gouvernement d'étudier une articulation plus efficiente des capacités nationales de recherche et technologie dans le domaine du numérique, fédérant notamment les ressources de l'INRIA, du CEA et du CNRS, dans une gouvernance commune. Cette gouvernance pourrait reposer sur une direction des applications civiles et une direction des applications de sécurité nationale. Son objectif, assorti des moyens nécessaires, consisterait à éclairer l'avenir par la recherche et à le préparer par l'investissement.

Auditions de la Commission supérieure du numérique et des postes

MM. Laurent BERNAT et **Ghislain de SALINS**, auteurs du rapport « Des politiques intelligentes pour les produits intelligents » publié par le Département Digital Security Policy de l'OCDE

M. Gérôme BILLOIS, Partenaire cybersécurité et confiance numérique en charge de la gestion des risques numériques de Wavestone

M. Bruno CHARRAT, Directeur du département cybersécurité au Commissariat à l'Energie Atomique

M. Bernard DUVERNEUIL, Président du Cigref

Mathieu HEURTEL, conseiller en charge des Entreprises et des Technologies auprès du cabinet du Secrétaire d'État chargé de la Transition numérique et des Communications électroniques

M. Guillaume POUPARD, Directeur général de l'ANSSI

Mme Myriam QUEMENER, Avocat général près la Cour d'appel de Paris, Docteur en droit

Bibliographie

"Enhancing the digital security of products: A policy discussion", OECD Digital Economy Papers, No. 306, OECD Publishing, Paris,

« Des politiques intelligentes pour les produits intelligents », Note sur les politiques de la Direction de la science, de la technologie et de l'innovation, OCDE, Paris.

"Encouraging vulnerability treatment: Overview for policy makers", OECD Digital Economy Papers, No. 307, OECD Publishing, Paris

Dossier de presse du 18 février 2021, "Cybersécurité faire face à la menace : la stratégie française", Gouvernement.

Dossier de presse du 22 mars 2021, « Cybersécurité : protéger les services publics et les collectivités territoriales avec France Relance », Gouvernement.

Sitographie

[Cybersécurité : Appel de Paris du 12 novembre 2018 pour la confiance et la sécurité dans le cyberspace](#)



COMMISSION SUPERIEURE DU NUMERIQUE ET DES POSTES

AVIS N°2021-04 DU 10 JUIN 2021 PORTANT CONTRIBUTION

A LA MISSION RELATIVE AUX NOUVELLES TECHNOLOGIES DANS LE DOMAINE DE LA SECURITE

La mission confiée par le Premier Ministre à notre collègue Jean-Michel Mis, Député de la Loire, porte sur la sécurité des Jeux olympiques et paralympiques de Paris en 2024, notamment en matière de choix technologiques et de mise en place des cadres d'expérimentation nécessaires pour favoriser les innovations proposées par la filière industrielle.

Alors que des choix stratégiques doivent être pris par le gouvernement, les membres de la CSNP souhaitent apporter une contribution dans le périmètre de leurs compétences : sans exclure *à priori* aucune technologie permettant de renforcer la sécurité de ces grands événements, les membres de la CSNP se prononcent pour un continuum entre sécurité physique et sécurité numérique (I).

Les membres de la CSNP considèrent que si la sécurité de ces grands événements constitue une obligation de résultats pour les autorités publiques, elle doit se faire en développant un cadre juridique respectueux des libertés publiques et individuelles (II). Pour répondre à cet objectif, des expérimentations sur des grands événements pourraient être mis en œuvre en associant autorités indépendantes et société civile (III).

I. Les solutions offrant un continuum entre sécurité physique et sécurité numérique doivent pouvoir être mises en œuvre

Le champ d'application du programme de sécurité des Jeux olympiques et paralympiques de Paris en 2024 vise à réduire les menaces de nature terroriste ou criminelle et, d'une manière plus générale, le niveau de sûreté pendant la phase de construction des sites, pendant les épreuves tests et pendant la période opérationnelle des Jeux. Ce programme concerne les sites de compétition et d'hébergement, les réseaux de transport, ainsi que toute autre infrastructure stratégique pour l'organisation des Jeux.

Cette responsabilité de la sécurité publique incombe à l'État français et intègre la lutte contre le terrorisme, les problématiques de délinquance liés aux phénomènes de bandes ou de constitution de black blocs ainsi que la gestion des crises sanitaires.

1. A ce stade, les membres de la CSNP considèrent que les autorités doivent pouvoir recourir à l'ensemble des technologies permettant de renforcer la sécurité des jeux contre les formes de délinquance classique ou contre le terrorisme, au nombre desquelles figurent:

- a. Le traitement des données biométriques. Les données biométriques comprennent les données relatives à notre corps ou à notre comportement : empreinte digitale, reconnaissance du visage, ADN, géométrie de la main, empreinte palmaire, reconnaissance de l'iris et de la

ré tine, rythme de frappe, démarche et posture physique ... Partout en Europe et dans le monde, des entreprises mettent au point des solutions innovantes pour mieux définir, analyser et prédire nos comportements individuels ou de masse.

Le traitement des données biométriques pourrait être utilisé à tous les stades du continuum sécuritaire : en amont (reconnaissance faciale a priori, pour prévenir l'intrusion d'individus dans des manifestations par exemple) ; en situation (pour accélérer l'enquête, du fait de la rapidité et de la précision de l'outil) et a posteriori (le traitement des bases existantes et le croisement des données permet des recoupements dynamiques).

La biométrie offre des solutions permettant la mise en œuvre de dispositifs d'authentification efficaces (déploiement de mots de passe biologiques non-falsifiables pour accès aux sites physiques ou numériques les plus sensibles).

La biométrie « *aux fins d'identifier une personne physique de manière unique* » entre dans une catégorie particulière définie par deux textes adoptés par les 27 États membres de l'Union européenne en avril 2016, le règlement général sur la protection des données (RGPD) et la directive police-justice. Il s'agit d'une catégorie de données considérées comme particulièrement sensibles. Le RGPD s'applique à l'ensemble des traitements de données personnelles effectués à la fois dans le secteur public et le secteur privé. La directive police-justice concerne, pour sa part, les traitements effectués à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales par les autorités compétentes (autorités judiciaires, police, autres autorités répressives ...). Elle précise que les données biométriques ne doivent être utilisées qu'en cas de nécessité absolue et sous réserve de garanties appropriées pour les droits et libertés de la personne concernée. Un tel traitement peut être effectué dans trois cas uniquement : lorsqu'il est autorisé par le droit de l'Union ou le droit d'un État membre, lorsqu'il porte sur des données manifestement rendues publiques par la personne ou pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne.

- b. Le traitement algorithmique des connexions et des données permet la détection de signaux faibles. Les prochains débats relatifs au projet de loi antiterroriste – que le Sénat examinera en séance publique à compter du 29 juin - poseront néanmoins la question de la portée de ce traitement, aujourd'hui limité aux noms de domaine et potentiellement étendue aux adresses URL.
- c. Les technologies sécuritaires de mobilité, notamment les caméras aéroportées, permettent de sécuriser les sites officiels et les cibles potentielles. Elles nécessitent un encadrement juridique plus spécifique en tant que la portée et les finalités de leur utilisation sont fonctions d'une doctrine sécuritaire définie en amont de leur déploiement.
- d. Les technologies d'inclusion de l'ensemble des objets connectés dans le continuum de sécurité (smartphones, capteurs des bâtiments, ...). Notamment, les smartphones peuvent être un outil efficace de communication. Ils peuvent permettre d'une part, d'alerter localement les participants par notifications, et d'autre part faciliter une remontée d'information plus rapide et précise aux services publics de sécurité.

Du point de vue des membres de la CSNP, aucune technologie ne peut être exclue *per se* : l'usage de l'Intelligence artificielle peut permettre la gestion des mouvements de foules et la détection des mouvements et des comportements suspects. La reconnaissance faciale, la biométrie les solutions de traçage et la *blockchain* permettent de sécuriser l'accès au site les plus sensibles en contrôlant les identités.

2. Dans le prolongement des recommandations publiées dans son avis n°2021-03 sur la sécurité numérique, les membres de la CSNP attirent l'attention des autorités françaises sur les risques que font peser les actes de cybercriminalité et de cyberattaques sur les Jeux olympiques et paralympiques de Paris en 2024. En deux ans, les cyber-attaques ont été multipliées par quatre et une projection à trois ans de ces cyber-menaces suppose l'adoption dès à présent des meilleurs systèmes de cyberdéfense.

En tout état de cause, la CSNP appelle les autorités françaises et notamment le Ministère de l'intérieur à apporter une attention toute particulière au continuum entre sécurité physique et sécurité numérique.

En effet, d'une part, toutes les technologies mises en œuvre dans les systèmes de sécurité embarquent désormais de manière native les vulnérabilités génériques du numérique (cyber-attaques, accès et vol de données, biais cognitifs). D'autres part, les activités criminelles, notamment de nature terroriste ou de déstabilisation, sont de plus en plus fréquemment précédés et accompagnés par des opérations dans l'espace numérique, comme la diffusion de fausses informations, la recherche d'information et l'espionnage, la neutralisation de systèmes de surveillance, la mise en cause de l'intégrité, de la confidentialité et de la disponibilité de données sensibles de sécurité et des traitements associés.

A ce titre, la CSNP suggère que ses recommandations en matière de sécurité par conception inscrites dans son avis sur la sécurité numérique du 29 avril 2021, soient adaptées et mises en œuvre dans le cadre du développement des systèmes technologiques nécessaires à la sécurisation des grands événements sportifs et des Jeux olympiques et paralympiques de Paris en 2024.

II. Développement d'un cadre juridique respectueux des libertés individuelles et collectives

La CSNP est transpartisane et à l'image de la société française : le curseur entre sécurité et libertés publiques et individuelles peut évoluer selon la sensibilité de ses membres.

Pour autant, les membres de la CSNP sont favorables à :

- un usage proportionné des technologies à des fins sécuritaires avec le respect des libertés publiques et individuelles,
- un encadrement et un contrôle par une autorité indépendante, en l'occurrence la CNIL, de la bonne application du cadre réglementaire en matière d'enregistrement des données, de leur traitement, de leur sécurité de conservation, de leur accès par des personnes autorisées, de leur usage circonscrits à certains motifs, et de leur effacement systématique après une durée de stockage déterminée.

Les membres de la CSNP ont pleinement conscience que le cadre législatif, réglementaire et jurisprudentiel portant sur les usages de l'intelligence artificielle, de la reconnaissance faciale et de l'utilisation des données est actuellement mouvant : les négociations sur le projet de règlement sur l'intelligence artificielle (IA) proposé par la Commission européenne le 21 avril dernier, et notamment les dispositions relatives à la reconnaissance faciale, sont en cours alors que les autorités françaises ont d'ores et déjà à opter pour des solutions en vue d'être prêtes pour les Jeux olympiques et paralympiques de Paris en 2024.

Nos concitoyens ont toujours porté une extrême vigilance sur les questions de libertés individuelles et publiques portées par le développement des technologies : le dernier exemple en date, sur la mise en

œuvre de l'application TousAntiCovid a conduit les autorités françaises à opter une solution souveraine alors que nos voisins européens se sont progressivement ralliés aux solutions compatibles avec les systèmes d'exploitation dominants dans le domaine de la téléphonie mobile.

Il nous paraît important de rappeler que la perception de nos concitoyens peut évoluer dès lors qu'ils mesurent les bénéfices que peuvent apporter ces technologies lorsqu'elles sont encadrées et qu'elles ont démontré leur efficacité.

L'évolution de l'opinion publique à l'égard des systèmes de vidéo-protection dans l'espace public nous paraît exemplaire : ce déploiement a donné lieu à de vives critiques avant d'être globalement accepté en vue de renforcer la sécurité dans l'espace public.

Aujourd'hui, ce sont la reconnaissance faciale et la surveillance biométrique qui font débat : une partie de la population y est farouchement opposée alors que ces technologies sont en mesure de renforcer de manière efficace la sécurité de certains sites.

Dans l'attente de l'adoption du règlement européen sur l'Intelligence artificielle¹, il nous paraît important pour l'acceptabilité de ces technologies de présenter une doctrine d'engagement qui précise de manière transparente dans quel contexte et dans quel périmètre elles seront utilisées ainsi que l'usage et l'exploitation des données ainsi recueillies dans le temps.

A cet égard, dans le cadre du rapport relatif à la proposition de loi sécurité globale² publié en mars 2021, MM. les Sénateurs Marc-Philippe Daubresse et Loïc Hervé ont souligné la nécessité d'affermir les garanties données aux citoyens sur les nécessités et finalités opérationnelles précises des captations d'images, sur la formation des personnels destinataires de ces images, sur la sécurité des enregistrements et la traçabilité des accès à ces enregistrements.

De ce point de vue, l'expérimentation qui pourrait être faite à l'occasion de prochains événements publics pour tester le déploiement de ces technologies devrait associer étroitement les autorités indépendantes telles que la CNIL et le Défenseur des droits, par exemple, mais également des associations et des représentants de la société civile pour garantir un usage raisonnable et proportionné de ces technologies. Il sera sans doute difficile d'aboutir à un consensus mais cette logique de dialogue nous semble pertinente pour encadrer le déploiement de ces technologies au plus près des craintes exprimées par nos concitoyens.

III. Un cadre permettant des expérimentations est attendu et souhaitable

Depuis le rapport publié en septembre 2018³ par Mme Alice Thourot, députée de la Drôme, et M. Jean-Michel Fauvergue, député de Seine-et-Marne, sur la sécurité globale, plusieurs autres travaux ont tenté de faire émerger une dynamique d'innovation en matière de technologies de sécurité. Ces initiatives, essentiellement portées par la filière industrielle de la sécurité, se sont fédérées dans le cadre de la création d'un Comité stratégique de la filière des industries de sécurité, et a abouti à la signature d'un contrat de filière en janvier 2020. L'un des cinq projets structurants prévu par ce contrat concerne directement la sécurité des grands événements et des Jeux olympiques et paralympiques de Paris en 2024.

Ce projet structurant vise à assurer la sécurité Jeux olympiques et paralympiques de Paris en 2024 en s'appuyant sur l'offre technologique et industrielle française, en la valorisant et en mettant l'innovation au cœur de la réponse.

¹ <https://ai-regulation.com/facial-recognition-in-the-draft-european-ai-regulation-final-report-on-the-high-level-workshop-held-on-april-26-2021/> La CNIL a publié une note en 2019 sur la reconnaissance faciale https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf

² <https://www.senat.fr/rap/120-409/120-4091.pdf>

³ https://www.gouvernement.fr/sites/default/files/document/document/2018/09/rapport_de_mme_alice_thourot_et_m.jean-michel_fauvergue_deputes_-_dun_continuum_de_securite_vers_une_securite_globale_-_11.09.2018.pdf

Les industriels de la filière expriment donc l'urgence absolue d'un cadre conventionnel exceptionnel, et éventuellement dérogatoire, permettant de mener, dès le mois de septembre 2021, les expérimentations nécessaires et de traiter les principaux points suivants :

- identification des principaux enjeux de souveraineté technologique ;
- disponibilité des données en quantité et qualité suffisante ;
- développement de l'environnement juridique et éthique adapté.

A titre d'exemple, l'industrie nationale dispose de nombreuses solutions en analyse vidéo pour l'analyse de foule, la reconnaissance faciale ou la lecture automatique des plaques d'immatriculation (LAPI), qui peuvent apporter des réponses très pertinentes sur des cas d'usages précis respectueux des libertés, mais les avancées juridiques sont extrêmement lentes.

La pandémie de COVID a *de facto* réduit considérablement le nombre de manifestations publiques et donc rendu difficiles ces types d'expérimentation mais il paraît, aux membres de la CSNP, assez urgent de les mettre en œuvre de manière pragmatique et sans délais.

Un tel cadre apparaît indispensable pour engager un plan d'accélération technologique et législatif en phase avec les échéances des Jeux olympiques et paralympiques de Paris en 2024 , en concertation avec les parties prenantes - collectivités participantes, citoyens, société civile - et avec des études d'impact (coûts/bénéfices) rigoureuses et transparentes.

Ces expérimentations doivent également permettre aux autorités de préciser les cas d'usage et la doctrine de déploiement des technologies, de retirer les bonnes pratiques et de tester la bonne coordination entre les différents services et, le cas échéant, avec nos partenaires étrangers.

Un cadre clair et adapté apparaît essentiel pour débattre de façon dépassionnée et dé-corrélée de la pression de l'actualité, notamment avec les membres du Parlement et les représentants de la société civile.

La CSNP peut offrir ce cadre.

ANNEXE : CADRE REGLEMENTAIRE ET JURISPRUDENTIEL

L'usage de l'intelligence artificielle est en cours de régulation au niveau européen :

- [stratégie européenne en matière d'intelligence artificielle](#) : création du premier [plan coordonné sur l'IA](#) en 2018,
- [lignes directrices pour une IA digne de confiance](#) publiée en 2019 par le groupe d'experts de haut niveau sur l'intelligence artificielle,
- [livre blanc](#) publié en 2020 par la Commission Européenne
- [consultation publique](#) concernant le livre blanc sur l'IA
- [rapport sur les conséquences de l'intelligence artificielle, de l'internet des objets et de la robotique sur la sécurité et la responsabilité](#)
- Avis du contrôleur européen de la protection des données sur la [régulation de l'intelligence artificielle ainsi que sur la surveillance biométrique](#).
- Annonce en 2021 du [nouveau plan coordonné](#) sur l'IA et [premier cadre juridique européen sur l'intelligence artificielle](#)

En France, l'usage de l'intelligence artificielle est peu encadré :

- La [loi pour une république numérique](#) (et la transposition du RGPD) renforce le contrôle de chacun sur l'usage de ses données privées sans pour autant définir un véritable cadre légal quant au développement et à l'utilisation de l'intelligence artificielle.
- [France IA](#), le [rapport Villani](#) ont proposé les fondations d'une stratégie nationale ambitieuse.

Reconnaissance faciale

En France, si de nombreuses jurisprudences et [délibérations](#) de la CNIL traitent de ce sujet, les tentatives d'encadrement législatif sont rares : on citera la [proposition de loi relative à la reconnaissance faciale dans les enquêtes terroristes et la prévention des attentats](#). De nombreuses expérimentations ont lieu dans des villes et lieux (aéroport de paris, lycées à Marseille et Nice...). Les parties prenantes, industriels comme associations de la société civile réclament un cadre légal clair.

Au niveau européen, la Commission propose d'encadrer la pratique au sein de la régulation de l'intelligence artificielle. Source : [Vers un encadrement de la reconnaissance faciale en Europe](#)

Détection des mouvements et des comportements

Plusieurs textes et décisions encadrent les dispositifs de détection des mouvements et des comportements :

- Déclaration de la [CNIL n° 94-056 du 21 juin 1994](#) qui protège les citoyens et encadre la vidéosurveillance
- Le texte de loi de référence est [la loi du 6 janvier 1978](#) qui encadre l'usage des données personnelles des citoyens.

- L'[ordonnance n° 2018-1125 du 12 décembre 2018](#) protège une « personne d'une décision de justice impliquant une appréciation de son comportement fondée sur le traitement automatisé de donné à caractère personnel ».
- [la loi du 21 janvier 1995 \(dite « loi Pasqua »\)](#) est centrée sur la régulation de la vidéosurveillance dans les lieux publics et les lieux privés recevant du public.
- La [loi du 6 août 2004](#) transpose les directives européennes et confère à [la CNIL](#) la responsabilité de contrôler l'usage de l'enregistrement, du traitement et de la conservation des données et des vidéosurveillances.
- La [loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure](#) vient renforcer la loi Pasqua en déployant plusieurs dispositifs supplémentaires. Cependant, face aux évolutions proposées, le texte fut contesté par la [CNIL](#) et le [Conseil Constitutionnel](#). Le texte prévoit la mise en place d'un véritable contrôle par la CNIL des systèmes de vidéoprotection dans les lieux ouverts au public, alors que jusqu'à présent, elle ne contrôlait que ceux installés dans les lieux privés.

Au niveau européen :

- Le [règlement général de protection des données](#) fait peser sur les organismes publics et privés qui traitent les données des citoyens / citoyennes une certain nombre de responsabilités. Les images de vidéosurveillance font partie de son domaine d'application : à partir du moment où les personnes filmées sont identifiables, les enregistrements sont des données privées.
- Dans son [« position paper »](#) le Conseil et le Parlement européen ont posé les bases de ce qu'il serait interdit de traiter comme données grâce à l'IA et aux productions de vidéosurveillances. A titre d'exemple, l'utilisation de l'IA pour élaborer des scores sociaux et pour évaluer la loyauté et la fiabilité des individus serait fermement interdite.

Drones

- [Drones : la CNIL sanctionne le ministère de l'Intérieur](#)
- [Suspension de l'utilisation des drones pour contrôler le déconfinement à Paris par le Conseil d'État : les contrôles de la CNIL](#)
- [Décision n° 2021-817 DC du 20 mai 2021 - Communiqué de presse 20 mai 2021](#)

Empreinte biométriques (digitale, œil)

- [Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.](#)
- [RAPPORT D'INFORMATION fait au nom de la Commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale \(1\) sur l'usage de la biométrie en France et en Europe](#)

Conservation et traitement des données personnelles

- Dans son optique de lutte contre le terrorisme et les menaces sécuritaires intérieures, la France impose aux opérateurs internet et mobile de conserver les données personnelles des utilisateurs pendant un an afin de subvenir aux besoins des renseignements en cas d'enquêtes pénales grâce à la [LOI n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale](#)

- Cependant, la CJUE a fortement limité la possibilité d'imposer aux opérateurs la conservation des données de connexion par [trois décisions rendues le 6 octobre 2020](#).
- Le Conseil d'Etat [relève que la conservation généralisée](#) aujourd'hui imposée aux opérateurs par le droit français est bien justifiée par une menace pour la sécurité nationale, comme cela est requis par la CJUE.

Blockchain

- Adaptation du [code monétaire et financier](#) grâce à l'[ordonnance n° 2017-1674 du 8 décembre 2017](#) qui facilite la transmission de certains titres financiers non cotés au moyen de la technologie « blockchain ».
- [stratégie nationale blockchain](#) de 2019 qui propose d'établir un cadre juridique permettant l'utilisation de la blockchain dans un cadre sécurisé.
- [La loi de finance 2019](#) et la [loi PACTE du 11 avril 2019](#) ont mis en place un cadre juridique pour les émissions de jetons numériques. L'Autorité des Marchés Financiers consacre ainsi en [avril 2019](#), un nouveau régime pour les cryptoactifs.
- [la mission d'information commune sur les chaînes de blocs \(blockchains\)](#) a abouti à la création de la [Fédération française des professionnels de la Blockchain](#) qui regroupe les acteurs français autour de mêmes normes de standards pour peser auprès des institutions françaises et européennes.

Au niveau européen :

- Création en 2018 de [l'observatoire Observatoire-forum des chaînes de blocs de l'UE](#)
- Proposition de [résolution du parlement européen](#),

Décision de la [Cour de Justice de l'Union Européenne](#)



COMMISSION SUPERIEURE DU NUMERIQUE ET DES POSTES

Avis n° 2021-05 du 10 novembre 2021 sur la modernisation et les apports du numérique aux processus électoraux

L'abstention aux élections régionales et départementales de juin 2021 a constitué un record en termes de désaffection démocratique : deux électeurs sur trois ne se sont pas rendus aux urnes pour exprimer leur vote alors que les élections municipales de 2020 avaient déjà été marquées par un taux d'abstention de 58,4% au second tour, en augmentation de vingt points par rapport à 2014.

Si la crise sanitaire du covid-19 n'est évidemment pas sans lien, elle ne peut expliquer seule cette progression qui n'a fait que s'amplifier depuis une dizaine d'années¹ : souvent associé à un sentiment de défiance de nos concitoyens à l'égard de la classe politique, le phénomène de l'abstention est avant tout multifactoriel et il serait illusoire de prétendre le résoudre au moyen d'une solution unique.

A partir de ce constat, la Commission supérieure du numérique et des postes a souhaité se saisir du sujet afin d'appréhender, dans son domaine de compétence, les axes d'amélioration des processus électoraux.

En effet, la CSNP considère que plusieurs obstacles pratiques ou techniques pourraient être levés et que de nouvelles initiatives pourraient être expérimentées afin de faciliter la participation de nos concitoyens aux processus électoraux.

Le numérique peut représenter à cet égard une véritable opportunité pour faciliter le parcours votant des citoyens et en adapter les modalités à une société davantage mobile et connectée.

Les membres de la CSNP notent que les résistances sont fortes pour mettre en place de véritables scénarii de rupture à court terme tant la sensibilité peut paraître parfois exacerbée lorsqu'il s'agit d'investiguer un droit fondamental et au cœur de notre état démocratique. Ces résistances sont d'autant plus établies que les solutions techniques n'offrent pas encore de garanties suffisantes et acceptables en termes de sécurité et de confidentialité. Pour autant, notre Commission estime que pour moderniser sa démocratie, la France doit s'en donner les moyens.

Elle doit aussi questionner l'objectif d'une sécurité absolue qui n'existe pas en matière électorale et aborder toute hypothèse d'évolution selon le principe du ratio bénéfice/risque, dès lors que toute initiative pouvant conduire à une fraude massive est écartée.

¹ Le taux de participation aux élections législatives permet de l'objectiver : l'abstention au second tour des élections législatives de 2017 s'élevait à 57,36 %, en augmentation de près de 13 points par rapport à 2012, de 17 points par rapport à 2007 et 2002, et de 28 points par rapport à 1997. A titre de comparaison, en 2021, les Pays Bas et l'Allemagne ont réussi à maintenir un niveau de participation élevé aux élections en dépit d'un contexte sanitaire plus défavorable alors que le Portugal a enregistré un taux d'abstention de 60,6% à l'élection présidentielle de janvier 2021.

Au terme des auditions menées, la CSNP souhaite donc émettre les recommandations suivantes.

I. Pour une véritable simplification de la procédure d'inscription sur les listes électorales :

Alors même que le code électoral pose pour principe à son article L. 9 une obligation d'inscription sur les listes électorales, la démarche relève d'une action purement volontaire des citoyens en application de son article L. 11. Il en est fait exception depuis 1998 pour les personnes venant d'atteindre la majorité et depuis 2019 pour celles venant d'acquérir la nationalité française, qui bénéficient d'une première inscription automatique.

Il est essentiel de simplifier les procédures d'inscription sur les listes électorales et de réduire de manière significative les démarches pour nos concitoyens. Aujourd'hui, les règles d'inscription sur les listes électorales sont encore trop souvent méconnues par nos concitoyens. Et lorsqu'elles sont connues, elles imposent de la part de nos concitoyens une démarche volontaire et d'entrer dans une procédure qui peut leur paraître trop lourde ou chronophage.

Les règles actuelles sont source de non-inscriptions et surtout de mal-inscriptions. Ce phénomène de mal-inscription - l'électeur n'est pas inscrit dans la commune dans laquelle il réside - correspond de fait à une réalité : de nombreux électeurs sont enregistrés sur les listes électorales à une autre adresse que celle de leur résidence principale, avec une incidence directe sur les chiffres de la participation électorale.

Il ressort des travaux menés par Céline Braconnier², auditionnée par la CSNP en qualité de chercheuse en sociologie des comportements politiques et électoraux, que la mal-inscription pourrait concerner à ce jour près de 15% des inscrits sur les listes électorales (7 millions d'électeurs mal-inscrits en 2012 et 7,6 millions d'électeurs mal-inscrits en 2017) qui ne peuvent pas voter à proximité directe de leur domicile.

Ce phénomène de mal-inscription est encore plus élevé chez les trentenaires (étudiants et cadres avec enfants) : 43% des trentenaires auraient été en situation de mal-inscription lors des élections de 2017. Or, ainsi que l'établissent ces travaux, l'abstention constante est multipliée par trois pour les personnes en situation de mal-inscription. Cette dernière touche toutes les catégories sociales mais se montre particulièrement importante chez les français les plus mobiles géographiquement.

Près d'un tiers de la population française change de domicile au cours d'un quinquennat sans que nos procédures électorales aient été adaptées à cette réalité, en particulier pour les jeunes étudiants amenés à changer de résidence au grès de leurs cursus.

Notre Commission considère que cette situation, qui empêche une part très importante de l'électorat de voter près de son lieu de résidence, n'est pas acceptable dans une grande démocratie.

Elle observe par ailleurs que la réforme adoptée dans le cadre de la loi n° 2016-1048 du 1^{er} août 2016, entrée en vigueur le 1^{er} janvier 2019 et visant à faciliter l'inscription sur les listes électorales en la rendant possible jusqu'au sixième vendredi précédent le jour du scrutin, n'a pas permis d'apporter une réponse à la hauteur des enjeux posés par les phénomènes de non-inscription et de mal-inscription en France.

Le Répertoire Electoral Unique dont la mise en place à partir de 2016 avait été confiée à l'INSEE en co-pilotage avec le Ministère de l'Intérieur avait agrégé les données des Ministères de la Justice et de la Défense ainsi que celles de la Caisse Nationale d'Assurance Vieillesse.

² Sociologie de la mal-inscription et de ses conséquences sur la participation électorale, Céline Braconnier, Jean-Yves Dormagen, Ghislain Gabalda, Xavier Niel – Revue française de sociologie 2016/1 (vol. 57), pages 17 à 44.

Les membres de la Commission considèrent que les pouvoirs publics qui ont ouvert plusieurs chantiers de simplification des procédures administratives avec notamment les initiatives portées par la DINUM et le guichet « Dites-le-nous une fois » doivent intégrer la simplification de la mise à jour du Répertoire Electoral Unique dans leurs priorités.

Cette mise à jour du Répertoire Electoral Unique à l'occasion de procédures administratives tierces a fait l'objet d'une recommandation du rapport sur « Le Bilan et les perspectives du répertoire Electoral Unique » dressé par l'Inspection générale de l'administration, l'Inspection générale des finances et l'Inspection générale des affaires étrangères en juin 2020.

Pour les membres de la Commission, il est essentiel d'aboutir rapidement à une mise-à-jour quasi systématique du Répertoire Electoral Unique.

Recommandation n° 1 - La CSNP recommande que les citoyens français soient inscrits automatiquement sur les listes électorales à l'occasion de l'accomplissement de démarches administratives (déclaration d'impôts, versement de prestations sociales par exemple).

Les citoyens qui ne souhaiteraient pas opter pour cette démarche resteraient soumis à une inscription volontaire sur les listes électorales.

La CSNP recommande qu'un groupe de travail associant la CNIL, le ministère de l'intérieur et les administrations fiscales et sociales puisse expertiser ce partage de données dans le respect du cadre juridique de la protection des données à caractère personnel.

II. Pour une meilleure information des français sur les échéances électorales

Les récents dysfonctionnements dans la distribution du matériel et de la propagande électorale lors des scrutins départementaux et régionaux des 20 et 27 juin 2021 ont mis en exergue le caractère central de l'information électorale dans la mobilisation du corps votant. Des missions dédiées à l'Assemblée nationale et au Sénat ont étudié les causes de ces dysfonctionnements.

La CSNP appelle le ministère de l'intérieur à mieux intégrer les contraintes liées à la gestion et l'organisation de la distribution de l'information électorale à l'occasion du marché public qui désignera le nouveau titulaire de l'accord cadre de distribution de la propagande électorale pour les échéances électorales de 2022, en relevant notamment la pondération des critères relatifs à la valeur technique de ces opérations.

Notre Commission tient toutefois à souligner le rôle complémentaire que peut jouer le numérique dans la mise à disposition dématérialisée d'une information électorale susceptible de favoriser la participation. La création du Répertoire Electoral Unique par la loi du 1^{er} août 2016 est à cet égard un atout solide qui mériterait d'être complété et exploité à cette fin, en l'enrichissant des coordonnées téléphoniques mobiles et les adresses courriels des électeurs.

La diffusion de la propagande électorale a un coût objectivé en 2015 par le rapport d'information de M. Hervé Marseille, fait au nom de la Commission des finances du Sénat, qu'une dématérialisation partielle de la diffusion aura pour effet de réduire³.

³ La distribution de la propagande électorale sur la période quadriennale 2021-2024 représente un coût de 166,6 millions d'euros hors taxe. Selon le rapport conjoint de l'IGA, l'IGF et l'IGMEAE, à l'occasion des élections municipales de 2020, une économie d'environ 22 millions

Notre Commission recommande d'évaluer les coûts de diffusion d'une information dématérialisée par mail ou sms sur les échéances électorales.

Pour autant, les membres de notre commission considèrent que le seul critère financier ne saurait prévaloir : la démocratie a un coût que l'Etat doit assumer.

Recommandation n° 2 - La CSNP se positionne en faveur de la recommandation n° 7 du rapport de la mission sur les dysfonctionnements dans la distribution de la propagande électorale pour les élections régionales et départementales des 20 et 27 juin 2021 déposé par les députés Jean-Michel Mis et Raphaël Schellenberger : « *laisser le choix aux électeurs d'opter en faveur du maintien de la distribution postale ou de l'accès dématérialisé à la propagande électorale* ».
La CSNP recommande que les pouvoirs publics assurent une promotion efficace de cette faculté d'accès dématérialisé à la propagande électorale.

Recommandation n° 3 - La CSNP recommande de compléter, sous le contrôle de la CNIL, les données du Répertoire Electoral Unique avec les coordonnées téléphoniques mobiles et les adresses courriels des électeurs dont disposent l'administration fiscale et les administrations sociales afin de disposer d'un outil permettant d'informer par voie dématérialisée, de manière neutre, les citoyens sur les échéances électorales.

III. Pour une procédure de procuration dématérialisée dans son ensemble

Peu répandu en Europe, le vote par procuration est une modalité dérogatoire au principe de secret du suffrage consacré par l'article 3 de la Constitution. Bien que n'étant pas recommandé par l'Organisation pour la sécurité et la coopération en Europe (OSCE), qui considère cette modalité comme pouvant porter atteinte au secret, à l'égalité du vote ainsi qu'au respect des choix des électeurs, le vote par procuration demeure en France, au-delà de son ancrage culturel, un outil pertinent de lutte contre l'abstention.

La crise sanitaire a démontré son utilité pour les publics les plus fragiles qui ne souhaitent pas se déplacer physiquement dans les bureaux de vote dans ce contexte sensible. La question se posera lorsque notre pays ne sera plus en situation de crise sanitaire si le système antérieur d'une seule procuration par mandataire doit être rétabli.

La CSNP estime que cet outil pourrait favoriser davantage la participation au moyen d'une procédure dématérialisée dans son ensemble. Elle observe que la mise en ligne de l'interface <https://www.maprocuration.gouv.fr/> n'a pas suffisamment répondu aux attentes de nos concitoyens dès lors qu'elle maintient l'obligation de se rendre physiquement dans un commissariat ou une gendarmerie pour attester de son identité.

Cette dernière formalité a été perçue comme décevante par une partie des électeurs mandants.

Notre Commission considère que le déploiement de l'identité numérique qui permettrait de dématérialiser l'ensemble de la procédure de procuration suppose une véritable volonté des pouvoirs publics. Cette politique volontariste repose également sur des actions de formation des agents publics chargés de la mettre en œuvre.

d'euros aurait pu être réalisée, sur un montant total d'environ 73,5 millions d'euros correspondant au coût global de la distribution de la propagande pour ces élections si 30 % des électeurs avaient choisi de recevoir la propagande par voie dématérialisée.

Notre Commission estime qu'il serait sans doute opportun de repenser le processus de procuration à l'aune de ce que pourrait permettre l'identité numérique.

Recommandation n° 4 - La CSNP recommande de poursuivre les travaux sur la dématérialisation complète de la procédure de procuration et engage les pouvoirs publics français à déployer plus activement l'identité numérique, qui constitue le dispositif le plus à même avec la signature électronique, d'assurer une authentification forte des électeurs mandants.

Recommandation n° 5 - A défaut de pouvoir complètement dématérialiser la procédure de vérification d'identité, la CSNP recommande d'ouvrir une réflexion sur la mobilisation des tiers de confiance, au rang desquels le facteur dûment assermenté, soumis au devoir d'honnêteté et de probité pour faciliter les démarches de nos concitoyens. Ce scénario éviterait un déplacement dans les services de police et de gendarmerie.

IV. Pour une expérimentation du vote par correspondance

Le vote par correspondance permet, tout comme la procuration, de voter au format papier sans se déplacer jusqu'au bureau de vote. A ce titre, il doit être envisagé comme un éventuel outil de lutte contre le phénomène de l'abstention.

Pratiqué en France de 1946 à 1975, le vote par correspondance a été abandonné en raison de fraudes constatées au niveau local. La possibilité de fraude tenait en réalité plus à un dispositif défaillant dans l'organisation et le contrôle de l'identité des électeurs qu'à la modalité même du vote par correspondance. Celle-ci est d'ailleurs répandue en Europe et fait l'objet de standards internationaux. En Allemagne, les électeurs disposent de la possibilité de voter par correspondance depuis 1957 et près de 48% d'entre eux ont fait ce choix lors des élections législatives de septembre 2021 (ils n'étaient que 28,6% à opter pour le vote par correspondance en 2017)⁴.

Les représentants du groupe La Poste considèrent que le groupe serait en mesure d'assurer la distribution des kits de vote et des bulletins.

Le vote par correspondance pose par ailleurs la question de la sécurité et de l'inviolabilité des bulletins pendant leur stockage, après l'acheminement des bulletins par voie postale et avant les opérations de dépouillement.

Recommandation n° 6 - La CSNP ne se prononce pas majoritairement pour le vote par correspondance : si celui-ci est répandu dans certains pays voisins, il représente un défi logistique et nécessite un dispositif de contrôle fiable de l'identité des électeurs, qui prévienne la fraude notamment lors de la phase de stockage des bulletins de vote avant le dépouillement. Des expérimentations locales devraient au préalable être conduites pour s'assurer des effets du vote par correspondance sur le taux d'abstention.

⁴ www.bundestagswahlleiter.de

V. Sur l'opportunité de recourir au vote électronique

Le vote par voie électronique comporte deux aspects distincts que sont les machines à voter et le vote sur internet. Ces deux aspects impliquent des approches différenciées.

- **Machines à voter : lever le moratoire de 2008**

L'article L. 57-1 du code électoral dispose que « *Des machines à voter peuvent être utilisées dans les bureaux de vote des communes de plus de 3 500 habitants figurant sur une liste arrêtée dans chaque département par le représentant de l'Etat* ». En raison de plusieurs dysfonctionnements lors du premier tour de la présidentielle de 2007, un moratoire a été mis en place depuis 2008, interdisant à toute nouvelle commune de s'équiper de machines à voter. L'État n'a agréé plus aucune machine : il gèle la possibilité pour de nouvelles communes d'y recourir. Les communes déjà équipées peuvent néanmoins continuer à les utiliser.

Les membres de la CSNP ne sont majoritairement pas favorables à la généralisation des machines à voter mais sont d'avis que le développement des consultations citoyennes sur des questions à choix multiples pourrait justifier à l'avenir le recours à ces machines. Ils considèrent, en tout état de cause, que le *statu quo* n'est plus tenable.

Les auditions conduites ont toutes conclu à la nécessité de lever ce moratoire. Plus d'un million d'électeurs utilisent des machines à voter désormais obsolètes car plus mises à jour, impliquant des vulnérabilités dans la sécurité des opérations de vote.

Recommandation n° 7 - La CSNP recommande une levée du moratoire décidé en 2008 qui rend impossible le recours aux machines de vote dans les communes non équipées et crée de l'obsolescence source de vulnérabilité sur les machines déjà installées. Elle préconise l'expérimentation afin de tendre vers des machines plus fiables et sécurisées, en lien étroit avec les services de l'Agence nationale de la sécurité des systèmes d'information.

- **Vote par internet : faire preuve de prudence et conserver le rôle central du vote papier**

La CSNP a pris note de la volonté du ministre de l'intérieur de travailler à la mise en place d'un dispositif de vote à distance pour de futures échéances électorales politiques.

Les auditions conduites dans le cadre du présent avis ont néanmoins mis l'accent sur les difficultés substantielles que soulèverait une généralisation du vote par internet en termes de sécurisation du scrutin, d'identification et d'authentification des électeurs ainsi que de vérifiabilité et de secret du vote :

- les tentatives d'ingérence dans des élections nationales ces dernières années, visant à créer du trouble pour mettre en tension des pays démocratiques comme la France, plaident pour une approche prudente sur le recours au vote en ligne. Le risque cyber avait d'ailleurs poussé le Gouvernement à annuler cette modalité pour les élections législatives des français de l'étranger de juin 2017⁵.

⁵ Arrêté du ministre des affaires étrangères du 17 mars 2017 relatif au vote par correspondance électronique pour l'élection de députés par les Français établis hors de France.

- la dématérialisation de la procédure de vote impose de déployer au préalable une identité numérique sécurisée et un dispositif d'authentification fiable à grande échelle en lien avec un prestataire de confiance. Cela suppose également une véritable volonté politique et la formation des agents chargés de la mettre en œuvre.
- la dématérialisation de la procédure doit permettre de vérifier la comptabilisation des votes des électeurs tout en garantissant leur secret, c'est-à-dire, ainsi que cela a été souligné au cours des auditions, empêcher toute traçabilité, de sorte qu'aucun lien ne puisse s'établir entre un bulletin et un électeur. Ce principe du secret du vote a valeur constitutionnelle. En l'état, il reste difficile d'assurer une stricte étanchéité entre une identité numérique électorale et empêcher toute traçabilité.

Par ailleurs, le vote immatériel n'offre pas de garantie contre les pressions externes ou la monétisation des suffrages.

Il en résulte une complexité à transposer dans le monde numérique les standards de la procédure de vote dans l'isoloir et à les déployer auprès de chaque votant. Plusieurs Etats ont fait le choix de s'appuyer sur des solutions de vote électronique à distance mais comme l'a montré une récente étude de la division de la législation comparée du Sénat⁶, cette modalité est en recul dans le monde et à l'arrêt dans la plupart des pays européens à l'exception de l'Estonie dont la taille du corps électoral est sans comparaison avec le nombre d'électeurs en France. Par ailleurs, les expériences passées de mise en œuvre d'un vote par internet ne semblent pas présenter d'impact sur la participation enregistrée à des élections politiques⁷.

Pour autant, et parce que le vote par internet est une modalité de vote pour nos concitoyens résidant à l'étranger pour les élections consulaires et législatives, les membres de la CSNP appellent les pouvoirs publics à favoriser la recherche de solutions technologiques aux exigences de la vie démocratique.

Une réflexion pourrait également être menée au niveau de l'Union européenne dans le cadre des travaux du Comité européen de la protection des données.

Recommandation n° 8 - La CSNP n'est pas favorable à une généralisation du vote par internet qui ne saurait, en tout état de cause, que constituer une offre complémentaire au rituel républicain du vote papier à l'urne, lequel présente aujourd'hui les meilleures garanties de sécurité et d'intégrité des opérations de vote.

La CSNP considère que le vote par internet aux élections consulaires et aux élections parlementaires des français de l'étranger se justifie au regard des particularités de ces élections.

Recommandation n° 9 - La CSNP recommande l'accélération du déploiement d'une identité numérique fiable et sécurisée pour l'ensemble du corps électoral qui constitue une condition préalable à la sécurisation des processus d'identification et d'authentification dans le cadre du parcours votant. La CSNP préconise d'encourager les travaux de recherche de sécurisation technologique mais également l'étude de la dimension sociologique du vote par internet.

⁶ <http://www.senat.fr/lc/lc293/lc293.pdf>

⁷ Voir notamment Rapport d'information fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du règlement et d'administration générale du Sénat sur le vote électronique du 9 avril 2014 ; Projet Netvoting_BE - Étude sur la possibilité d'introduire le vote Internet en Belgique, volet 1, 4 décembre 2020.

Recommandation n° 10 - D'une manière générale, la CSNP propose de relever le niveau des exigences techniques et juridiques applicables au vote par internet en s'appuyant sur d'autres modèles étrangers, comme la Suisse qui a défini des exigences de nature à développer des solutions plus sûres en adoptant notamment des niveaux d'exigences supplémentaires (niveau 4 ou niveau 5).

Elle constate que les exigences françaises actuelles relatives au vote par internet relèvent d'une simple recommandation de la CNIL de 2010, actualisée en 2019, et que les traitements de données à caractère personnel liées à l'organisation des élections nationales ne font l'objet d'aucun sous-encadrement du cadre juridique de la protection des données à caractère personnel.

Annexe

Au cours des auditions, d'autres réflexions hors du champ de compétence de la Commission supérieure du numérique et des postes ont pu émerger avec la modernisation des processus électoraux. Les membres souhaitent en faire état en marge de cet avis sur les apports du numérique à la modernisation du processus électoral :

- **Sur le vote par anticipation**

La CSNP observe qu'une partie de la population est attachée au rituel républicain d'un vote le dimanche sur une plage horaire définie mais que le vote sur une seule journée entraîne sans doute l'abstention d'un certain nombre d'électeurs, moins attachés à cette tradition.

Le vote par anticipation, permettant à tout ou partie de l'électorat de se rendre dans un bureau de vote avec une pièce d'identité valide pendant certaines heures avant le jour du scrutin, existe au Danemark, en Estonie, en Finlande, en Lettonie, en Norvège, en Suède et en Suisse.

Une expérimentation portant sur l'ouverture de bureaux de vote en semaine sur une courte plage horaire compatible avec l'activité professionnelle des citoyens, ou sur les lieux d'étude, en complément du vote le dimanche, permettrait de vérifier et mesurer :

- la pertinence du vote par anticipation dans le contexte français,
- les effets du vote par anticipation sur le taux de participation,
- les mesures qui doivent être prises pour sécuriser la bonne tenue du scrutin et limiter les risques de fraude pendant une période de stockage des bulletins de plusieurs jours.

Les difficultés à mobiliser tous les intervenants (art. R.42 du code électoral) pour une bonne tenue des bureaux de vote iront probablement de manière croissante dans l'avenir et obligent à anticiper cet appauvrissement du personnel.

- **Sur l'apprentissage de la démocratie**

L'analyse des comportements électoraux démontre que la pratique du vote est une habitude qui nécessite un apprentissage. En France, l'accompagnement dans le processus électoral reste trop dépendant de l'enseignement dispensé par la cellule familiale générant ainsi de très fortes inégalités alors même que le vote est un phénomène collectif. Cela dans un contexte de cellules familiales de plus en plus déstructurées. Comme l'a souligné Céline Braconnier, les enseignements civiques dispensés au sein de l'école républicaine sont trop théoriques. Paradoxalement, la France est l'un des pays dont les programmes scolaires comprennent le plus d'heures d'instruction civique mais sans implications concrètes sur la pratique citoyenne. Un apprentissage concret de la pratique du vote dans les programmes scolaires pourrait générer une habitude que les élèves conserveront tout au long de leur vie de citoyens. En tout état de cause, les jeunes pourraient être davantage associés et impliqués dans le vote démocratique.

- **Sur la création d'une autorité indépendante de supervision des élections**

L'organisation des élections en France est placée sous la responsabilité du Ministère de l'intérieur et sous le contrôle du Conseil constitutionnel. Cette place centrale du Gouvernement ne semble pas constituer un motif d'inquiétude particulier chez nos concitoyens et dans la classe politique. Dans l'optique d'une modernisation ambitieuse des processus électoraux, la création d'une autorité indépendante en charge du bon déroulement du processus électoral pourrait cependant constituer une garantie supplémentaire en matière de transparence démocratique.

Liste des personnes auditionnées par la CSNP

Mme Céline Braconnier, directrice de science-po Saint-Germain-en-Laye, professeure de science politique, chercheuse au centre de recherches sociologiques sur le droit et les institutions pénales (CESDIP)

Mme Véronique Cortier, directrice de recherche au Centre national de la recherche scientifique (CNRS), spécialiste des protocoles de sécurité informatique

Mme Laurence Haguenaer, directrice des français de l'étranger et de l'administration consulaire

Mme Christine Hennion, députée des Hauts-de-Seine, membre de la Commission supérieure du numérique et des postes, rapporteure de la mission d'information commune sur l'identité numérique

M. Yannick Imbert, directeur des affaires territoriales et publiques du groupe La Poste

M. Guillaume Poupard, directeur général de l'Agence nationale de sécurité des systèmes d'information (ANSSI)

M. Romain Rambaud, professeur des universités, agrégé de droit public, Université Grenoble-Alpes

M. Olivier Vallet, président directeur général de Docaposte

Représentants de la Commission nationale de l'informatique et des libertés

M. Louis Dutheillet de Lamothe, secrétaire général

Mme Nina Le Bonniec, juriste service des affaires régaliennes et des collectivités territoriales

M. Armand Heslot, chef du service de l'expertise technologique

Bibliographie

- Rapport d'information de M. François-Noël Buffet du 16 décembre 2020 fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur le vote à distance ;
- Rapport d'information de Mme Jacky Deromedi et MM. Christophe-André Frassa et Jean-Yves Leconte du 16 décembre 2020 fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur l'organisation des élections consulaires en 2021 ;
- Rapport d'information de Mme Christine Hennion et M. Jean-Michel Mis du 8 juillet 2020 en conclusion des travaux de la mission d'information commune sur l'identité numérique ;
- Rapport d'information de Mme Jacky Deromedi et M. Yves Détraigne du 24 octobre 2018 fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur le vote électronique ;
- Rapport d'information de MM. Alain Anziani et Antoine Lefèvre du 9 avril 2014 fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du règlement et d'administration générale du Sénat sur le vote électronique ;
- Sociologie de la mal-inscription et de ses conséquences sur la participation électorale, Céline Braconnier, Jean-Yves Dormagen, Ghislain Gabalda, Xavier Niel – Revue française de sociologie 2016/1 (vol. 57) ;
- Contribution écrite de M. Romain Rambaud, professeur des universités, agrégé de droit public, sur les modalités alternatives de vote et l'abstention ;
- Projet Netvoting_BE - Étude sur la possibilité d'introduire le vote Internet en Belgique, volet 1, 4 décembre 2020 ;
- Site internet du bureau des institutions démocratiques et des droits de l'homme de l'Organisation pour la sécurité et la coopération en Europe (OSCE) – <https://www.osce.org/odihr>
- Site internet de l'International Institute for Democracy and Electoral Assistance (IDEA) - www.idea.int
- Rapport sur le « Bilan et les perspectives du Répertoire Electoral Unique » publiée par l'Inspection générale de l'administration, l'Inspection générale des finances et l'Inspection générale des affaires étrangères en juin 2020



COMMISSION SUPERIEURE DU NUMERIQUE ET DES POSTES

AVIS N°2021-06 DU 8 DECEMBRE 2021

**SUR LE PROJET DE RAPPORT
AU GOUVERNEMENT ET AU PARLEMENT
SUR LE COÛT NET EN 2020 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 15 octobre 2021 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 2020 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 2020/2022 signé entre l'Etat, l'Association des Maires de France et des Présidents d'intercommunalité, et La Poste ;

Vu les réunions techniques préparatoires du :

- 3 novembre 2021 pour le groupe La Poste :
 - o M. Vincent MOULLE, directeur de la Régulation, de la Concurrence et des Relations Institutionnelles ;
 - o M. Denis JORAM, directeur de la Régulation et des Etudes ;
 - o M. Julien BECHU, chargé du pôle Economie des Réseaux et de la Distribution ;
 - o Mme Rebecca PERES, déléguée aux Affaires Territoriales et Parlementaires.
- 10 novembre 2021 pour l'Arcep :
 - o Mme Anne YVRANDE-BILLON, directrice Economie, Marchés et Numérique ;
 - o M. Hisham ABBAS, chef de l'unité Coût et Audit réglementaire postale et audiovisuel ;
 - o M. Victor MARCHAND, chargé de mission au sein de l'unité Coût et Audit réglementaire postale et audiovisuel.

Ces deux réunions techniques ont été menées pour la CSNP par Mme Valérie MONTANE, secrétaire générale, M. Valentin MUGNIE, secrétaire général adjoint et Mme Françoise SOKOLOWSKI, personnalité qualifiée.

Vu les auditions du 19 novembre 2020 réalisées en visioconférence :

- pour l'Arcep :
 - o Mme Anne YVRANDE-BILLON, directrice Economie, Marchés et Numérique ;
 - o M. Hisham ABBAS, chef de l'unité Coût et Audit réglementaire postale et audiovisuel
- pour le groupe La Poste :
 - o M. Nicolas ROUTIER, directeur général adjoint, en charge du Service Public et de la Régulation ;
 - o M. Vincent MOULLE, directeur de la Régulation, de la Concurrence et des Relations Institutionnelles ;
 - o M. Yannick IMBERT, directeur des affaires territoriales et publiques
 - o M. Julien BECHU, chargé du pôle Economie des Réseaux et de la Distribution ;
 - o Mme Rebecca PERES, déléguée aux Affaires Territoriales et Parlementaires
 - o M. Jean BIDEAU, stagiaire

Ces auditions ont été menées dans le cadre d'une séance de la CSNP, sous la présidence de Mme Mireille CLAPOT, Présidente de la CSNP et de M. Patrick CHAIZE, pilote du groupe de travail sur La Poste au sein de la CSNP. Ont également participé aux visioconférences :

- o Mme Toine BOURRAT, sénatrice des Yvelines ;

- M. Jean-Pierre CORBISEZ, sénateur du Pas-de-Calais ;
- M. Christian REDON-SARRAZY, sénateur de la Haute-Vienne ;
- Mme Denise SAINT-PE, sénatrice des Pyrénées-Atlantiques ;
- Mme Jeanne BRETECHER, personnalité qualifiée ;
- Mme Françoise SOKOLOWSKI, personnalité qualifiée ;

- Mme Valérie MONTANE, secrétaire générale ;
- M. Valentin MUGNIE, secrétaire général adjointe
- Mme Quynh-Anh TO, stagiaire.

I. ELEMENTS DE CONTEXTE

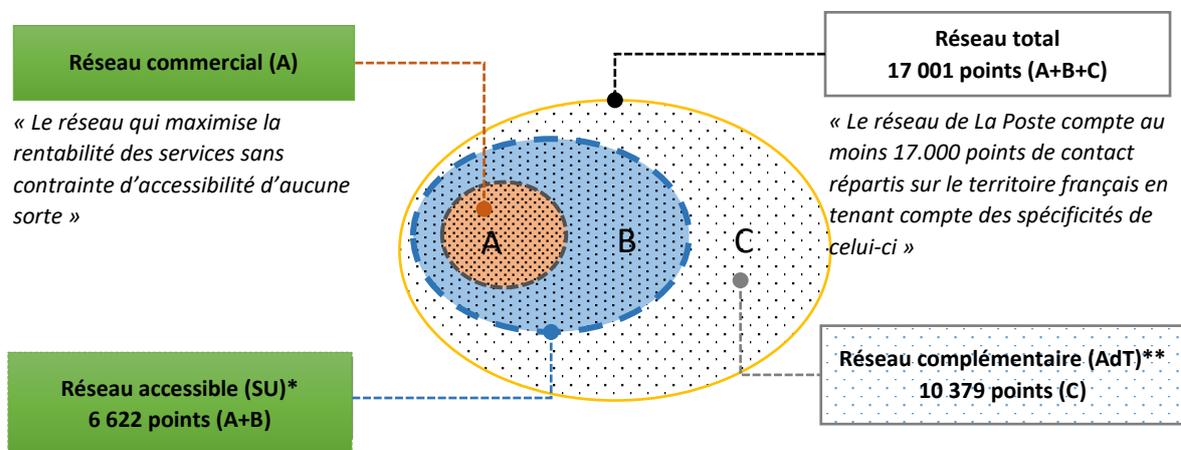
L'article 6 de la loi n°90-568 du 2 juillet 1990 prévoit qu'en complément de ses obligations de service universel, La Poste contribue à l'aménagement du territoire par son réseau de points de contact. Un fonds postal national de péréquation territoriale est constitué pour financer le coût du maillage territorial complémentaire. « Les ressources du fonds proviennent de l'allègement de fiscalité locale dont bénéficie La Poste en contrepartie de sa mission d'aménagement du territoire ».

Le présent avis porte donc sur le projet de rapport au Gouvernement et au Parlement déterminant le coût net en 2020 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 12^{ème} évaluation du coût net de cette mission.

1. Le réseau postal de points de contact remplit deux missions de service public de présence postale territoriale : le service universel postal (SU), dit réseau accessible, et l'aménagement et développement du territoire (AdT), dit réseau complémentaire.

Les périmètres de chacun de ces deux réseaux sont **interdépendants**. La somme des deux est égale au réseau total des points de contact de La Poste (au moins 17 000 points de contact répartis sur l'ensemble du territoire français).

Le calcul du coût net des obligations de service public nécessite d'identifier trois réseaux théoriques au sein du réseau total réel de La Poste.



Source : La Poste – Nombre au 30/06/2020

*Accessibilité au Service Universel (A+B)

« Au moins 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 toutes les communes de plus de 10.000 hab. disposent d'au moins 1 point de contact par tranche de 20.000 hab ». Article R. 1-1 du CPCE

**Aménagement du territoire (A+B+C)

« Pas plus de 10 % de la population d'un département n'est éloignée de plus de 5 km et de plus de 20 mn de trajet automobile des plus proches points de contact de La Poste ». Article 6 de la loi du 2 juillet 1990

2. Le coût net de la mission du service universel postal et celui de la mission d'aménagement du territoire sont déterminés en mesurant la perte de contribution liée aux contraintes des missions de service public par rapport au « réseau commercial optimal » (A), qui est le réseau « optimal » non contraint en nombre de points et qui maximise la rentabilité des services sans contrainte d'accessibilité.

3. En 2020, la mise en place d'une nouvelle méthodologie actualise les périmètres du réseau postal : cette nouvelle méthodologie de sélection des points de contact reflète plus fidèlement la répartition des bassins de population et des centres économiques sur l'ensemble du territoire. La précédente méthode datait de 2007 et n'avait pas été mise à jour depuis.

L'évolution démographique, économique et technologique imposait cette évolution afin de continuer d'assurer le respect des contraintes légales des deux missions de service public, notamment celle du service universel. Cette nouvelle approche s'appuie sur des données « *démographiques officielles et publiques issues des bases de l'INSEE et sur des référentiels pérennes ayant une légitimité administrative, économique et sociodémographique (unités urbaines, territoires des bassins de vie, cantons...* » (extrait du projet de rapport de l'ARCEP).

Annoncée en 2020, cette adaptation avait été encouragée par la CSNP dans son avis n°2020-11 du 1^{er} décembre 2020.

Suite à cette actualisation, les périmètres des deux missions de service public ont donc substantiellement évolué. Ces périmètres étant interdépendants, se produit alors un phénomène de « vases communicants » à réseau constant, réseau qui correspond à l'obligation d'aménagement du territoire (loi n° 2010-123 du 9 février 2010) qui prévoit que le réseau de La Poste « *compte au moins 17 000 points de contact répartis sur le territoire français* ».

II. RESULTATS DE L'EVALUATION 2020

A. Une augmentation substantielle du coût de la mission d'aménagement du territoire

Pour l'année 2020, l'Arcep évalue le coût net de la mission d'aménagement du territoire à 325 M€, soit une progression de 94 M€ par rapport au coût évalué en 2019 (231 M€).

Cette hausse est essentiellement due à l'actualisation de la méthode de sélection des points de contact de La Poste qui a fait basculer du périmètre accessible vers le périmètre complémentaire 911 points de contact, faisant passer le périmètre complémentaire à 10 379 points de contact contre 9 475 points de contacts selon la précédente méthodologie.

	Périmètre avant actualisation		Périmètre après actualisation	
	Réseau accessible (SU)	Maillage complémentaire (AdT)	Réseau accessible (SU)	Maillage complémentaire (AdT)
Points en propre	6 417	1 265	5 438	2 244
Points partenaires	1 116	8 203	1 184	8 135
Total	7 533	9 468	6 622	10 379

Source : Arcep

Le réseau complémentaire compte désormais une proportion plus importante de bureaux de poste (points gérés en propre), 977 points, dont les charges sont plus élevées que celles des points partenaires.

EVOLUTION DU RESEAU GLOBAL DE LA POSTE 2019/2020

	2019	2020
Total réseau	17 020	17 001
dont bureaux en propre	7 948	7 682
dont partenaires	9 072	9 319
- agences postales communales	6 184	6 337
- relais poste	2 888	2 982

Source : Arcep

Au 30 juin 2020, le réseau de La Poste compte 7 682 bureaux de poste gérés en propre, soit 266 bureaux de moins par rapport à l'année précédente. La logique d'adaptation et de transformation du réseau se poursuit avec le développement du nombre de points de contact en partenariat (agences postales communales et intercommunales, relais commerçants ou toute autre forme de partenariats), 247 de plus qu'en 2019.

A cette date, le réseau de points partenaires représente près de 55 % du réseau postal.

Ainsi que le souligne l'Arcep dans son rapport, « *le douzième exercice d'évaluation du coût net de la mission d'aménagement du territoire de La Poste par l'ARCEP est un exercice singulier, d'une part, parce qu'il est réalisé à partir de l'actualisation des périmètres des réseaux accessible et complémentaire et, d'autre part, parce qu'il s'inscrit dans le contexte de la crise sanitaire* ». (extrait du projet de rapport de l'Arcep).

La baisse du nombre d'opérations dans les points de contact observée ces dernières années a été fortement accentuée par la crise sanitaire entre 2019 et 2020. La baisse des produits des opérations est elle aussi importante, mais dans une moindre mesure. Le produit des opérations dans le réseau de La Poste se compose du produit net bancaire (PNB) des services financiers et du produit des ventes du courrier et du colis.

Selon le rapport de l'Arcep, l'activité de La Poste est concentrée dans un nombre restreint de points de contact : plus de 60 % de l'activité et 50 % du chiffre d'affaires seraient concentrés dans 2 000 points de contact. Les 10 000 points de contact les moins actifs représentent 86 % des points de contact relevant de la mission d'aménagement du territoire et ne génèrent que 7 % de l'activité et seulement 12 % du chiffre d'affaires du réseau.

Pour sa part, La Poste estime le coût net de la mission d'aménagement du territoire à **358 M€**, pour l'année 2020 soit un écart de 33 M€, représentant 1,4 % du périmètre des charges. Cet écart s'explique principalement par les raisons suivantes :

- l'Arcep s'appuie sur une photographie à un instant T de l'activité des points de contact postaux ;
- La Poste utilise des méthodes de calcul des coûts à des fins plus larges (gestion du réseau et allocation des coûts et des moyens pour l'ensemble de ses activités).

B. Un « transfert » des coûts de la mission du service universel postal vers la mission d'aménagement du territoire

En complément de l'évaluation établie par l'Arcep (325 M€), qui est la référence officielle pour le calcul annuel du coût net de la mission d'aménagement du territoire, il convient de zoomer sur les chiffres de La Poste qui donnent une lecture globale du coût des contraintes territoriales (service universel postal et aménagement du territoire).

La Poste met en évidence à la fois l'impact de l'actualisation sur l'évolution de la structure des points de contact et sur l'allocation des coûts des contraintes.

Impact sur l'évolution de la structure des points de contact			
	Avant actualisation du réseau accessible	Après actualisation du réseau accessible	
Taille du réseau accessible	7 533	6 622	-911
dont points en propre	6 404	5 438	-966
dont partenaires	1 129	1 184	55
Taille du réseau complémentaire	9 468	10 379	911
dont points en propre	1 278	2 244	966
dont partenaires	8 190	8 135	-55

Allocation du coût des obligations (en M€) – Estimations par La Poste			
	Avant actualisation du réseau accessible	Après actualisation du réseau accessible	
Coût net de la présence territoriale	709	709	-
dont Accessibilité du SU	461	351	-110
dont Aménagement du Territoire	248	358	110

Source : La Poste

III. POSITION DE LA COMMISSION

1. La Commission supérieure prend acte de la forte progression du coût net de la mission d'aménagement du territoire pour 2020, soit 325 M€, liée au changement de méthodologie de sélection des points de contact.

Si cette nouvelle méthode de sélection lui paraît intégrer de manière plus pragmatique et réaliste la réalité des territoires, la Commission supérieure regrette que les délais pris pour actualiser la méthodologie initialement retenue en 2007 créent un effet de bord de l'ordre de 100 M€ pour le seul exercice 2020.

La Commission supérieure souhaite que la nouvelle méthodologie, présentée comme fiable et stable en raison des données utilisées (données INSEE et autres référentiels pérennes) puisse éviter, pour l'avenir, de tels effets d'un exercice à l'autre.

2. La Commission supérieure relève que cette augmentation liée à une évaluation plus fine du coût des réseaux d'accessibilité pose, avec encore plus d'acuité, la question du financement des missions de service public tant celle de l'aménagement du territoire, largement sous-compensée, que celle du service universel postal.

La question du financement de cette dernière va se poser de façon cruciale puisque l'activité du courrier est déficitaire depuis 2018 et que l'évaluation du coût net de cette mission pourrait être confié à l'Arcep (cf. rapport du sénateur Patrick CHAIZE d'avril dernier).

Quant à la mission d'aménagement du territoire, des ajustements budgétaires conjoncturels ont permis de préserver son financement, mais la question reste entière à quelques mois de la négociation du futur contrat tripartite (Etat, AMF et La Poste) de présence postale territoriale et de la préparation du prochain contrat d'entreprise qui lie l'Etat et La Poste.

A cet égard, la Commission supérieure rappelle sa position concernant le financement des missions de service public confiées au groupe La Poste : il est essentiel que l'Etat assume la juste compensation des coûts générés par la mise en œuvre de ces missions.

La Commission supérieure s'interroge sur les conséquences des transferts de coût de la mission du service public universel vers la mission d'aménagement du territoire.

Le financement de ces deux missions ne relevant pas des mêmes mécanismes :

- un fonds de compensation financé par les prestataires postaux non activé jusqu'à présent pour la mission du service universel postal,
- un fonds de péréquation sous forme d'abattements de fiscalité locale pour la mission d'aménagement du territoire. Depuis 2021, une dotation est prévue par l'Etat en plus de l'abattement de fiscalité pour compenser la baisse du fonds liée à la réforme de la cotisation sur la valeur ajoutée des entreprises(CVAE).

3. La Commission supérieure demande que le rôle et les pouvoirs de l'Arcep évoluent afin que celle-ci puisse disposer d'une vision plus prospective conformément à ce que la Commission supérieure a demandé dans son précédent avis pour le même exercice (avis n° 2020-11 du 1^{er}

décembre 2020). Les nouveaux outils utilisés permettent *a priori* de faire des projections jusqu'à 2030.

Elle demande qu'un cahier des charges puisse être rédigé pour travailler ces différents aspects, d'autant qu'elle considère que les quatre missions de service public sont de plus en plus dépendantes les unes des autres et que leurs coûts respectifs pourraient en être impactés.

Elle souhaite également qu'au-delà du seul calcul des coûts nets puisse être menée une réflexion sur la définition d'indicateurs.

Par ailleurs, la Commission supérieure regrette que ne soient pas encore intégrés dans le périmètre de calcul des coûts, ceux liés à la non-qualité : cette demande est exprimée de manière récurrente par la Commission supérieure.

Sur l'ensemble de ces points, la Commission supérieure se dit prête à s'investir dans toute démarche qui permettrait d'optimiser les travaux de l'Arcep.

IV. CONCLUSION

La Commission supérieure prend acte de la forte progression du coût net 2020 de la mission d'aménagement du territoire confiée à La Poste (+ 94 M€). Si elle valide le nouveau mode de sélection des points de contact postaux et l'impact sur le calcul du coût net de la mission, elle s'interroge sur les conséquences de ce changement sur le financement de la mission d'aménagement du territoire. En tout état de cause, elle donne un avis favorable sur le projet de rapport de l'Arcep destiné au Gouvernement et au Parlement.

La Commission supérieure émet dans cet avis un certain nombre de recommandations et d'exigences qu'elle entend voir prises en compte et suivies de faits concrets. Dans un contexte économique, social et sanitaire plus que jamais difficile, il y va de la pérennité des missions de service public portées par La Poste, leur réalité et leur efficacité sur les territoires.