

Le projet de loi résilience, en clair

LES FAITS

Présenté le 15 octobre 2024 au Sénat, le projet de loi sur la résilience des infrastructures critiques, dit loi résilience, vise à renforcer la sécurité des infrastructures essentielles face aux menaces croissantes. Ce texte est en cours d'examen au Parlement et devrait être adopté en avril 2025.

LE CONTEXTE

L'intensification des cyberattaques contre les infrastructures critiques, l'émergence de nouvelles menaces hybrides et les tensions géopolitiques ont rendu nécessaire l'adaptation du cadre réglementaire européen. Ce projet de transposition de plusieurs directives européenne s'inscrit dans une stratégie européenne plus large de renforcement de la cybersécurité.

LES DIRECTIVES	CLARIFICATION
Directive REC	La directive REC sur la résilience des entités critiques encadre les entités critiques. Celles-ci sont désignées par les Etats membres. Le projet de loi résilience intègre ces principes en établissant des standards minimaux pour les équipements utilisés dans les infrastructures critiques et en imposant une surveillance du cycle de vie des produits numériques déployés dans ces environnements sensibles.
Directive NIS 2	La directive Network and Information Security 2 est la colonne vertébrale du projet, élargissant considérablement le champ d'application de NIS 1. En France, cette transposition multiplie le nombre d'entités régulées incluant désormais les moyennes entreprises de secteurs critiques. Le texte renforce également les exigences de notification d'incidents, les contrôles de conformité et prévoit un régime de sanctions administratives plus dissuasif.
Directives techniques de DORA	Le règlement DORA est axé sur le secteur financier. Le projet de loi introduit des obligations spécifiques pour les prestataires de services numériques du secteur financier, notamment en matière de tests de résilience et de gestion des risques liés aux tiers.

L'ANALYSE

Giuliano Ippoliti,
directeur cybersécurité de Cloud Temple

«Le projet de loi résilience transpose en droit français les directives européennes NIS 2, REC et DORA, renforçant la protection des infrastructures critiques nationales. Présenté au Sénat en octobre 2024, ce texte répond à l'augmentation de 15% des incidents cyber observés en 2024. En élargissant le périmètre des entités régulées et en imposant des standards techniques stricts, la France affirme sa souveraineté numérique tout en s'inscrivant dans la stratégie européenne de cybersécurité.»

COMPARATIF DU NOMBRE D'INCIDENTS ET SIGNALEMENTS 2023/2024

Sur l'année 2024, 3004 signalements et 1361 incidents ont été portés à la connaissance de l'ANSSI soit une augmentation de 15% par rapport à l'année 2023. Source : ANSSI

Au cours de la période des JOP 2024, des tentatives de déstabilisation, de l'espionnage et des attaques à but lucratif ont été observés.

