



## COMMUNIQUE DE PRESSE

### **LA COMMISSION SUPERIEURE DU NUMERIQUE ET DES POSTES (CSNP) APPELLE A L'EXAMEN DU PROJET DE LOI RESILIENCE DANS LES PLUS BREFS DELAIS**

Publiée le 14 décembre 2022, la directive NIS 2 s'appuie sur les acquis de la directive NIS de 2016, qui avait posé les bases d'une cybersécurité commune européenne, et vise à élever le niveau de sécurité à travers toute l'Union européenne. Alors que NIS 1 concernait environ 300 opérateurs de services essentiels (OSE), NIS 2 devra s'appliquer, en France, à plus de 15 000 entités dans 18 secteurs essentiels (énergie, santé, transports, télécoms...), ainsi qu'à près de 1 000 communautés de communes et 300 communes de plus de 30 000 habitants.

Dans son avis n°2024-07 du 3 octobre 2024, les membres de la Commission supérieure du numérique et des postes (CSNP) disaient accueillir très favorablement la transposition de la directive NIS 2, soulignant l'urgence de relever rapidement le niveau de sécurité numérique global de nos entreprises, administrations publiques et collectivités territoriales.

Le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité présenté le 15 octobre 2024 par le gouvernement a pour objet de transposer les dispositions relatives aux directives européennes NIS 2, REC et DORA au sein du droit français.

**Ce texte, bien qu'adopté par le Sénat le 12 mars 2025, n'a toujours pas été examiné par l'Assemblée nationale et achevé son parcours législatif, alors même que la directive NIS 2 devait être transposée dans le droit de chaque État membre avant le 17 octobre 2024.**

Ce retard fragilise notre écosystème numérique et place l'ensemble des acteurs concernés dans une situation d'incertitude injustifiable. Il intervient au moment même où le gouvernement vient de dévoiler une nouvelle stratégie nationale de cybersécurité, pourtant dépourvue d'un cadre réglementaire indispensable. **Cette situation illustre un décalage préoccupant entre les ambitions de l'État et sa capacité à en assurer la mise en œuvre, au risque de fragiliser la protection de nos entreprises, administrations publiques et collectivités territoriales face à des menaces cyber toujours plus nombreuses et importantes.**

**Au 1er janvier 2026, 20 Etats membres sur 27 avaient déjà procédé à la transposition de la directive, plaçant la France dans une situation de décalage préoccupante vis-à-vis de ses homologues européens. Cette situation est d'autant plus paradoxale que la France s'est historiquement positionnée parmi les Etats moteurs de l'Union européenne en matière de cybersécurité et de régulation du numérique. Dans un domaine où la crédibilité repose aussi sur l'exemplarité, ce retard affaiblit fortement la position de la France au moment même où se redessine l'architecture européenne de la cybersécurité, notamment par les négociations sur la révision du Cybersecurity Act.**

Le retard pris dans l'achèvement de l'examen de ce texte appelle une clarification. Celui-ci ne procède pas de l'agenda parlementaire ou d'un désaccord de fond, la nécessité de transposer la directive NIS 2 étant largement consensuelle au sein du Parlement, mais d'un point de clivage politique : l'article 16 bis, introduit au Sénat afin de consacrer dans la loi la protection du chiffrement et d'interdire l'imposition de dispositifs de portes dérobées (« *backdoors* ») aux messageries instantanées, fait l'objet d'une opposition du gouvernement. **Un tel désaccord politique ne saurait justifier de retarder volontairement l'adoption d'un texte aussi essentiel pour la sécurité numérique de notre pays.**

Or, le programme législatif transmis par le gouvernement aux parlementaires le 17 février dernier prévoit désormais un examen du texte en juillet 2026, et ce sous réserve de la convocation d'une session extraordinaire. **Un tel calendrier reporte de plusieurs mois encore l'adoption de ce texte, si toutefois il est examiné avant l'été 2026.**

Alors que les cyberattaques visant nos entreprises, administrations publiques et collectivités territoriales se multiplient et gagnent en intensité, la France ne peut plus se permettre de demeurer sans un cadre réglementaire adapté. L'absence prolongée de cette transposition fragilise notre sécurité collective, entretient l'incertitude pour les acteurs concernés et affaiblit la position de la France au niveau européen.

**Dans ce contexte, les membres de la CSNP appellent à l'inscription, dans les plus brefs délais, du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité à l'ordre du jour de l'Assemblée nationale, afin que la France se dote enfin des outils indispensables à la protection de son économie, de ses institutions et de ses citoyens.**