SÉNAT

COMMISSION SPECIALE
PROJET DE LOI
RELATIF A LA
CYBERSECURITE ET A LA
RESILIENCE

PETIT-DEJEUNER DU HAUT COMITE FRANÇAIS POUR LA RESILIENCE NATIONALE SUR LE THEME DE « LA SECURITE DES ACTIVITES D'IMPORTANCE VITALE A LA RESILIENCE DES ENTITES CRITIQUES, QUEL EQUILIBRE ENTRE LE BESOIN DE SECURITE NATIONALE ET L'ACCEPTATION DES NORMES PAR LES ACTEURS ? »

MARDI 18 MARS 2025 A 8 HEURES 30
(RESTAURANT DU SENAT – SALON POURPRE)

INTERVENTION OLIVIER CADIC

Mesdames, Messieurs,

Je tiens tout d'abord à remercier MM. Pierre Lellouche, Président, et Christian Sommade, Délégué général, du Haut comité français pour la résilience nationale de m'associer régulièrement à vos travaux. L'an dernier, j'avais pu m'exprimer à votre invitation dans les locaux de la Direction générale de la Gendarmerie nationale sur les questions de cybersécurité, de souveraineté du cloud et des ingérences numériques étrangères dont je suis depuis 8 ans le rapporteur budgétaire pour avis de la commission des affaires étrangères et de la défense du Sénat. Nous avions alors regretté l'absence d'un représentant du Secrétariat général de la défense et de la sécurité nationale !

Quoiqu'il en soit, je suis encore plus touché que cet événement annuel se déroule aujourd'hui au Sénat et que vous m'ayez proposé d'ouvrir le débat.

Le thème sur lequel vous avez sollicité mon intervention est le suivant : « **la sécurité des activités d'importance vitale à la résilience des entités critiques, quel équilibre entre le besoin de sécurité nationale et l'acceptation des normes par les acteurs ?** ».

Ce sujet est d'actualité car je préside la commission spéciale sénatoriale sur le projet de loi relatif à la résilience des entité critiques et au renforcement de la cybersécurité. Ce projet de loi a été adopté par le Sénat la semaine dernière avec exactement 100 amendements adoptés donc 61 amendements adoptés en commission et 39 amendements en séance publique.

Ce projet de loi prévoit la transposition de 3 directives différentes a fait l'objet d'un :

- la directive sur la résilience des entités critiques, dite « REC » ;

- la directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, dite « NIS2 » ;

- et la directive qui concerne la résilience opérationnelle numérique du secteur financier, dite « DORA ».

Je reviendrai plus en détail sur leur contenu car il entre tout à fait dans le thème de votre question relative à l'acceptation de nouvelles normes, contraignantes et coûteuses, dont le gouvernement n'est pas en mesure d'en présenter précisément l'impact pour les entreprises et les collectivités territoriales.

Cela me permet donc d'aborder très concrètement la question de l'équilibre entre le besoin de sécurité nationale et l'acceptation des normes par les acteurs. Ce sujet a été une préoccupation constante des travaux de la commission spéciale.

Le besoin de cybersécurité est indiscutable. J'en donne tous les ans les chiffres dans mon rapport sur le financement du programme 129 relatif au SGDSN, à l'ANSSI et à Viginum notamment. Quelques exemples :

- L'ANSSI publie chaque année un panorama de la cybermenace. En 2023, 3 703 événements de sécurité, contre 3 018 en 2022, ont été portés à la connaissance de l'Agence dont 1 112 incidents traités contre 832 en 2022 ;
- Les attaques par rançongiciels portées à la connaissance de l'agence ont connu une progression de 30 % passant de 109 en 2022 à 143 en 2023, ces nombres non exhaustifs se limitent aux cas nécessitant une analyse de l'agence mais traduisent une tendance générale qui n'épargne aucun secteur d'activité avec par ordre de ciblage les TPE/PME/ETI (34 %), les collectivités territoriales (24 %), les établissements de santé (10 %) et les entreprises stratégiques (10 %) ;
- Dans le secteur de la santé, 30 établissements ont été affectés par des compromissions et chiffrements causés par des rançongiciels en 2022 et en 2023.
- Le panorama de la cybermenace 2024 que vient de publier l'ANSSI fait état d'une augmentation de 15 % des événements de sécurité traité par l'Agence.

Je pourrais multiplier les exemples mais ce qui est intéressant, c'est la réponse que le Gouvernement y apportera, soit pour appliquer la loi qui va maintenant être examinée à l'Assemblée nationale, soit pour créer des normes réglementaires dont le détail échappera de facto à la représentation nationale, avec le risque de sur-transposition et donc de distorsion de concurrence avec nos voisins européens.

J'en viens au contenu de la transposition de ces directives, car c'est dans le détail que le diable se niche, et c'est ce que nous avons voulu corriger en première lecture au Sénat :

- La directive REC, qui a été négociée sous présidence française de l'Union européenne, s'inspire en grande partie du dispositif français existant et sa transposition en droit national consiste donc essentiellement en une actualisation du dispositif de sécurité des activités d'importance vitale (SAIV) en place depuis 2006. Le nombre d'opérateurs d'importance vitale, qui est d'environ 300, ainsi que le nombre de points d'importance vitale, de l'ordre de 1 500, ne devraient pas évoluer de manière significative. Globalement, les acteurs concernés sont déjà sensibilisés au passage d'une logique de protection des infrastructures d'importance vitale à une approche axée sur la résilience.
- Seulement, plusieurs différences doivent être signalées entre le texte qui nous est présenté et la directive. Les opérateurs « régaliens », c'est-à-dire exerçant dans le domaine de la défense ou de la sécurité nationales, qui étaient déjà soumis au dispositif de SAIV, sont intégrés dans le champ de la transposition, alors que cela n'était pas prévu par la directive.

- De même, le Gouvernement a choisi d'inclure les collectivités territoriales dans le champ de la transposition ce que n'imposait pas la directive.
- le champ d'application de la directive va concerner 11 secteurs, contre 2 seulement – énergie et transport ¬– précédemment. Concrètement, pour la France, la transposition de la directive REC se traduira par un élargissement du champ d'application du dispositif national actuel à plusieurs sous-secteurs, notamment les réseaux de chaleur et de froid, l'hydrogène et l'assainissement.
- Enfin, un mécanisme de sanction administrative pouvant être prononcée par une commission des sanctions (qui reste à créer) est prévu en cas de manquement. Sur ce dernier point, on s'interroge sur les plafonds de sanction inscrits dans le projet de loi, ces derniers (2 % du chiffre d'affaires ou 10 millions d'euros) étant sensiblement plus importants que dans d'autres États membres.

Les deux autres directives NIS 2 et DORA obéissent également à cette nouvelle orientation basée sur la résilience. Ce qui interroge plus particulièrement c'est l'absence de définition dans la loi des périmètres d'activité, des obligations mises à la charges des entreprises et collectivités, l'ensemble étant renvoyé au décret, c'est-à-dire à la discrétion du Gouvernement. La encore un exemple précis vaut mieux qu'un long discours :

- Nos voisins belges qui ont déjà transposé la directive NIS 2 nous ont dit lors que nos auditions hors les murs qu'ils prenaient pour référence le respect de la norme ISO 27001

dites « Systèmes de management de la sécurité de l'information ». En d'autres termes, une entreprise qui respecte cette norme est considérée en Belgique comme remplissant les obligations de la directive.

- J'ai posé directement la question au Directeur de l'ANSSI : « Est-ce qu'une entreprise française qui respecterait la norme ISO 27001 remplirait aussi ses obligations dans notre cadre national ? ». La réponse est « non, la norme ISO 27001 ne sera pas suffisante pour répondre aux obligations réglementaires que fixera l'ANSSI ».
- Cette réponse n'est pas anodine pour les plus de 15 000 entreprises, près de 1 500 collectivités territoriales, groupements de collectivités et organismes placés sous leur tutelle (dont l'ensemble des régions et des départements, près de 1 000 communautés de communes et de 300 communes de plus de 30 000 habitants) qui seront assujettis à ces nouvelles obligations ;
- Cette réponse est le révélateur que ce fameux point d'équilibre entre le besoin de sécurité nationale et l'acceptation des normes par les acteurs ne peut être laissé à la seule discrétion d'une agence qui ne rend aucun compte devant les entreprises et les collectivités. Dans la discussion, nous avons accepté un amendement du Gouvernement visant à créer un label national. J'attends de voir ce que l'ANSSI va proposer !

Je voudrais vous donner deux derniers exemples sur ce qui pose un problème d'acceptation de la norme quand celle-ci se fonde sur le contrôle et la sanction alors qu'elle est censée protéger et inciter les

acteurs à renforcer leur propre sécurité. Je pourrais multiplier les exemples mais je me contenterais de vous parler de deux cas de figure :

- Outre le montant des sanctions qui a été évoqué, une commission des sanctions, dont les membres sont nommés par l'autorité administrative, aurait le pouvoir d'interdire à un dirigeant d'entreprise d'exercer ses responsabilités jusqu'à ce que l'entité ait remédié au manquement !
- Autre exemple, les contrôles effectués par l'ANSSI se feraient à la charge des personnes contrôlées, entreprises ou collectivités territoriales ! Certains ont pu relever que si l'Urssaf sanctionne par des relèvements de charge et des pénalités, elle ne fait pas payer le coût du contrôle proprement dit. Le Sénat a limité le reste à charge des contrôles aux seuls audits ciblés, les contrôles proprement dits restant à la charge de l'ANSSI.

Je pourrai encore multiplier les exemples sur lesquels la commission spéciale et le Sénat ont modifié le texte.

La commission spéciale a adopté 61 amendements dont 53 de ses rapporteurs pour préciser les modalités de transposition des 3 directives.

o Inscrire dans la loi l'élaboration par le Gouvernement d'une stratégie nationale de cybersécurité ;

o Compléter et encadrer les définitions et délais d'application ;

o Clarifier les obligations pesant sur les entités assujetties ;

- o éviter des différences de traitement injustifiées entre les entreprises ;
- o simplifier la vie des entreprises ;
- o modérer les effets de surtranspositions.

Les travaux en séance publique ont permis de revenir sur des rédactions communes avec le gouvernement sur les questions de contrôle et de reste à charge des coûts des contrôles, certains désaccords subsistants principalement sur le titre III relatif à la transposition de la directive DORA, notamment sur 2 mesures :

→ faire de l'Autorité des marchés financiers le guichet unique, en matière de déclaration d'incidents informatiques, pour les entreprises de marché et les prestataires de services sur cryptoactifs ;

→ appliquer le principe de proportionnalité pour l'application du règlement DORA aux sociétés de financement petites et non complexes.

Par ailleurs une mesure emblématique a été adoptée à mon initiative pour empêcher toute mesure instaurant des backdoors ou des failles dans le chiffrement des messageries.

Un mot plus particulier sur cet amendement qui a été adopté par 181 voix contre 134 après un débat en séance publique. Cet amendement vise à éviter d’imposer aux fournisseurs de services de chiffrement l’intégration de dispositifs techniques visant à affaiblir volontairement la sécurité de leur système ! Ces dispositifs sont appelés backdoors – portes dérobées – et constitue des failles de vulnérabilités afin que nos autorités puissent exercer un contrôle sur les données échangées. Cet aspect a été

mis en évidence publiquement par l'ancien directeur général de l'ANSSI, Guillaume Poupard.

Des collègues LR se sont opposés en faisant valoir que le Sénat avait adopté une position inverse à l'article 8 ter lors de la proposition de loi Narcotrafic, suite à un amendement de leur groupe. J'ai rappelé que cette disposition n'existait pas dans le rapport de la commission d'enquête de lutte contre le Narcotrafic ; que l'article 8 Ter avait eu un avis défavorable de la commission des Lois du Sénat ; et qu'il avait été adopté par le Sénat dans un contexte particulier qui ne correspondait pas au sujet débattu.

Il a été supprimé ensuite à l'unanimité de la commission spéciale de l'Assemblée nationale. Cette disposition n'existe donc plus avant l'examen en séance publique à l'Assemblée nationale où je doute fort qu'elle soit rétablie.

Aussi, il paraissait important de remettre l'église au milieu du village à la faveur de ce texte destiné justement à élever le niveau de notre sécurité numérique.

Face à des arguments caricaturaux et parfois déplacés des LR, j'ai indiqué en conclusion pour justifier l'amendement, que je suis en politique pour défendre des idées de liberté, de confiance dans nos réseaux dans le numérique, et notre sécurité.

En adoptant à une large majorité mon amendement, les sénateurs ont rappelé que le Sénat est et reste la maison des libertés publiques !

Enfin, la commission spéciale a formulé plusieurs recommandations:

- Fournir un effort de simplification des mesures d'application réglementaires, en se gardant de toute surtransposition réglementaire ;

- Accompagner les collectivités territoriales dans cette démarche nouvelle pour elles en tenant compte des problématiques de compétences et de financement ;

- Communiquer et faire œuvre de pédagogie, à l'échelle du pays, sur l'effort de résilience et de cybersécurité, en lien avec la stratégie nationale de cybersécurité.

Pour conclure, je voudrais dire ici que ce travail n'est possible que grâce à l'implication de tous les acteurs et parties prenantes de ce projet de loi. C'est comme cela que j'ai entendu conduire cette commission spéciale, en organisant ayant 7 réunions publiques entre le 17 décembre 2024 et le 11 février 2025 :

- deux auditions de responsables publics (M. Vincent Strubel, directeur général de l'ANSSI et Mme Clara Chappaz, ministre délégué à l'intelligence artificielle et au numérique) ;

- et 5 tables rondes avec les organisations professionnelles (MEDEF, CPME), des représentants des entreprises cyber (ACN, CyberCercle, CyberTaskForce, Clusif), les associations d'élus (association des maires de France, association des départements de France, association des régions de France, intercommunalités de France, Métropole du Grand Paris), les autorités de régulation financière (AMF

et ACPR) et 3 grands acteurs de la cyberdéfense (Airbus, Orange et Thales).

Certains sont présents aujourd'hui et je les en remercie.

J'espère avoir été dans le thème en introduisant cette conférence par un aspect très concret des travaux de la commission spéciale et de mon rôle de Sénateur.

Je vous remercie et me réjouis par avance du débat qui s'ouvre maintenant.