CSNP

COMMISSION SUPÉRIEURE DU NUMÉRIQUE ET DES POSTES

RAPPORT N° 2024-07 DU 3 OCTOBRE 2024

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

RAPPORT N°2024-07 DU 3 OCTOBRE 2024

LES ENJEUX DE LA TRANSPOSITION DE LA DIRECTIVE NIS 2 EN FRANCE

PRESENTE PAR

M. DAMIEN MICHALLET, SENATEUR DE L'ISERE, PRESIDENT DE LA CSNP

ET

MME ANNE LE HENANFF, DEPUTEE DU MORBIHAN, RAPPORTEURE

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

Les membres de la Commission supérieure du numérique et des postes (CSNP) accueillent très favorablement la transposition de la directive NIS 2 qui a été adoptée le 14 décembre 2022 avec le plein soutien des autorités françaises : il est essentiel de relever le niveau de sécurité numérique global et la directive NIS 2 constitue un levier essentiel pour atteindre cet objectif.

Alors que la directive NIS 1 concernait près de 600 entités, c'est un changement d'échelle qui est opéré avec la transposition de la directive NIS 2 puisque près de 15 000 entités seraient désormais concernées selon l'ANSSI. Ce changement d'échelle correspond également à un véritable changement de paradigme en matière de sécurité numérique.

A l'automne 2023, l'ANSSI a lancé une phase de consultations auprès des différents acteurs concernés par la transposition de la directives NIS 2 : les fédérations d'entreprises, les représentants des collectivités locales et territoriales, les fédérations d'acteurs et des usagers…

La restitution de ces consultations a eu lieu le 24 avril 2024 et, en prévision de sa saisine par l'ANSSI, les membres de la CSNP ont confié en mars 2024 à M. Damien MICHALLET, sénateur de l'Isère et président de la CSNP, et Mme Anne LE HÉNANFF, députée du Morbihan, le pilotage d'un groupe de travail sur la transposition de la directive *Network and Information Systems 2*, dite NIS 2 pour lequel Mme Anne Le Hénanff a été nommée rapporteure.

Ce groupe de travail est surtout né de la volonté d'analyser l'impact que les nombreuses nouvelles obligations de la directive auront sur les entités concernées et de la meilleure manière d'adapter notre droit en conséquence avant même que le projet de loi transposant la directive ne soit présenté en conseil des ministres et inscrit à l'ordre du jour du Parlement.

De mars à mai 2024, le groupe de travail a auditionné 41 acteurs, notamment l'Agence nationale de la sécurité des systèmes d'information (ANSSI), des éditeurs de logiciels, des *clouders* européens et extra-européens, des associations représentant des collectivités et des entreprises, des cabinets de conseils, des responsables de systèmes d'information, des juristes, etc…

Il ressort de ces auditions que la transposition de la directive NIS 2 fixée au 17 octobre 2024 soulève un certain nombre de défis pour les entités qui vont se retrouver régies par ces dispositions.

La dissolution de l'Assemblée nationale le 9 juin 2024 a, de fait, perturbé le calendrier d'adoption du projet de loi de transposition de la directive NIS 2.

Au terme de ses travaux, le groupe de travail a présenté au cours de la séance plénière du 18 septembre 2024 aux membres de la CSNP le présent rapport sur les enjeux posés par la transposition de la directive NIS 2 et formule 32 recommandations.

RECOMMANDATIONS

Recommandation n°1 : Organiser une véritable campagne de communication à destination des entreprises et des collectivités locales. Cette campagne d'information à large échelle pourrait également inclure le grand public.

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

Recommandation n°3 : Préciser dans la loi que les délais de mise en conformité sont fixés au 31 décembre 2027. Si les décrets et textes règlementaires étaient pris avec beaucoup de retard, comme cela avait été le cas dans le cadre de la transposition de la directive NIS1, le législateur serait en mesure de voter une loi rectificative.

Recommandation n°4 : Compléter l'étude d'impact sur les coûts humains, techniques et financiers pour les entités ainsi que sur les délais de mise en conformité.

Recommandation n°5 : Créer une commission spéciale pour l'examen du projet de loi *relatif à la résilience des activités d'importance vitale, à la protection des infrastructures critiques, à la cybersécurité et à la résilience opérationnelle numérique du secteur financier.*

Recommandation n°6 : Créer une commission permanente en charge du numérique à l'occasion de la prochaine révision du règlement de l'Assemblée nationale et de celui du Sénat.

Recommandation n°7 : Limiter au maximum le renvoi à des décrets en Conseil d'État.

Recommandation n°8 : Réintégrer dans le projet de loi les seuils et critères précisés dans la directive NIS 2 et ses annexes.

Recommandation n°9 : Confier à l'ANSSI la responsabilité de désigner les collectivités locales soumises à NIS 2.

Recommandation n°10 : Préciser dans le texte de loi la notion d'*« incident important »* en publiant une liste de critères objectivables par les entité essentielles et importantes.

Recommandation n°11 : Prévoir dans la loi des mécanismes explicites de protection des informations divulguées lors de signalement d'incidents, afin de garantir la confidentialité des données sensibles et stratégiques des entreprises qui pourraient être transmises dans le cadre d'une notification.

Recommandation n°12 : Prévoir dans la loi une clause d'adaptabilité aux évolutions technologiques liées notamment à l'usage de l'intelligence artificielle en matière de cybersécurité.

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

Recommandation n°14 : Mettre en place un guichet unique pour déclarer les incidents en élargissant les fonctionnalités de la plateforme 17Cyber

Recommandation n°15 : Uniformiser les formulaires de remontées d'incidents.

Recommandation n°16 : Renforcer la présence de l'ANSSI en région.

Recommandation n°17 : Certifier par l'ANSSI les prestataires privés susceptibles d'intervenir auprès d'une entité soumise à la directive NIS 2.

Recommandation n°18 : Clarifier le rôle des CSIRT territoriaux dans la transposition de NIS 2.

Recommandation n°19 : Créer une mission d'information parlementaire sur le rôle, le fonctionnement et le financement des CSIRT régionaux et sectoriels.

Recommandation n°20 : Allouer des crédits supplémentaires au SGDSN dans le cadre du programme 129 lors du PLF pour 2025, crédits qui seront fléchés vers le GIP ACYMA.

Recommandation n°21 : Accompagner financièrement les entités ne disposant pas des moyens nécessaires à leur mise en conformité.

Recommandation n°22 : Faire auditer par l'ANSSI le degré de maturité des collectivités locales qui seront soumises à la directive NIS 2 et en mesure de se conformer au calendrier de mise en œuvre. Un accompagnement spécifique, technique et financier sera prévu pour celles n'ayant pas les moyens nécessaires. La mobilisation des financements de la stratégie nationale d'accélération cyber vers des outils intégrés conformes aux exigences posées par l'ANSSI doit être étudiée.

Recommandation n°23 : Introduire plus de progressivité dans la mise en œuvre de la directive NIS 2 et réaliser une étude d'impact plus précise pour qualifier les risques, les menaces et les coûts financiers, administratifs, démocratiques des cyberattaques pesant sur les collectivités territoriales. Les membres de la CSNP appuient les demandes des collectivités territoriales exprimées en ce sens.

Recommandation n°24 : Inciter les collectivités, notamment celles qui n'ont pas les moyens humains nécessaires, à faire le choix d'une solution dite SaaS afin de maintenir le meilleur niveau de cybersécurité possible.

Recommandation n°25 : Renforcer le rôle des préfets dans l'accompagnement des collectivités à se conformer aux obligations de la directive NIS 2.

Recommandation n°26 : Prévoir un accompagnement financier des acteurs les plus fragiles afin que la mise en œuvre de la directive NIS 2 constitue un levier puissant pour encourager la mutualisation et renforcer la sécurisation des systèmes d'information des acteurs de la santé.

Recommandation n°27 : Renforcer la concertation entre l'ANSSI, le ministère de la Santé et les entités du secteur de la santé potentiellement concernées par un relèvement de leur statut d'entité importante à entité essentielle en cas de crise sanitaire sur les mesures adaptées et proportionnées à mettre en place.

Recommandation n°28 : Préciser le régime applicable au secteur des assurances en application de la *lex specialis* pour lever les risques de double régulation entre la directive NIS 2 et le règlement DORA.

Recommandation n°29 : Intégrer dans le texte de transposition de la directive NIS 2 la nécessité pour les entités essentielles et importantes de modifier les obligations contractuelles qui les lient à leurs sous-traitants.

Recommandation n°30 : Préciser dans la loi le périmètre de l'article 28 de la directive NIS 2 relatif à la base des données d'enregistrement des noms de domaine.

Recommandation n°31 *(en cas d'évolution du projet de loi)* : Faire le choix de déléguer à une commission *ad hoc* et indépendante le pouvoir de sanctions en cas de non-respect des obligations introduites par la directive.

Recommandation n°32 : Accorder une certaine souplesse dans l'appréciation des infractions aux obligations et les sanctions relatives jusqu'au 31 décembre 2027.

I. LA DIRECTIVE NIS 2 : UN LEVIER PUISSANT POUR RELEVER LE NIVEAU DE SECURITE NUMERIQUE DE LA FRANCE

➢ La directive NIS 2 : un changement de paradigme par rapport à la directive NIS 1

Six ans après son adoption, la directive (UE) 2016/1148 du 6 juillet 2016[1], dite NIS1, est révisée et remplacée par la directive (UE) 2022/2555 du 14 décembre 2022[2] , dite NIS 2. **Cette directive répond à un besoin d'harmonisation des normes communes en matière de cybersécurité et à la nécessité de faire face à l'augmentation des cyberattaques dans l'Union européenne**. La Commission européenne avait soumis, le 16 décembre 2020, une proposition tendant à réviser la Directive NIS 1, qui constituait le premier texte législatif de l'Union européenne sur la cybersécurité et dont le champ d'application devait être étendu.

Cette proposition s'inscrivait dans la ligne des priorités de la Commission pour la stratégie 2020-2025 visant à rendre l'Europe apte à l'ère numérique[3].

Dans un communiqué de presse du 13 mai 2022, Thierry Breton, alors commissaire européen au commerce intérieur, avait souligné l'importance de cette révision de la Directive NIS 1: « *Malgré leurs accomplissements notables et leur incidence positive, ces règles ont dû être mises à jour en raison du degré croissant de numérisation et d'interconnexion de notre société et de l'augmentation des actes de cybermalveillance à l'échelle mondiale*[4]. »

La directive a été publiée au Journal officiel de l'Union européenne le 27 décembre 2022. **Les États-membres doivent désormais transposer les nouvelles dispositions dans leur droit national au plus tard le 17 octobre 2024 et les appliquer à partir du 18 octobre 2024**. L'Article 40 de la directive prévoit un nouveau réexamen par la Commission au plus tard le 17 octobre 2027 et tous les 36 mois par la suite.

Le projet de loi *relatif à la résilience des activités d'importance vitale, à la protection des infrastructures critiques, à la cybersécurité et à la résilience opérationnelle numérique du secteur financier*, transposant notamment la directive NIS 2, devait être présenté en conseil des ministres le 12 juin dernier, en vue d'être inscrit à l'ordre du jour du Parlement. La dissolution de l'Assemblée nationale, annoncée par le Président de la République le 9 juin au soir, a mis un coup d'arrêt au parcours de ce texte de loi avant même son commencement. A l'heure où parait le présent rapport, ledit texte de loi n'a toujours pas été présenté en conseil des ministres, et la date du 17 octobre 2024 approchant, son avenir sous la forme qu'on lui connait, est incertain.

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

La directive NIS 1 avait identifié six secteurs essentiels. Dans son annexe I, la directive NIS 2 reprend et complète certains secteurs inclus par la France au niveau national en 2018. **Elle établit une liste des secteurs hautement critiques.** Dans son annexe II, **la directive NIS 2 établit également une liste des secteurs critiques.**

---

[1] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016L114

[2] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022L2555&from=FR

[3] https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333#:~:text=The%20NIS2%20Directive%3A%20A%20high%20common%20level%20of%20cybersecurity%20in%20the%20EU,

[4] https://ec.europa.eu/commission/presscorner/detail/fr/ip_22_2985

Tableau comparatif des secteurs concernés

Directive NIS 1	Directive NIS 2
Secteurs essentiels • Energie • Transport • Banques • Infrastructures de marchés financiers • Secteur de la santé • Fourniture et distribution d'eau potable • Infrastructures numériques	**Secteurs hautement critiques** • Energie • Transports • Secteur bancaire • Infrastructures des marchés financiers • Santé • Eau potable • Eaux usées • Infrastructure numérique • Gestion des services TIC (interentreprises) • Administration publique (dont les activités ne portent pas sur la sécurité nationale, sécurité publique, la défense ou l'application de la loi) • Espace **Autres secteurs critiques :** • Services postaux et d'expédition • Gestion des déchets • Fabrication, production et distribution de produits chimiques • Production, transformation et distribution des denrées alimentaires • Fabrication • Fournisseurs numériques • Recherche

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

- **Plus de 15 000 entités concernées par la transposition de la directive NIS 2**

Selon l'ANSSI, ce sont près de 15 000 entités qui seront concernées par la transposition de la directive NIS 2 contre près de 600 entités concernées par la directive NIS 1.

La directive NIS 2 comme le projet de loi transmis par l'ANSSI distingue deux catégories entrant dans son périmètre : **les entités essentielles actives dans des secteurs hautement critiques et les entités importantes.**

Les entités essentielles sont des organisations appartenant à des secteurs d'activité hautement critiques, fixés par décret en Conseil d'Etat, dont les effectifs, le chiffre d'affaires annuel et le total du bilan annuel excèdent des seuils définis par voie règlementaire. Ces entités incluent des

établissements publics à caractère industriel et commercial, des opérateurs de services de confiance qualifiés, des offices d'enregistrement, des fournisseurs de service de système de noms de domaine, ainsi que certaines administrations publiques et collectivités territoriales.

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

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

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

Le changement majeur introduit par la transposition de la directive NIS 2 porte sur l'extension aux entités importantes, **aux collectivités locales de plus de 30 000 habitants et aux entreprises privées qui dépasseront certains seuils** (nombre de salariés, chiffre d'affaires, bilan).

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

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

Source : ANSSI

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

Le nombre d'entreprises privées concernées seraient, selon l'ANSSI, de l'ordre de 14 000.

Les organisations représentatives des entreprises consultées par la CSNP considèrent que ce nombre pourrait être plus élevé.

II. UNE CAMPAGNE DE COMMUNICATION AMBITIEUSE NECESSAIRE

Il ressort des auditions conduites par la CSNP, qu'à quelques semaines de l'entrée en vigueur de la directive NIS 2, le 17 octobre prochain, il est plus que vraisemblable que de très nombreuses entreprises et collectivités locales ne soient pas pleinement informées de l'existence de cette entrée en vigueur, des nouvelles obligations qui pèseront sur elles et des mesures qu'elles devront prendre pour s'y conformer.

Si l'ANSSI travaille actuellement à un questionnaire en ligne *via* une plateforme qui permettra de répondre aux interrogations des entités concernées, on se rend compte que la transposition de cette directive appelle un travail d'outillage important qu'il conviendra de faire dans les meilleurs délais : guichet unique, communication, guide, etc... Ces outils devront être accessibles, clairs, compréhensibles y compris pour les entités les moins accoutumées au domaine cyber.

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

Recommandation n°1 : Organiser une véritable campagne de communication à destination des entreprises et des collectivités locales. Cette campagne d'information à large échelle pourrait également inclure le grand public.

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

LA TRANSPOSITION DE LA DIRECTIVE NIS 2

UNE OPPORTUNITE POUR COMMUNIQUER PLUS ET MIEUX SUR LES ENJEUX DE SECURITE NUMERIQUE

La directive NIS 2, marque une évolution significative en matière de cybersécurité en Europe, élargissant considérablement le nombre d'entités assujetties à ses règles de 600 à 15 000.

Cette expansion inclut non seulement les entreprises mais aussi les collectivités locales, qui, pour la plupart, ne sont pas encore pleinement informées des nouvelles obligations qui leur incomberont.

Dans ce contexte, il est crucial de mettre en place une campagne de communication impactante pour sensibiliser ces acteurs aux enjeux de la directive NIS 2.

Actuellement, une majorité des nouvelles entités concernées n'ont pas conscience des mesures à venir et des critères qu'elles devront analyser elles-mêmes pour déterminer leur conformité.

Il est nécessaire d'organiser une campagne de communication nationale pour informer les entreprises et les collectivités locales des nouvelles obligations réglementaires, des mesures de conformité et des bénéfices associés.

Il est impératif d'informer les entités sur les nouvelles exigences de la directive NIS 2. Contrairement à la directive NIS 1, où l'ANSSI désignait les entités régulées, les nouvelles entités devront auto-évaluer leur conformité. Cette auto-évaluation nécessite une compréhension claire des critères et des seuils pertinents.

La communication doit également mettre en avant les avantages de la mise en œuvre de la directive. *En améliorant leur niveau de sécurité numérique, les entreprises et les collectivités locales peuvent protéger plus efficacement les données de leurs clients et usagers, renforcer leur résilience face aux cyberattaques et, par conséquent, augmenter leur compétitivité.* ***Une communication efficace doit souligner ces points pour encourager une adhésion enthousiaste à la directive.***

La mise en place d'un label NIS 2 pour les entités conformes pourrait constituer une incitation supplémentaire*. Ce label pourrait être utilisé comme un gage de qualité et de sécurité, valorisant les efforts des entreprises et des collectivités pour se conformer aux nouvelles régulations. Une telle reconnaissance pourrait également servir de différenciateur compétitif sur le marché.*

Le cyber-mois qui est organisé en octobre chaque année, un événement européen annuel, est une occasion idéale pour sensibiliser aux bénéfices et à la nécessité de la directive NIS 2. *Profiter de cette période permet d'informer sur les nouvelles exigences réglementaires, d'expliquer les bénéfices pour la résilience des infrastructures et de promouvoir des sessions de formation et des mises à niveau de systèmes. Communiquer durant cet événement bénéficiant d'une visibilité accrue permettra de renforcer la confiance des clients et partenaires, et engager les parties prenantes dans les préparatifs nécessaires à la conformité.*

III. DES POINTS DE VIGILANCE IDENTIFIES

➢ Des délais de mise en conformité trop courts

La date d'entrée en vigueur de la directive est fixée au 17 octobre 2024. A quelques semaines de cette échéance, le projet de loi n'a toujours pas été présenté en conseil des ministres et n'a pas encore été présenté devant le Parlement.

Pourtant, dès l'entrée en vigueur de la loi, les entités concernées auront l'obligation de s'enregistrer auprès de l'autorité nationale de cybersécurité.

La directive NIS 2 ne traite pas des délais, c'est un angle mort de ce texte, cependant il est nécessaire que le législateur en tienne compte lors des débats.

Le projet d'étude d'impact produit par l'ANSSI indique que « *la réglementation NIS 2, telle que mise en œuvre en France, définira des délais de mise en conformité qui tiendront compte des efforts de compréhension, de montée en compétence et d'investissement que les exigences imposent aux assujettis. Les lignes directrices et les objectifs de haut niveau font partie des textes publiés depuis fin 2022, mais les textes précis de transposition ne seront connus du grand public qu'à la suite de la phase règlementaire*[5]*. Une mise en œuvre de contrôles susceptibles de découler sur des sanctions n'est pas envisagée avant plusieurs années.* »

Il ressort des auditions qu'un alignement sur le délai de mise en œuvre du RGPD, à savoir un délai de 3 ans, apparait comme une option à privilégier car il prendrait en compte le principe de réalité opérationnelle. La définition d'une feuille de route avec un rétroplanning pour la mise en conformité pourrait sensiblement aider les entités à relever leur niveau de cybersécurité. Il sera sans doute nécessaire d'établir des étapes intermédiaires avec des délais spécifiques, en fonction de la nature et des moyens dont disposent les différentes catégories d'entités régulées, pour la mise en place des mesures de sécurité.

Pour la feuille de route, la CSNP préconise les 3 stades progressifs suivants :

1- Formation/sensibilisation
2- Évaluation/audit
3- Contrôle/sanction

<u>Recommandation n°3 :</u> Préciser dans la loi que les délais de mise en conformité sont fixés au 31 décembre 2027. Si les décrets et textes règlementaires étaient pris avec beaucoup de retard, comme cela avait été le cas dans le cadre de la transposition de la directive NIS1, le législateur serait en mesure de voter une loi rectificative.

➢ De la nécessité d'avoir une véritable étude d'impact

Lors des auditions, la CSNP a pu constater que l'absence d'une étude d'impact complète et détaillée à l'échelle européenne, en raison de la crise sanitaire puis de la modification du projet de

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

directive, avait largement participé à soulever des inquiétudes chez les entités potentiellement assujetties à la directive NIS 2, sans y apporter de réponses.

Le législateur pâtit également de cette étude d'impact incomplète laquelle doit de se pencher tout particulièrement sur les coûts humains, techniques et financiers pour les entités ainsi que sur les délais de mise en conformité.

<u>Recommandation n°4 :</u> Compléter l'étude d'impact sur les coûts humains, techniques et financiers pour les entités ainsi que sur les délais de mise en conformité.

- **Donner au législateur les bons outils**

Compte tenu de l'importance de ce texte, notamment au regard du nombre de secteurs concernés et d'entités, et des différentes commissions qui devraient être saisies au fond sur le projet de loi (commissions des lois, de la Défense nationale, des affaires économiques, etc…), la CSNP recommande vivement la création d'une commission spéciale pour son examen.

Par ailleurs, cela interroge sur le recours à des commissions spéciales pour l'examen des textes relatifs au numérique, comme cela a été le cas en 2023 avec l'examen du projet de loi *visant à sécuriser et réguler l'espace numérique*. Le numérique est un sujet transverse et n'a pas de commission permanente dédiée.

<u>Recommandation n°5 :</u> Créer une commission spéciale pour l'examen du projet de loi *relatif à la résilience des activités d'importance vitale, à la protection des infrastructures critiques, à la cybersécurité et à la résilience opérationnelle numérique du secteur financier.*

<u>Recommandation n°6 :</u> Créer une commission permanente en charge du numérique à l'occasion de la prochaine révision du règlement de l'Assemblée nationale et de celui du Sénat.

- **Un renvoi trop systématique à la voie règlementaire**

Sur les sujets du numérique tout particulièrement, les projets de loi renvoient beaucoup à des décrets, notamment pour pallier des études d'impact parfois approximatives et laisser le temps de la consultation avec l'écosystème.

Cependant, la grande majorité des textes relatifs au sujet du numérique débattus et adoptés ces dernières années sont des adaptations et des transpositions d'actes juridiques européens, tels que le *Digital Services Act* (DSA) ou encore le *Digital Markets Act* (DMA).

Or, comme le prévoit l'article 288 du traité sur le fonctionnement de l'Union européenne (TFUE), les actes juridiques contraignants, telles que les directives, doivent être transposés dans chacun des États-membres dans un délai fixé lors de leur adoption (généralement dans les deux ans), ce qui permet une possible anticipation de leur transposition.

Si la CSNP entend qu'il est parfois nécessaire de garder une certaine souplesse et ne pas être « trop disant » en inscrivant dans le marbre de la loi des critères et définitions trop précises ou des listes trop exhaustives, le renvoi trop fréquent aux décrets nuit à la clarté et à la lisibilité du texte pour les entités concernées et ceux qui les conseillent. En effet, lors des auditions menées dans le cadre du

présent rapport, nombreuses ont été les remarques sur ces nombreux renvois. Cela d'autant plus qu'ils ont tendance à se multiplier ces derniers temps et que les délais de parutions des décrets peuvent être assez longs, mettant à mal certaines mises en application.

Par ailleurs, ces renvois peuvent mettre à mal le rôle du législateur. Dans le projet de loi *relatif à la résilience des activités d'importance vitale, à la protection des infrastructures critiques, à la cybersécurité et à la résilience opérationnelle numérique du secteur financier* sur lequel la CSNP a été saisie pour avis en mai dernier, il est demandé au législateur de débattre et de voter des articles sans connaitre précisément le périmètre des entités concernées ainsi que le type d'incidents qu'il faudra déclarer puisque ces informations, pourtant essentielles, seront précisées par décret. Dès lors, comment savoir s'il n'y aura pas d'effet de bord ?

La CSNP tient à rappeler que le rôle des parlementaires n'est pas seulement de faire la loi mais également de contrôler l'action du Gouvernement. Alors que le contenu de la directive NIS 2 est connu depuis plusieurs années ainsi que son étude d'impact européenne, demander aux entités potentiellement concernées ainsi qu'au législateur de faire confiance au Gouvernement et au Conseil d'État sur des dispositions aussi importantes interroge.

A l'issue des auditions conduites par le groupe de travail, des interrogations subsistent sur la faculté pour certaines entités de savoir précisément si elles relèveront du champ d'application de la nouvelle loi.

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

Ces interrogations sur le périmètre de la directive NIS 2 sont également partagées par certaines entreprises qui ne sont pas concernées en raison des critères de seuils mais dont l'activité relève des secteurs économiques critiques et hautement critiques.

La plateforme mise en place par l'ANSSI ne répondrait que partiellement aux préoccupations de ces entités.

La CSNP tient à souligner qu'un autre choix aurait été possible : le législateur belge, pour sa part, a choisi de confier à l'homologue belge de l'ANSSI la responsabilité de désigner les collectivités locales qui seraient soumises à la transposition de la directive NIS 2. Ce choix permet de clarifier la situation et place régulateur et régulés face à leurs responsabilités.

<u>Recommandation n°7 :</u> Limiter au maximum le renvoi à des décrets en Conseil d'État.

<u>Recommandation n°8 :</u> Réintégrer dans le projet de loi les seuils et critères précisés dans la directive NIS 2 et ses annexes.

<u>Recommandation n°9 :</u> Confier à l'ANSSI la responsabilité de désigner les collectivités locales soumises à NIS 2.

- **Des précisions attendues sur la notion de *« tout incident ayant un impact important »***

Les entités qui auront constaté un incident ayant un impact important auront l'obligation d'en informer l'ANSSI. Il ressort des auditions que l'obligation de notification *« sans retard injustifié »* à l'ANSSI de *« tout incident ayant un impact important »* (article 33 de la directive NIS 2) sur la fourniture de leurs services paraît insuffisamment précis.

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

La notion d'incident important retenue par l'ANSSI est celle de la loi n° 2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense, dite loi de Programmation Militaire, et correspond à la jurisprudence construite de manière itérative dans le cadre de la transposition de la directive NIS 1.

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

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

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

Le législateur belge a fait le choix de ne laisser libre court à aucune appréciation en inscrivant ces définitions dans la loi. Si certains acteurs auditionnés ont fait part de leur souhait de voir une définition inscrite dans la loi, d'autres ont souligné qu'il était davantage judicieux de laisser de la souplesse afin d'éviter des effets de bord, mais que des critères devaient toutefois être clairement écrits.

En effet, un « incident important » ne sera pas forcément perçu de la même manière selon les entités, ou entre un client et un fournisseur. Dans tous les cas, la CSNP recommande au législateur de ne pas inscrire une définition « incident important » dans la loi en partant de l'impact.

En tout état de cause, un guide de bonnes pratiques est souhaité et attendu par les entités interrogées.

<u>Recommandation n°10 :</u> Préciser dans le texte de loi la notion d'*« incident important »* en publiant une liste de critères objectivables par les entité essentielles et importantes.

<u>Recommandation n°11 :</u> Prévoir dans la loi des mécanismes explicites de protection des informations divulguées lors de signalement d'incidents, afin de garantir la confidentialité des données sensibles et stratégiques des entreprises qui pourraient être transmises dans le cadre d'une notification.

<u>Recommandation n°12 :</u> Prévoir dans la loi une clause d'adaptabilité aux évolutions technologiques liées notamment à l'usage de l'intelligence artificielle en matière de cybersécurité.

- **La difficulté de prouver la mise en conformité à NIS 2**

Lors des auditions, de très nombreux acteurs ont fait part de leur inquiétude quant à la manière dont ils pourraient prouver leur conformité à la directive NIS 2 à leurs clients. Comme proposé précédemment dans le présent avis, **la CSNP recommande la mise en place d'un système de labellisation.** Cette labellisation permettrait, en plus d'être incitative, d'être un gage de confiance entre les acteurs.

- **La question de la souveraineté**

Lors des auditions, menées au printemps 2024, le projet d'acte d'exécution de la Commission européenne n'était pas encore connu, aussi la CSNP n'a pu recueillir de remarques de la part des différents acteurs.

Toutefois, sur la base du projet d'acte d'exécution paru fin juin 2024, la CSNP constate que qu'il laisse entrevoir le fait que le champ d'action de l'ANSSI va désormais être élargi au contrôle du niveau de disponibilité et de qualité de service des fournisseurs de services numériques, et non plus seulement des incidents de cybersécurité. Cela fait craindre une multiplication d'incidents considérés comme « significatifs » et augmentera le nombre de notifications des différents acteurs auprès de l'ANSSI.

IV. UN IMPERATIF : PAS DE SURTRANSPOSITION QUI PORTERAIT ATTEINTE A UN CADRE EUROPEEN HARMONISE

Les membres de la CSNP sont très attentifs à ce que la transposition de la directive NIS 2 en France ne soit pas assortie de dispositions supplémentaires qui entraineraient une surtransposition susceptible de compromettre l'harmonisation des normes de cybersécurité à travers l'Union européenne.

Une surtransposition, en imposant des exigences supplémentaires et potentiellement plus strictes que celles prévues par la directive, créerait des divergences réglementaires entre les États membres. Cette situation placerait les entreprises françaises opérant à l'échelle européenne dans une situation défavorable. Les entreprises françaises seraient en effet confrontées à des exigences de conformité différentes et parfois contradictoires, générant des coûts administratifs et opérationnels et affectant *de facto* leur compétitivité face à des concurrents soumis à des régulations moins strictes.

Cette situation favoriserait l'apparition de "pavillons de complaisance" et pourrait conduire certaines entreprises à s'implanter dans des pays avec des exigences moins contraignantes pour réduire leurs coûts de mise en conformité, comme cela a été observé avec l'application du RGPD.

Il est donc essentiel que la directive NIS 2 ne fasse pas l'objet de surtransposition tant au niveau de la loi de transposition que de ses décrets d'application.

Il est également important que les options retenues pour transposer la directive NIS 2 soient proportionnées eu égards aux objectifs fixés par la directive NIS 2.

Dans cette perspective, les entités auditionnées par la CSNP recommandent d'impliquer davantage les collectivités territoriales et les acteurs du secteur privé dans le processus de transposition afin de s'assurer que les nouvelles exigences seront proportionnées et réalistes.

La CSNP salue le travail de consultation des parties prenantes mené par l'ANSSI à partir de l'automne 2023. Toutefois, la restitution de ces consultations organisée en avril 2024 n'a pas complètement dissipé les questionnements ou les craintes de l'ensemble de ces acteurs. Une approche collaborative est indispensable pour maintenir la compétitivité des entreprises françaises tout en garantissant un cadre de cybersécurité cohérent et efficace à l'échelle européenne.

Les membres de la CSNP considèrent que la loi de transposition de la directive NIS 2, en renvoyant certaines mesures de transposition au pouvoir réglementaire, ne permet pas au législateur de vérifier si *in fine* la directive NIS 2 ne sera pas surtransposée.

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

V. UN ACCOMPAGNEMENT NECESSAIRE DES NOUVELLES ENTITES

L'élargissement considérable du périmètre des entités qui seront soumises aux dispositions de la directive NIS 2 suppose un accompagnement approprié des entités potentiellement concernées.

En effet, jusqu'à présent les 600 entités couvertes par la directive NIS 1 disposaient de structures, d'équipes et de moyens dédiés nécessaires pour se conformer aux dispositions de la directive NIS 1.

Le profil des entités qui seront soumises aux dispositions de la directive NIS 2 sera sensiblement différent : certaines entités disposeront de moyens comparables tandis que d'autres seront bien moins préparées et dotées en ressources humaines, techniques et financières.

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

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

En effet, certains territoires ne disposent tout simplement pas des ressources humaines ou des prestataires compétents en matière de cybersécurité pour accompagner les nouvelles entités essentielles ou importantes au sens de la directive NIS 2.

Il apparaît donc essentiel de prévoir un accompagnement de ces entités. Pour les membres de la CSNP, cet accompagnement passe par un renforcement de la présence de l'ANSSI en région, par la clarification du rôle des CSIRT régionaux dont plusieurs acteurs ont fait part des limites de leur efficacité quant à l'accompagnement des entités dans les territoires, et par la montée en puissance

du dispositif *cybermalveillance.gouv.fr*, mais aussi par la mise en place de procédures simplifiées et de guide de bonnes pratiques.

La CSNP attend un certain nombre de clarifications sur les moyens et l'organisation que mettra en œuvre l'ANSSI pour répondre à la charge supplémentaire significative à laquelle l'organisation va devoir faire face dès lors que la directive NIS 2 entrera en vigueur.

Enfin, la CSNP demande que les acteurs, relais opérationnels du terrain, soient rapidement et de manière transparente identifiés par l'ANSSI. Le réflexe de faire systématiquement appel au secteur privé ne doit en aucun cas être la règle unique dans les territoires.

- **Faciliter la déclaration des incidents**

Lors des auditions, de nombreux acteurs ont fait part de leurs inquiétudes quant à la surcharge administrative que pourrait représenter la déclaration d'un incident cyber. En effet, la majorité des entités qui seront concernées par NIS 2 doivent déjà déclarer un certain nombre d'incidents auprès de plusieurs acteurs tels que la CNIL. Aussi, la CSNP formule deux recommandations afin de simplifier ces démarches, dans un souci d'efficacité et de gain de temps.

<u>Recommandation n°14 :</u> Mettre en place un guichet unique pour déclarer les incidents en élargissant les fonctionnalités de la plateforme 17Cyber.

<u>Recommandation n°15 :</u> Uniformiser les formulaires de remontées d'incidents.

- **Maitriser les effets de bord et alerter sur les effets d'aubaine**

Il est nécessaire que le législateur prenne des dispositions afin d'alerter les entités nouvellement régulées par la directive NIS 2 et qui auraient un faible niveau de maturité et de connaissance en termes de cybersécurité sur les effets d'aubaine pour certains organismes, tels que les cabinets de conseil et assureurs car comme pour chaque nouvelle régulation des marchés peuvent s'ouvrir pour certains acteurs et des offres commerciales abusives et trompeuses peuvent émerger.

- **Accompagnement par l'ANSSI**

Passant de 600 entités concernées par la directive NIS 1 à 15 000 entités environ concernées par la directive NIS 2, l'ANSSI sollicite la création de 60 emplois temps plein.

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

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

<u>Recommandation n°16 :</u> Renforcer la présence de l'ANSSI en région.

- **La certification des prestataires privés**

La CSNP souhaite que l'ensemble des prestataires privés qui peuvent intervenir auprès d'une entité soumise à la directive NIS 2 fassent l'objet d'une certification par l'ANSSI selon les qualifications existantes : PACS, PASSI, PRIS, PDIS, PAMS[6]. La CSNP souhaite rappeler que, dans le respect naturellement des règles de concurrence, il est important de faire appel aux différentes entités existantes (tels que le GIP ACYMA cybermalveillance.gouv.fr, les gendarmes pour les actions de sensibilisation, les DSI, les chambres consulaires, etc…) et non uniquement aux seules entreprises privées.

<u>Recommandation n°17 :</u> Certifier par l'ANSSI les prestataires privés susceptibles d'intervenir auprès d'une entité soumise à la directive NIS 2.

- **Clarification du rôle joué par les CSIRT territoriaux**

Les Computer Security Incident Response Team (CSIRT) territoriaux pourraient être une réponse partielle à la présence régionale pour accompagner les entités concernées par la directive NIS 2, notamment celles de petites tailles dans la déclaration et la résolution d'incidents.

Issus d'un projet du plan France Relance en 2021, les CSIRT territoriaux (Computer Security Incident Response Team) sont des centres de réponse aux incidents cyber au plus près des entités implantées sur leurs territoires. Ils traitent les demandes d'assistance des acteurs de taille intermédiaire (ex : PME, ETI, collectivités territoriales et associations) et les mettent en relation avec des partenaires de proximité : prestataires de réponse à incident et partenaires étatiques.

Selon l'ANSSI, l'émergence de ces CSIRT doit permettre de fournir localement un service de réponse à incident de premier niveau gratuit, complémentaire de celui proposé par les prestataires, la plateforme Cybermalveillance.gouv.fr et les services du CERT-FR.

Ces équipes portent également des missions de prévention, sensibilisation et d'accompagnement dans la montée en maturité des acteurs de leurs territoires.

Le dispositif est à ce jour constitué de 13 CSIRT territoriaux, en métropole comme dans les Outre-mer. Toutefois, ce dispositif couvre encore inégalement notre territoire puis que la région Auvergne-Rhône-Alpes et la Corse ne disposent pas de CSIRT. De même, un seul CSIRT (CSIRT-ATLANTIC) couvre l'ensemble des territoires ultramarins.

Si lors des auditions, il en ressort que les CSIRT territoriaux ne seraient pas adaptés pour la remontée des incidents cyber, ils pourraient avoir un rôle à jouer dans la réponse aux incidents.

Aussi, pour les membres de la CSNP, il paraît important de préciser le positionnement des CSIRT régionaux et sectoriels dans le dispositif d'accompagnement du projet de loi. Les membres de la

[6] https://cyber.gouv.fr/referentiels-dexigences-pour-la-qualification

CSNP ne souhaitent pas une surtransposition de la directive NIS 2 mais considèrent que l'adoption de la loi pourrait être l'occasion de clarifier le rôle des CSIRT régionaux dans le dispositif français de la cybersécurité. Le financement national des CSIRT régionaux prendra fin en 2024, les régions prenant le relai : la question de la consolidation et de la pérennité des écosystèmes cyber régionaux se pose donc de manière urgente.

Recommandation n°18 : Clarifier le rôle des CSIRT territoriaux dans la transposition de NIS 2.

Recommandation n°19 : Créer une mission d'information parlementaire sur le rôle, le fonctionnement et le financement des CSIRT régionaux et sectoriels.

- **Montée en puissance du dispositif cybermalveillance.gouv.fr**

Le dispositif *cybermalveillance.gouv.fr* mis en place en 2017 avec le GIP ACYMA semble recueillir la confiance des usagers, des collectivités locales et des entreprises d'après nos auditions. Comme le préconise le rapport de la Cour des comptes de mars 2022, une montée en puissance et un renforcement des moyens du dispositif, à budget constant depuis des années alors que ses missions se renforcent et les sollicitations se multiplient, serait de nature à combler la « diagonale du vide » dont souffrent certains territoires.

Recommandation n°20 : Allouer des crédits supplémentaires au SGDSN dans le cadre du programme 129 lors du PLF pour 2025, crédits qui seront fléchés vers le GIP ACYMA.

Recommandation n°21 : Accompagner financièrement les entités ne disposant pas des moyens nécessaires à leur mise en conformité.

- **Nécessité d'un accompagnement spécifique des collectivités locales**

Les collectivités territoriales rencontrent des difficultés spécifiques dans la mise en œuvre de la directive NIS 2. Les petites communes, en particulier, sont moins préparées et ne disposent pas des ressources nécessaires pour se conformer aux exigences imposées aux entités essentielles.

Les associations d'élus ont été sensibilisées aux problèmes de cybersécurité par l'ANSSI, mais un écart significatif persiste entre les petites et grandes collectivités. La CSNP constate qu'un travail de pédagogie et de sensibilisation sera nécessaire vis-à-vis des collectivités dont la très large majorité se sent encore très éloignée des enjeux cyber alors qu'elles sont souvent la cible privilégiée de cyberattaques.

Les collectivités, et notamment les communautés de communes, s'inquiètent également de la mise en jeu de leurs responsabilités en cas de non-conformité des systèmes d'information des petites communes ou de leurs prestataires externes. En effet, il y a une incertitude sur la responsabilité en cas de non-conformité des prestataires aux exigences de la directive NIS 2. Elles demandent des clarifications sur les rôles et les responsabilités, et une meilleure collaboration avec les structures régionales.

La question des ressources humaines et financières est évidemment cruciale pour les collectivités. Les collectivités font face à une concurrence du secteur privé pour le recrutement de

talents en cybersécurité, compliquée par les grilles salariales de la fonction publique. La CSNP recommande de mettre l'accent sur les formations, y compris interne, et sur la reconversion.

S'agissant des formations en cybersécurité, un référentiel de formations en cybersécurité pour les entités publiques mais également privées pourrait être intégré au Répertoire national des compétences professionnelles. Ce référentiel des compétences minimales en matière de sécurité numérique pourrait être facilement constitué par l'ANSSI.

De manière générale, un débat sur le budget dotation pour les collectivités devra être engagé au Parlement puisque ces dernières ne cessent de voir leurs dotations baisser alors que la mise en œuvre de cette directive sera, à n'en point douter, très couteuse.

Par ailleurs, il nous faudra soutenir les actions des collectivités à inclure des clauses cyber face à des centrales d'achats pas toujours adaptées aux collectivités et face aux critères d'appels d'offres. La question des contrats en cours qui ne respecteraient pas les conformités cyber imposées par la directive NIS 2 se pose.

Les centrales d'achat comme l'UGAP peuvent jouer un rôle de levier important dans le relèvement du niveau de sécurité numérique des collectivités locales.

Évoquer le niveau de maturité cyber des collectivités à travers les choix effectués auprès des éditeurs de logiciels peut s'avérer une approche intéressante. En effet, la vulnérabilité de certaines collectivités peut varier selon qu'elles ont choisi une solution dite SaaS (« *Software as a Service* ») ou *on-premise* pour leurs logiciels. De nombreuses collectivités choisissent d'avoir leurs logiciels *on-premise,* à savoir hébergées et maintenus par le propre service informatique de la collectivité. Or, force est de constater que faute de temps ou de ressources humaines nécessaires, les mises à jour peuvent être effectuées dans un certain délai, voire pas du tout, exposant ainsi ces collectivités aux risques cyber. Le choix du mode dit SaaS présente à cet égard plusieurs avantages dont celui d'être hébergé dans le cloud et exploité en dehors de la collectivité par le fournisseur de service, permettant ainsi de conserver un meilleur niveau de cybersécurité même si l'actualité récente a démontré que cette solution ne présentait pas un niveau de sécurité absolu.

Reprenant l'esprit d'une recommandation de l'avis n°2023-06 du 12 septembre 2023 de la CSNP sur la souveraineté numérique, la CSNP pose à nouveau le rôle que les préfets pourraient jouer dans la mise en conformité à NIS 2 des collectivités.

<u>Recommandation n°22 :</u> Faire auditer par l'ANSSI le degré de maturité des collectivités locales qui seront soumises à la directive NIS 2 et en mesure de se conformer au calendrier de mise en œuvre. Un accompagnement spécifique, technique et financier sera prévu pour celles n'ayant pas les moyens nécessaires. La mobilisation des financements de la stratégie nationale d'accélération cyber vers des outils intégrés conformes aux exigences posées par l'ANSSI doit être étudiée.

<u>Recommandation n°23 :</u> Introduire plus de progressivité dans la mise en œuvre de la directive NIS 2 et réaliser une étude d'impact plus précise pour qualifier les risques, les menaces et les coûts financiers, administratifs, démocratiques des cyberattaques pesant sur les collectivités territoriales. Les membres de la CSNP appuient les demandes des collectivités territoriales exprimées en ce sens.

<u>Recommandation n°24 :</u> Inciter les collectivités, notamment celles qui n'ont pas les moyens humains nécessaires, à faire le choix d'une solution dite SaaS afin de maintenir le meilleur niveau de cybersécurité possible.

<u>Recommandation n°25 :</u> Renforcer le rôle des préfets dans l'accompagnement des collectivités à se conformer aux obligations de la directive NIS 2.

VI. DES ENJEUX SPECIFIQUES POUR CERTAINS SECTEURS ECONOMIQUES

Au cours des auditions qui ont été conduites, les membres de la CSNP ont pu observer des attentes particulières de certains acteurs économiques à l'égard de la transposition de la directive NIS 2.

- **Le secteur de la santé**

La mise en œuvre de la directive NIS 2 dans le secteur de la santé présente plusieurs enjeux majeurs. Tout d'abord, elle intervient après la transposition de la directive NIS 1, du RGPD et des modifications du code de santé publique. Les professionnels de santé appréhendent la création d'une couche de complexité supplémentaire aux exigences déjà multiples qui leur sont imposées. Le changement d'échelle de la directive NIS 2 passe notamment par le fait que tous les services d'information du secteur de la santé seront désormais concernés, nécessitant la mise en œuvre de moyens considérables.

Les établissements de santé ont des systèmes d'information autonomes et diversifiés : ils auront donc à harmoniser leurs pratiques. Ceci représente un défi d'autant plus grand que tous les établissements de santé ne disposent pas des ressources financières et humaines suffisantes.

La directive NIS 2 constitue sans nul doute un levier puissant pour encourager la mutualisation et renforcer la sécurisation de l'ensemble de la chaîne de valeur, des fournisseurs de médicaments aux systèmes internes.

S'agissant des délais de transposition, il apparait crucial d'aménager des délais de mise en conformité et de prévoir des dispositifs d'accompagnement, en particulier pour les petits établissements dépourvus de RSSI ou de DSI, afin de garantir une adoption efficace et pérenne de la directive NIS 2.

Les entreprises de dispositifs médicaux réunies au sein du SNITEM ont attiré l'attention de la CSNP sur la qualification d'entités essentielles de certaines entreprises de dispositifs médicaux en cas de crise sanitaire. En cas de crise sanitaire, il sera difficilement envisageable de passer, pour ces entreprises, du statut d'entité importante à celui d'entité essentielle et de relever immédiatement le niveau supplémentaire attendu pour une entité essentielle.

<u>Recommandation n°26 :</u> Prévoir un accompagnement financier des acteurs les plus fragiles afin que la mise en œuvre de la directive NIS 2 constitue un levier puissant pour encourager la mutualisation et renforcer la sécurisation des systèmes d'information des acteurs de la santé.

<u>Recommandation n°27 :</u> Renforcer la concertation entre l'ANSSI, le ministère de la Santé et les entités du secteur de la santé potentiellement concernées par un relèvement de leur statut d'entité importante à entité essentielle en cas de crise sanitaire sur les mesures adaptées et proportionnées à mettre en place.

- **Le secteur des assurances**

France Assureurs a souhaité attirer l'attention des membres de la CSNP sur l'articulation de la directive NIS 2 avec le règlement Digital Operational Resilience Act (DORA).

Le règlement DORA entrera en vigueur en janvier 2025 et a vocation à constituer le cadre légal en matière de cyberrésilience applicable au secteur financier dont fait partie le secteur de l'assurance. Ce règlement prévoit un cadre de gestion des risques cyber et la notification des incidents majeurs à l'ACPR, ainsi que la réalisation de programmes de tests de résilience.

France Assureurs craint que les assureurs ne soient à la fois soumis à la directive NIS 2 et au règlement DORA ce qui engendrerait une insécurité juridique alors qu'il est admis au niveau européen que DORA a un effet au moins équivalent à la directive NIS 2. Si certaines dispositions de la directive NIS 2 devaient s'appliquer aux assureurs, cela entrainerait *de facto* des coûts pour les assureurs français par rapport à leurs concurrents européens et les soumettraient à une double supervision : celle de l'ANSSI et de l'ACPR.

Recommandation n°28 : Préciser le régime applicable au secteur des assurances en application de la *lex specialis* pour lever les risques de double régulation entre la directive NIS 2 et le règlement DORA.

- **Le cas des sous-traitants et des éditeurs de logiciels**

Le projet de loi transposant la directive NIS 2 impose la protection des réseaux et systèmes d'information, y compris en cas de recours à la sous-traitance.

Cette extension aux sous-traitants interroge et inquiète. En effet, de nombreux représentants des entités essentielles ou importantes considèrent qu'ils ne disposent d'une vision ni partielle ni complète de leurs fournisseurs et sous-traitants.

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

Les éditeurs de logiciels font face, quant à eux, à des défis particuliers, notamment en ce qui concerne la mise en œuvre des audits de conformité. La nécessité de réaliser ces audits par des sous-traitants représente une charge considérable pour les grandes entreprises et encore plus pour les petites entreprises qui pourraient être totalement dépassées par les coûts et les ressources nécessaires. Il leur parait essentiel de clarifier les rôles et les devoirs des éditeurs envers les entités qu'ils assistent, notamment les collectivités locales, et de distinguer les exigences selon les types de données protégées.

Recommandation n°29 : Intégrer dans le texte de transposition de la directive NIS 2 la nécessité pour les entités essentielles et importantes de modifier les obligations contractuelles qui les lient à leurs sous-traitants.

- **Le cas des noms de domaines**

Les noms de domaines (DNS) étaient déjà concernés par la directive NIS1, mais pas les bureaux d'enregistrement. Ces derniers sont toutefois désormais concernés par la directive NIS 2. Des clarifications sur le périmètre de l'article 28 de la directive semblent nécessaires afin de ne pas créer de ruptures d'égalité entre les bureaux d'enregistrement européens et extra européens.

Recommandation n°30 : Préciser dans la loi le périmètre de l'article 28 de la directive NIS 2 relatif à la base des données d'enregistrement des noms de domaine.

VII. UN DISPOSITIF DE SANCTIONS INEDIT

De manière inédite, la directive NIS 2 prévoit l'instauration de diverses sanctions administratives en cas de non-respect des dispositions qu'elle introduit. Ces sanctions prennent, selon les cas, la forme d'amendes administratives, d'astreintes, de suspensions de certaines activités ou d'interdictions temporaires d'exercice des responsabilités du dirigeant de l'entité concernée, de l'abrogation d'une certification, d'une qualification ou d'une autorisation.

La CSNP salue le choix retenu, parmi les trois options possibles pour l'établissement d'une autorité de sanctions évoquées lors de l'élaboration du projet de loi, de créer un collège *ad hoc* et indépendant. Composée de magistrats du Conseil d'État, de la Cour de cassation et de la Cour des comptes, ainsi que de personnalités qualifiées, cette instance est de nature à rassurer les professionnels du droit et les parties prenantes sur l'indépendance de cette commission vis-à-vis de l'ANSSI qui exerce les fonctions de conseil et de superviseur.

Le projet de loi précise les modalités de la supervision et de la constatation des manquements et confie à ladite commission des sanctions la faculté de décider dans chaque cas d'un montant individualisé, proportionné à la gravité des faits dans la limite du niveau maximum à savoir 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial hors taxes ou 7 millions d'euros ou 1,4 % du chiffre d'affaires annuel mondial hors taxes en fonction des entités concernées.

La création de cette commission indépendante permettra également de ne pas dénaturer le rôle de l'ANSSI qui est avant tout d'accompagner les entités françaises, répondant ainsi à de nombreuses inquiétudes soulevées par de nombreuses entités auditionnées.

Par ailleurs, ce dispositif permettra de pérenniser la confiance des entités en l'ANSSI. Si cette dernière devait se doter du pouvoir de sanction, il aurait été à craindre que certaines entités puissent être frileuses à l'idée de faire part à l'ANSSI de certaines failles de cybersécurité.

La CSNP tient cependant à appeler l'attention de la future commission des sanctions sur deux aspects :

- Premièrement, bien qu'il ne faille pas négliger l'effet dissuasif du risque de sanction, incitant fortement les entités concernées par la directive à s'y conformer, la CSNP abonde dans le sens de l'ANSSI qui ne souhaite pas voir les collectivités être soumises à des sanctions en cas de non-conformité. Comme évoqué précédemment, l'accompagnement des collectivités dans la mise en conformité sera un véritable enjeu de l'application de cette directive.

- Enfin, la CSNP recommande, compte tenu des délais de mise en conformité pour l'ensemble des entités concernées, une certaine souplesse dans l'appréciation des infractions aux obligations jusqu'au 31 décembre 2027.

<u>Recommandation n°31</u> *<u>(en cas d'évolution du projet de loi)</u>* : Faire le choix de déléguer à une commission *ad hoc* et indépendante le pouvoir de sanctions en cas de non-respect des obligations introduites par la directive.

<u>Recommandation n°32</u> : Accorder une certaine souplesse dans l'appréciation des infractions aux obligations et les sanctions relatives jusqu'au 31 décembre 2027.

LISTE DES PERSONNES AUDITIONNÉES

(par ordre alphabétique)

ADF (Assemblée des départements de France)

- M. Jean-Baptiste ESTACHY, conseiller sécurité

ADN Ouest

- M. Franz JARRY, délégué général

AFNIC (Association française pour le nommage Internet en coopération)

- M. Pierre BONIS, directeur général
- M. Régis MASSÉ, directeur des systèmes d'information et directeur technique

AFNUM (Alliance française des industries du numérique)

- Mme Stella MORABITO, déléguée générale
- M. Léo LAFARGE, chargé de mission politiques numériques

AMF (Association des Maires de France)

- M. Patrick MOLINOZ, co-président de la commission du numérique
- Mme Véronique PICARD, chargée de mission numérique

ANSSI (Agence nationale de la sécurité des systèmes d'information)

- M. Vincent STRUBEL, directeur général
- Mme Jennyfer CHRÉTIEN, directrice de cabinet

APSSIS (Association pour la sécurité des systèmes d'information de santé)

- M. Vincent TRELY, président fondateur

ARPEGE

- M. Grégoire BINET, directeur des systèmes d'information
- Mme Julie LE TRAON, déléguée à la protection des données, responsable équipe contrats et marchés publics
- M. Nathanaël VERON, responsable de la sécurité des systèmes d'information

AVICCA (Association des villes et collectivités pour les communications électroniques et l'audiovisuel)

- M. Ariel TURPIN, délégué général
- M. Guilhem DENIZOT, chargé de mission juridique et réglementaire

AWS

- M. Stephan HADINGER, directeur de la technologie chez AWS France
- M. Arnaud DAVID, directeur des Affaires publiques

BERGER LEVRAULT

- M. Jérôme BONNET, directeur de la technologie, membre du comité exécutif
- M. Alain DUWEZ, responsable de la sécurité des systèmes d'information
- Mme Valérie REINER, directrice des Affaires publiques

Centre pour la Cybersécurité Belgique :

- M. Dirk DE PAEPE, CCB Certification Service, Centre for Cybersecurity Belgium
- M. Stephan ANDRE, service juridique du CCB
- M. Nathanaël ACKERMAN, Head of AI4Belgium - Digital Minds Unit
- M. Taco MULDER, directeur général BOSA

CDSE (Club des directeurs de sécurité des entreprises)

- M. Émile PEREZ, vice-président, directeur de la sécurité et de l'intelligence économique du groupe EDF
- M. Florent JANSSEN, chargé de mission

Cigref (Club informatique des grandes entreprises françaises)

- M. Jean-Claude LAROCHE, président, directeur de mission auprès du Président d'ENEDIS
- M. Henri d'AGRAIN, délégué général

CLOUD TEMPLE

- M. Nicolas ABRIOUX, responsable Gouvernance de la Sécurité
- Mme Laure MARTIN-TERVONEN, directrice des Affaires publiques

Club des RSSI de Santé

- M. Jean-Sylvain CHAVANNE, secrétaire général

CPME (Confédération des petites et moyennes entreprises)

- M. Marc BOTHOREL, référent cybersécurité
- M. Jérôme NORMAND, économiste
- M. Adrien DUFOUR, responsable des Affaires publiques

Cybercercle

- M. Philippe LOUDENOT, senior advisor & cybersecurity strategist, délégué à la protection des données
- M. Christian DAVIOT, senior advisor

DOCAPOSTE

- M. Guillaume POUPARD, directeur général adjoint
- Mme Fanny LANNOY, responsable des Affaires publiques

EGERIE

- M. Jean LARROUMETS, président fondateur
- Mme Marie AUDREN, directrice des Affaires publiques

EY

- M. Marc AYADI, associé chargé des expertises cyber, technologiques et data pour la France
- M. Fabrice NAFTALSKI, avocat associé chargé du droit du numérique, de protection des données personnelles et de la propriété

FFTélécoms (Fédération française des télécoms)

- M. Patrick GUYONNEAU, président de la commission sécurité de la FFT et Directeur de la sécurité du groupe Orange
- M. Alexandre GALDIN, directeur délégué à la sécurité

FIEEC (Fédération des industries électriques, électroniques et de communication)

- Mme Aridge KHAYATI, chargée d'Affaires publiques

FNCCR (Fédération nationale des collectivités concédantes et régies)

- M. Jean-Luc SALLABERRY, chef du département numérique

France Assureurs

- Mme Mélodie LELOUP-VELAY, directrice Droit et Conformité
- Mme Olympia FEKETE, responsable d'études juridiques
- Mme Viviana MITRACHE, directrice des Affaires publiques France
- M. Arnaud GIROS, responsable Affaires parlementaires et gouvernementales
- Mme Anne-Marie PAPEIX, responsable RC Médicale, RC et Environnement

GOOGLE cloud

- M. Thiébaut MEYER, directeur des stratégies de cybersécurité
- M. Frédéric GIRAUD de LESCAZES, directeur des Affaires publiques

HEXATRUST

- M. Jean-Noël de GALZIN, président fondateur, président fondateur de Wallix
- Mme Dorothée DECROP, déléguée générale
- M. Armand NOURY, directeur conseil influence d'Agence Proches

HUAWEI

- M. Minggang ZHANG, directeur général adjoint de Huawei France
- Mme Myriam LAGARDE, directrice des Affaires institutionnelles de Huawei France

Intercommunalités de France

- Mme Marlène LE DIEU DE VILLE, vice-Présidente de la commission numérique
- M. Clément BAYLAC, conseiller économie et attractivité, numérique et commerce

Iteanu Associés

- Maître Alexandra ITEANU, avocate, responsable du pôle data et RGDP au cabinet Iteanu

MEDEF (Mouvement des entreprises de France)

- Mme Maxence DEMERLÉ, directrice du numérique
- M. Alexis KASBARIAN, responsable du pôle transition numérique et innovation
- Mme Mathilde BRIARD, chargée de mission économie numérique

MICROSOFT

- M. Lionel BENATIA, directeur senior des Affaires gouvernementales
- M. Marc GARDETTE, directeur technique adjoint

NUMEUM

- Mme Nolwenn LE STER, présidente de la commission cybersécurité, directrice des activités cybersécurité chez Capgémini
- M. Paul PASTOR, délégué aux Affaires publiques et cybersécurité
- M. Clément EMINE, délégué aux Affaires publiques

ONE POINT

- M. Alexis BOUIN, expert cybersécurité
- M. Vincent CHRIQUI, conseiller du président

OUTSCALE 3DS

- M. Grégory ABATE, secrétaire général de Dassault Systèmes
- M. David CHASSAN, directeur de la Stratégie

OVHCloud

- M. Julien LEVRARD, responsable de la sécurité informatique
- Mme Blandine EGGRICKX, responsable des Affaires publiques

Régions de France

- Mme Sinaa THABET, conseillère développement économique, recherche, innovation et numérique

Renaissance Numérique

- Mme Rayna STAMBOLIYSKA, présidente, RS Strategy
- M. Samuel LE GOFF, vice-président, consultant chez Commstrat

SCALEWAY

- Mme Ombeline BARTIN, directrice des Affaires publiques d'Iliad
- Mme Naphsica PAPANICOLAOU, chargée d'Affaires publiques d'Iliad

Service économique de Bruxelles

- M. Arnaud BELLANGER, chef du service
- M. Andri RABEHANTA, adjoint au chef du Service économique

WAVESTONE

- M. Pascal IMBERT, président directeur général et co-fondateur
- M. Gérôme BILLOIS, associé cybersécurité et confiance du numérique, chargé de la gestion des risques numériques, des situations de crises et d'innovation cyber

Contributions écrites

(par ordre alphabétique)

ACN (Alliance pour la confiance numérique)

CESIN (Club des experts de la sécurité de l'information et du numérique)

SNITEM (Syndicat national de l'industrie des technologies médicales)

Renaissance Numérique

BIOGRAPHIES

M. Damien MICHALLET

Elu Sénateur (Les Républicains) de l'Isère en septembre 2023, **M. Damien Michallet** est engagé depuis plusieurs années dans la stratégie et l'aménagement numérique de nos territoires au service de nos concitoyens et de nos entreprises, pendant 8 ans à la Communauté d'Agglomération de Porte de l'Isère en tant que Vice-Président en charge de la stratégie du numérique, et en tant que Vice-président du Département de l'Isère délégué à l'aménagement numérique et aux systèmes d'information. Membre de l'AVICCA, M. Damien Michallet, a rejoint le Groupe d'Etudes "Numérique" du Sénat présidé par M. Patrick Chaize, Sénateur de l'Ain et dont il a été élu Vice-président le 30 janvier dernier.

Mme Anne LE HENANFF

Mme Anne Le Hénanff, députée au Parlement français, a été élue pour la première fois députée en Juin 2022 et appartient au parti Horizons. Elle est membre de la Commission supérieure du numérique et des postes depuis 2022. Elle siège à la Commission de la défense et des forces armées à l'Assemblée nationale. Elle était également vice-présidente du groupe de travail sur l'économie numérique, la sécurité et la souveraineté. Elue à Vannes depuis 2008, elle a été première adjointe au maire en charge du Numérique et conseillère communautaire en charge du numérique à Golfe du Morbihan Vannes agglomération. Elle est l'auteure en 2023 d'un rapport sur les défis de la cyberdéfense et a été rapporteur sur le titre relatif au Cloud pour la loi Sécuriser et réguler l'espace numérique à l'Assemblée nationale.

CSNP
COMMISSION SUPÉRIEURE DU NUMÉRIQUE ET DES POSTES

100, rue Richelieu
75002 PARIS
Tel : 06.84.40.91.95.
contact@csnp.fr

@CSNUMPOST CSNP https://csnp.fr