NIS2 : la France ne peut pas se payer le luxe d'un retard de plus

Olivier CADIC
Sénateur représentant les Français établis hors de France
Vice-président de la commission des Affaires étrangères, de la Défense et des Forces armées
Président de la commission spéciale du Sénat sur le « PJL Résilience »

La directive européenne NIS2 devait être transposée en droit français avant le 17 octobre 2024. Nous en sommes loin. Pendant que les cyberattaques se multiplient, que les fuites de données touchent entreprises, hôpitaux, collectivités et administrations, la France laisse s'installer une zone grise : celle d'un cadre juridique incomplet, d'obligations encore théoriques, et d'une responsabilité publique qui s'efface au moment même où la menace s'intensifie.

Le projet de loi dit « Résilience & Cyberscurité », qui transpose NIS2 (aux côtés de DORA et REC), a pourtant avancé : le Sénat l'a adopté en première lecture le 12 mars 2025, puis la commission spéciale de l'Assemblée nationale l'a approuvé à l'unanimité le 10 septembre dernier. Plus de 6 mois ont passé et le texte n'est toujours pas inscrit à l'ordre du jour du Palais Bourbon.

Ce blocage est incompréhensible et préoccupant.

Avec Philippe Latombe, chacun en notre qualité de président de la commission spéciale chargée de l'examen du texte – lui à l'Assemblée nationale, moi au Sénat – nous avons tenu le 4 février 2026 une conférence de presse pour alerter sur ce retard. Nous l'avons fait parce que le temps politique n'est pas celui de la menace : dans le cyber, une intrusion se joue parfois en quelques minutes, quand une loi met des mois à aboutir. Dans ce décalage, ce sont nos concitoyens qui en paient le tribut par le vol de leurs données, la perte de confiance, et parfois l'indisponibilité de services essentiels.

La cause du blocage est connue : l'article 16 *bis*, introduit à mon initiative lors des débats au Sénat qui interdit d'imposer aux fournisseurs de services de chiffrement l'intégration de dispositifs techniques visant à affaiblir volontairement la sécurité des systèmes d'information et des communications électroniques qu'il s'agisse de « portes dérobées » (*backdoors*), de « clés maîtresses » ou de tout mécanisme permettant un accès non consenti à des données protégées.

Je l'assume pleinement.

Cet article 16 *bis*, dit « anti-backdoors », ne vise pas à entraver le travail des enquêteurs ou des services de renseignement. Il vise à protéger un principe simple : on ne renforce pas la cybersécurité en créant volontairement une vulnérabilité structurelle. Une porte dérobée n'est pas une « bonne faille » réservée aux autorités : c'est une faille, point. Et si elle existe, elle peut être découverte et exploitée par des criminels ou des puissances étrangères. Ce risque n'est pas théorique : l'histoire récente montre que

des dispositifs d'interception peuvent être retournés contre ceux qui les ont conçus, au détriment de millions d'utilisateurs.

Le paradoxe est total : d'un côté, l'exécutif affirme que le chiffrement est un socle de la résilience numérique ; de l'autre, il bloquerait la transposition de NIS2 au nom d'une contestation de la protection du chiffrement.

Nous ne demandons pas l'impossible. Nous demandons une décision : inscrire le texte à l'ordre du jour. Transposer NIS2, c'est enfin donner aux acteurs concernés - plus nombreux que jamais - un cadre clair de gestion des risques, de notification d'incidents et de gouvernance.

Retarder NIS2, c'est retarder la protection. La France ne peut pas se permettre d'être en retard sur sa propre sécurité.