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

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

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

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

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

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

***

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

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

Le présent avis formule 14 recommandations :

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

I. Eléments de contexte

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Source : ANSSI

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

Article 6 du projet de loi

I. – Sont des entités essentielles :

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

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

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

4° Les prestataires de service de confiance qualifiés ;

5° Les offices d'enregistrement ;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

A. Les nouvelles obligations introduites par la directive NIS 2

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

A ce stade, ces obligations portent :

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

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

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

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

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

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

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

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

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

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

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

C. Extension du périmètre aux sous-traitants

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

A. Accompagnement par l'ANSSI

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

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

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

B. Clarification du rôle jouée par les CSIRT régionaux

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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