



Philippe Latombe

Député de la Vendée

Madame Anne Le Hénanff
Ministre déléguée
chargée de l'Intelligence artificielle
et du Numérique

Le 13 janvier 2026

Madame la Ministre,

Voté début septembre dernier en première lecture en commission spéciale, le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité est à ce jour toujours dans l'attente de sa mise à l'agenda de la séance de l'Assemblée nationale.

Ce texte vise à transposer dans le droit français la directive NIS2 mais, également, celle sur la résilience des entités critiques (REC), et à intégrer les dispositions de la directive du 14 décembre 2022 accompagnant le règlement Digital Operational Resilience Act (DORA).

Dans un contexte géopolitique particulièrement éruptif, tant par la dégradation des relations transatlantiques que par la multiplication des ingérences étrangères, russes notamment, cette transposition ne constitue pas une simple évolution réglementaire, mais un enjeu majeur de consolidation de nos capacités et de notre résilience en matière de cybersécurité.

Si NIS 2 impose des exigences proportionnées de résilience opérationnelle à près de 15 000 entités qualifiées d'essentielles ou d'importantes au niveau européen, en soumettant l'ensemble de leurs systèmes d'information à des obligations précises, c'est bien dans le but d'améliorer leur maturité informatique et, *in fine*, de les protéger. Le retard mis à finaliser l'examen de ce texte est donc particulièrement préoccupant. Les entreprises et les collectivités attendent depuis longtemps, s'inquiètent d'ailleurs et nous demandent de la visibilité pour pouvoir s'organiser.

En attendant, les attaques contre les systèmes d'information sont quotidiennes, y compris contre des entités étatiques ou exerçant une mission de service public : hôpitaux publics ou privés, France Travail (à plusieurs reprises, la première fois n'ayant à elle seule visiblement pas servi de leçon), le ministère des Sports... La liste est interminable. Le ministère de l'Intérieur lui-même a mis plus de trois semaines à réaliser qu'il était piraté. Faut-il en rire ou en pleurer ?

Indépendamment de cette difficulté calendaire de notre pays à se mettre en conformité avec la législation européenne et du risque encouru de pénalités, l'État, en cas de défaillances de certaines entités critiques, pourrait même se voir attaqué en justice pour ne pas avoir rempli son rôle de protection, en raison de ce processus législatif inabouti. Alors que ces directives sont applicables depuis 2024, une victime de cyberattaque pourrait ainsi se retourner contre

lui pour manquement et/ou demander à un juge d'appliquer la directive européenne, notamment les sanctions financières et les peines complémentaires qui y sont prévues.

Vous pourriez même, Madame la Ministre, être *de facto* tenue pour responsable, au moins médiatiquement.

Vu de l'étranger, ce manquement à nos obligations européennes dégrade la France aux yeux des observateurs, de ses partenaires, marquant encore un peu plus ce que certains esprits chagrins qualifient de déclassement. Il est donc urgent que ce texte qui, cela mérite d'être noté, a été voté à l'unanimité en commission, soit programmé en séance, lors d'un examen qui devrait être aussi rapide qu'essentiel.

Je vous remercie, Madame la Ministre, de bien vouloir m'indiquer quand le gouvernement envisage son inscription à l'ordre du jour de l'Assemblée nationale et vous prie de croire à l'assurance de ma considération distinguée.


~~P. LAFONT~~