NIS2 : la France condamnée à l'astreinte pendant que le référentiel cyber s'impose aux collectivités

Le 8 juillet 2026, la Commission européenne a saisi la Cour de justice de l'Union européenne (CJUE) contre la France, faute de transposition de la directive NIS2 sur la cybersécurité. Au même moment, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) fait déjà descendre son référentiel technique vers les régions, les départements et les communes de plus de 30 000 habitants. L'État se voit reprocher son propre retard réglementaire pendant qu'il prépare un régime contraignant pour des collectivités aux budgets numériques sans commune mesure avec les siens. Cet article lit cette asymétrie non comme une contradiction accidentelle, mais comme la signature d'un instrument précis de l'action publique : le mandat non financé.

Par Alexandre Berge · 3 octobre 2026 · 16 min de lecture · Analyse

Bruxelles sanctionne l'État pendant que le référentiel descend vers le local

Le fait précède l'analyse. La directive (UE) 2022/2555, dite NIS2, entrée en vigueur le 16 janvier 2023, devait être transposée dans les droits nationaux au plus tard le 17 octobre 2024. La France a laissé passer l'échéance. Après une lettre de mise en demeure adressée à vingt-trois États membres le 28 novembre 2024, puis un avis motivé notifié à dix-neuf d'entre eux le 7 mai 2025, la Commission a décidé, le 8 juillet 2026, de renvoyer devant la CJUE les quatre retardataires restants : la France, l'Espagne, l'Irlande et les Pays-Bas. Son communiqué officiel (IP/26/1499) demande à la Cour d'imposer des sanctions financières « consistant en une somme forfaitaire et des astreintes journalières jusqu'à la notification de la transposition complète ». Aucun montant n'est chiffré dans le communiqué : la fixation relève de la Cour, qui n'a pas encore statué.

Le véhicule de transposition français, le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, transpose d'un seul texte trois normes européennes (NIS2, la directive REC sur la résilience des entités critiques et la directive accompagnant le règlement DORA pour le secteur financier). Son parcours s'est enlisé : dépôt au Sénat le 15 octobre 2024, adoption en première lecture par le Sénat le 12 mars 2025, adoption d'un texte amendé par la commission spéciale de l'Assemblée nationale le 10 septembre 2025, puis un blocage durable. Le texte n'a jamais été inscrit en séance publique.

Au 31 août 2026, il ne figurait à aucun ordre du jour, son examen ayant glissé de la session extraordinaire de juillet 2026 à la rentrée de septembre au plus tôt. Le point d'achoppement est documenté : un article, introduit au Sénat, interdisant d'imposer des portes dérobées (les *backdoors*, accès dérobés ménagés dans un logiciel) aux fournisseurs de services de chiffrement, disposition combattue par les services de renseignement.

Pendant que la loi patiente, l'administration avance. L'ANSSI a publié le 17 mars 2026, au Campus Cyber, la version de travail 2.5 de son Référentiel Cyber France (ReCyF), qui décline les objectifs de sécurité fixés par NIS2. Ce document, juridiquement non contraignant tant que les décrets d'application ne sont pas pris, structure déjà la conformité future. Il fixe vingt objectifs de sécurité : les quinze premiers s'imposent aux entités importantes comme aux entités essentielles, les cinq derniers (objectifs 16 à 20 : approche par les risques, audit, sécurisation des configurations, administration dédiée, supervision) étant réservés aux seules entités essentielles au nom du principe de proportionnalité (l'exigence croît avec la criticité de l'entité). Ces vingt objectifs se déclinent en 152 exigences, dont 77 communes et 75 réservées aux entités essentielles. Le contenu de la norme est donc connu avant que la norme n'existe. Seule sa date d'opposabilité reste ouverte.

Le périmètre local a été tranché au Sénat : sont concernés les régions, les départements, les communes de plus de 30 000 habitants, ainsi que les métropoles, communautés urbaines et communautés d'agglomération comprenant au moins une commune de plus de 30 000 habitants. Sur les quelque 15 000 entités françaises attendues dans le champ de NIS2, les collectivités et leurs groupements en représentent environ 10 pour cent. Selon les calculs de l'ANSSI repris par la Commission supérieure du numérique et des postes (CSNP) et rapportés par Localtis (Banque des Territoires), au moins 2 481 structures locales seraient concernées, soit 1 489 collectivités et groupements relevant des entités essentielles et 992 communautés de communes relevant des entités importantes.

Le mandat non financé nomme l'asymétrie que le discours de la protection masque

Le fait empirique installé, le mécanisme peut être nommé. La science politique dispose d'un concept qui décrit précisément la situation : le mandat non financé (*unfunded mandate*), tel que l'a analysé Paul L. Posner dans *The Politics of Unfunded Mandates : Whither Federalism ?* (Georgetown University Press, 1998). Posner y étudie la pratique par laquelle un échelon supérieur de gouvernement impose à des échelons inférieurs la mise en œuvre d'une politique publique sans transférer les ressources correspondantes. Sa thèse centrale est que le mandat n'est pas un accident de la décentralisation mais un instrument politiquement rationnel : il permet à l'autorité qui commande d'afficher la vertu d'une politique (ici la résilience cyber) tout en externalisant vers d'autres le coût de sa réalisation et l'impopularité de la contrainte.

> **Le mandat non financé (Posner, 1998)**
>
> Paul L. Posner définit le mandat comme l'obligation faite par un niveau de gouvernement à un autre d'exécuter une politique, sans compensation financière intégrale. Son ouvrage montre que cet outil prospère parce qu'il dissocie la décision (qui revient à l'autorité supérieure et lui vaut le crédit) de la charge (qui pèse sur les collectivités et leur vaut la responsabilité de l'exécution). Le mandat déplace ainsi la ligne de front budgétaire sans déplacer la ligne de front politique.

L'opérationnalisation sur le cas NIS2 est directe. L'obligation naît à Bruxelles, elle est portée par l'État qui la transpose et la précise via l'ANSSI, mais elle s'exécute et se finance largement au niveau local. Le régime des sanctions confirme la mécanique : les entités publiques, dont les collectivités, sont exemptées des amendes pécuniaires que NIS2 prévoit pour les entités privées (jusqu'à 10 millions d'euros ou 2 pour cent du chiffre d'affaires mondial pour une entité essentielle), mais elles restent soumises aux obligations de fond et aux contrôles. La contrainte demeure entière, la sanction financière directe disparaît, ce qui déplace la pression du registre de l'amende vers celui du coût de mise en conformité, entièrement à la charge de la collectivité.

Cette lecture éclaire ce que le vocabulaire institutionnel de la « protection » et de l'« accompagnement » tend à recouvrir. Le discours public présente NIS2 comme un bouclier offert aux territoires. La grille du mandat non financé montre l'autre face : un transfert de charge dont le montant, les compétences et la mise en œuvre incombent à des organisations qui n'ont ni décidé de la norme ni obtenu les moyens de l'appliquer. Le découplage néo-institutionnel entre la règle affichée et la pratique réelle, décrit par Meyer et Rowan en 1977, n'est ici qu'une conséquence possible du dispositif, non son moteur : le moteur est budgétaire et institutionnel.

Les budgets locaux mesurent l'écart entre la norme et la capacité d'adoption

L'asymétrie n'est pas rhétorique, elle est chiffrée. Une étude de la Fédération nationale des collectivités concédantes et régies (FNCCR), réalisée avec Tactis, Parme avocats et Devoteam à partir d'une enquête diffusée début 2021 et rapportée par Localtis, établissait que la part du budget informatique consacrée à la cybersécurité atteignait « seulement 4,5 % dans les départements, 6,5 % chez les EPCI », seuls les syndicats et structures de mutualisation dépassant le seuil de 10 pour cent considéré comme un minimum par l'ANSSI. Le troisième baromètre publié par Cybermalveillance.gouv.fr avec OpinionWay (enquête menée du 26 août au 4 octobre 2024 auprès de 1 710 élus et agents de communes de moins de 25 000 habitants) documente un tissu encore plus fragile en bas de l'échelle : 73 pour cent des petites et moyennes collectivités disposent d'un budget informatique annuel inférieur à 5 000 euros et 77 pour cent consacrent moins de 2 000 euros par an à leur sécurité informatique. Or NIS2 ne prévoit pas d'application graduelle selon la taille, ce que les

associations d'élus ont explicitement regretté.

Le coût de la mise en conformité, lui, se compte en milliards. Un amendement débattu au Sénat estimait le coût global de mise en conformité à environ 2 milliards d'euros, dont 690 millions d'euros par an pour les seules collectivités, hors recrutements. Une note interne de l'ANSSI, citée dans un avis budgétaire du Sénat sur le projet de loi de finances pour 2025, avançait un coût moyen de mise en conformité de 400 000 euros par entité, quel que soit son type. Ces chiffres sont des estimations ex ante, à manier avec prudence, mais leur ordre de grandeur est sans ambiguïté au regard des budgets réels décrits plus haut : l'écart entre ce qu'exige la norme et ce que peut financer l'échelon chargé de l'appliquer est structurel, non conjoncturel.

Cet écart ne se lit pas seulement en euros, mais aussi en exposition. La menace est réelle et documentée. Dans sa synthèse « Collectivités territoriales » (CERTFR-2025-CTI-002) publiée le 24 février 2025, l'ANSSI indique avoir traité 218 incidents de cybersécurité affectant les collectivités en 2024, soit une moyenne de dix-huit par mois et 14 pour cent de l'ensemble des incidents traités par l'Agence (dont 144 touchant des communes, 44 des départements, 29 des régions, et 25 liés à des rançongiciels). Son panorama de la cybermenace 2024 recense par ailleurs les collectivités parmi les principales victimes de rançongiciels, à hauteur de 17 pour cent des victimes connues. La justification de fond de NIS2 n'est donc pas contestable. Ce qui l'est, c'est le mode de financement de la réponse.

> **La norme précède ses moyens : le ReCyF en trois chiffres**
>
> Version de travail 2.5 du 17 mars 2026. Vingt objectifs de sécurité d'atteinte obligatoire, dont quinze communs aux entités importantes et essentielles et cinq réservés aux entités essentielles. Cent cinquante-deux exigences détaillées, dont 75 réservées aux entités essentielles. Le référentiel existe et se diffuse ; la loi qui le rend opposable, elle, n'est pas promulguée.

Le RGPD de 2018 a déjà écrit ce scénario

Le mécanisme n'est pas inédit. Le parallèle le plus proche structurellement n'est pas une autre affaire de cybersécurité, mais l'entrée en application du Règlement général sur la protection des données (RGPD) le 25 mai 2018. La proximité est presque terme à terme : une norme d'origine européenne, applicable à toutes les collectivités quelle que soit leur taille, assortie d'une obligation nouvelle (la désignation d'un délégué à la protection des données) et d'un besoin de compétences rares, dans un contexte de budgets contraints.

Surtout, le RGPD illustre le refus assumé du financement dédié. Interrogé sur la création d'une dotation destinée à aider les collectivités à se mettre en conformité, le gouvernement a répondu qu'une telle dotation était écartée, notamment comme contraire à l'article 40 de la Constitution. La réponse apportée aux collectivités n'a pas été un transfert de ressources,

mais un dispositif de contournement de la contrainte : la mutualisation. Le RGPD autorise expressément, pour le secteur public, la désignation d'un délégué à la protection des données mutualisé entre plusieurs autorités, présentée par la CNIL comme la solution adaptée aux plus petites structures pour diminuer les coûts. La mutualisation ne réduit pas l'obligation, elle en répartit la charge entre des acteurs déjà sous-dotés. Elle est la forme concrète que prend l'adaptation à un mandat non financé.

Le résultat de ce scénario est connu : une adoption lente, inégale, et une capacité de contrôle qui met des années à devenir effective. La transposition de NIS2 vers les collectivités emprunte la même trajectoire, avec les mêmes instruments de report de charge (mutualisation intercommunale ou départementale, recours à des prestataires, appui des centres de réponse à incident régionaux). D'autres précédents confirment le motif sans qu'il soit utile de les développer : l'obligation d'accessibilité numérique des sites publics au titre du référentiel général d'amélioration de l'accessibilité, longtemps peu appliquée faute de moyens et de sanction effective, ou la condamnation de la France par la CJUE en 2005 dans l'affaire dite des « poissons sous-taille », qui montre qu'une astreinte européenne peut effectivement frapper l'État.

> **Ce qu'une astreinte peut coûter : le précédent de 2005**
>
> Le 12 juillet 2005 (affaire C-304/02, arrêt dit « merluchon »), la Cour de justice a condamné la France, pour la première fois, à cumuler une somme forfaitaire de 20 millions d'euros et une astreinte de 57 761 250 euros par période de six mois, pour ne pas avoir exécuté un arrêt de 1991 relatif au contrôle des pêches. Cet ordre de grandeur ne préjuge pas de ce que la Cour décidera sur NIS2, mais il rappelle que la sanction pécuniaire d'un manquement persistant n'est pas symbolique.

L'angle mort : l'accompagnement se retire à mesure que l'obligation arrive

Le non-dit du discours institutionnel n'est pas le coût, largement reconnu, mais la synchronisation inverse entre l'arrivée de l'obligation et le retrait de l'accompagnement. L'État a bien financé une montée en compétence des collectivités, mais ce financement était temporaire et son extinction coïncide avec l'entrée en vigueur de la contrainte. Le programme « parcours de cybersécurité », doté de 100 millions d'euros dans le cadre de France Relance, a accompagné 945 entités, dont 707 collectivités territoriales (près de 75 pour cent des bénéficiaires), et a permis, selon l'ANSSI, de faire passer en moyenne leur score de maturité cyber d'un niveau « D+ » à un niveau « B ». Mais son bilan, publié le 28 avril 2025, est celui d'un programme clos sur le plan financier. Il s'agit d'un dispositif d'amorçage arrivé à terme, non d'un soutien pérenne.

La suite illustre la même tension. Les centres de réponse à incident cyber territoriaux (CSIRT), issus de France Relance, voient leur pérennité fragilisée par le contexte budgétaire : l'ANSSI,

qui avait demandé 35 millions d'euros et soixante emplois supplémentaires pour 2025, notamment au titre de NIS2, n'a obtenu que 27 millions d'euros et aucun poste. La revue nationale stratégique de juillet 2025 a réaffirmé un engagement de soutien aux CSIRT et aux collectivités pour 2026, mais sans en détailler les moyens. L'obligation, elle, est précise ; le financement de son exécution reste indicatif.

Un dernier angle mort mérite d'être signalé, loyalement, car il est régulièrement soulevé par les intéressés eux-mêmes : l'absence d'étude d'impact chiffrant, pour les collectivités, les coûts financiers, humains et administratifs de la mise en conformité. Les associations d'élus (Association des maires de France, Régions de France, Départements de France, Intercommunalités de France) l'ont réclamée à plusieurs reprises comme une garantie préalable à la transposition. Ce vide documentaire n'est pas neutre : il rend le débat sur le juste dimensionnement de l'accompagnement structurellement incomplet.

Ce comportement de l'État se laisse enfin éclairer par un second concept, distinct du premier. R. Kent Weaver, dans « The Politics of Blame Avoidance » (*Journal of Public Policy*, 1986), soutient que les responsables publics cherchent d'abord à éviter le blâme plutôt qu'à revendiquer le crédit, et qu'ils recourent pour cela à des stratégies comme la limitation de l'agenda et le transfert de la décision à d'autres acteurs. L'enlisement du projet de loi, suspendu à un désaccord sur le chiffrement plutôt qu'arbitré, et le report de la charge financière vers l'échelon local relèvent moins de la négligence que de cette logique d'évitement : différer une décision impopulaire et diffuser la responsabilité de son exécution.

Conclusion : un mandat qui s'exécutera avant d'être financé

L'État sanctionné pour son retard et les collectivités contraintes par le référentiel qu'il prépare ne sont pas deux dossiers distincts, mais les deux extrémités d'un même instrument. Le mandat non financé, au sens de Posner, permet de tenir ensemble ce qui paraît contradictoire : une puissance publique en défaut vis-à-vis de Bruxelles peut, sans incohérence de sa part, imposer un régime exigeant à des organisations moins dotées, parce que le dispositif dissocie précisément la décision de la charge. L'astreinte européenne pèse sur l'État ; le coût de la conformité pèse sur le local.

De ce diagnostic découle une hypothèse vérifiable. Si la lecture par le mandat non financé est juste, alors la promulgation de la loi et la publication des décrets d'application ne s'accompagneront pas d'une dotation nationale dédiée et fléchée vers les collectivités, comparable en ampleur au programme France Relance clos en 2024, mais reposeront sur des instruments de report de charge (mutualisation, prestataires, CSIRT à budget contraint). Un lecteur extérieur pourra tester cette hypothèse à l'aide d'un indicateur observable : la présence, ou l'absence, d'une ligne budgétaire pluriannuelle dédiée à la cybersécurité des collectivités dans la première loi de finances votée après la promulgation. L'horizon est daté : la loi de finances pour 2027, examinée à l'automne 2026, en constituera le premier test, et les

décrets d'application attendus dans les douze à vingt-quatre mois suivant la promulgation, le second.

Note méthodologique

Sources principales : le communiqué IP/26/1499 de la Commission européenne (8 juillet 2026), le référentiel ReCyF v2.5 de l'ANSSI (17 mars 2026), la synthèse « Collectivités territoriales » de l'ANSSI (24 février 2025), les dossiers législatifs du Sénat et de l'Assemblée nationale, et la presse spécialisée pour le suivi du calendrier. Réserve de lecture : la date de saisine de la CJUE est retenue au 8 juillet 2026 (date de la décision figurant au communiqué officiel), plusieurs organes de presse ayant mentionné le 9 juillet ou évoqué l'affaire à des dates ultérieures. Aucun montant d'astreinte ou de somme forfaitaire n'a été publié par la Commission ; les chiffres de coût de mise en conformité sont des estimations ex ante et sont présentés comme telles. Arbitrage théorique : le concept suggéré par le brief, le découplage néo-institutionnel de Meyer et Rowan (1977), a été écarté comme cadre central au profit du mandat non financé de Paul L. Posner (1998), plus directement opérationnel pour rendre compte de l'asymétrie entre l'État qui décide et les collectivités qui financent ; le découplage n'est mobilisé qu'en appui secondaire, et l'évitement du blâme de Weaver (1986) n'est convoqué que pour éclairer le comportement de l'État. Recherche de sources, croisement des données et structuration du raisonnement s'appuient sur une assistance par intelligence artificielle. Le choix de l'angle et du cadre théorique, la vérification des sources, les arbitrages et l'établissement du texte final relèvent de l'auteur.

Sources

Sources primaires institutionnelles

- Commission européenne, « Commission refers Ireland, Spain, France and the Netherlands to the Court of Justice for failing to transpose the rules on cybersecurity », communiqué IP/26/1499, 8 juillet 2026. https://ec.europa.eu/commission/presscorner/detail/en/ip _26_ 1499
- ANSSI, « Référentiel Cyber France (ReCyF), version de travail 2.5 », 17 mars 2026. https:// messervices.cyber.gouv.fr/documents-ressources/20260317_NIS_V2_ReCyF_v2.5.pdf
- ANSSI / CERT-FR, « Collectivités territoriales – Synthèse de la menace » (CERTFR-2025-CTI-002), 24 février 2025. https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-002.pdf
- ANSSI, « Panorama de la cybermenace 2024 », 2025. https://cyber.gouv.fr/actualites/ panorama-de-la-cybermenace-2024-mobilisation-et-vigilance-face-aux-attaquants/
- Sénat, dossier législatif « Résilience des infrastructures critiques et renforcement de la cybersécurité » (pjl24-033). https://www.senat.fr/dossier-legislatif/pjl24-033.html

- Assemblée nationale, dossier législatif DLR5L17N50731. https://www.assemblee-nationale.fr/dyn/17/dossiers/DLR5L17N50731

Rapports et travaux officiels

- ANSSI, « Les parcours de cybersécurité : rapport d'activité 2024 – Volet cybersécurité de France Relance », 28 avril 2025. https://cyber.gouv.fr/actualites/bilan-du-volet-cybersecurite-de-france-relance-un-defi-reussi
- Sénat, avis budgétaire sur le PLF 2025 (coordination du travail gouvernemental), estimation ANSSI du coût de conformité. https://www.senat.fr/rap/a24-146-9/a24-146-94.html
- CSNP, « Les enjeux de la transposition de la directive NIS 2 en France », rapport 2024. https://csnp.fr/wp-content/uploads/2024/10/Rapport-NIS-2-V12-Couverture-originale-1.pdf
- CNIL, « Guide pratique RGPD – Délégués à la protection des données ». https://www.cnil.fr/sites/cnil/files/atoms/files/guide _pratique_rgpd_-_delegues_a_la_protection_des_donnees.pdf
- Cybermalveillance.gouv.fr / OpinionWay, « 3e étude sur la maturité cyber des collectivités », 2024. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/cp-etude-2024-cybersecurite-collectivites

Cadres théoriques

- Paul L. Posner, *The Politics of Unfunded Mandates : Whither Federalism ?*, Georgetown University Press, 1998.
- R. Kent Weaver, « The Politics of Blame Avoidance », *Journal of Public Policy*, vol. 6, n° 4, 1986, p. 371-398.
- John W. Meyer et Brian Rowan, « Institutionalized Organizations : Formal Structure as Myth and Ceremony », *American Journal of Sociology*, 1977 (mention secondaire).

Parallèle historique

- Sénat, réponse à question écrite sur le coût de la mise en conformité RGPD des collectivités, 2019. https://www.senat.fr/questions/base/2019/qSEQ190108488.html
- CJCE, arrêt du 12 juillet 2005, Commission c/ France, affaire C-304/02 (« poissons sous-taille »).

Presse spécialisée

- Maire-info, « Directive NIS 2 : une transposition sensible pour les collectivités actuellement débattue au Sénat ». https://www.maire-info.com/cybermalveillance/directive-nis-2-une-transposition-sensible-pour-les-collectivites-actuellement-debattue-au-senat--article-29492

- Banque des Territoires (Localtis), « La cybersécurité, parent pauvre des budgets informatiques des collectivités » et « L'Anssi dresse un premier bilan des CSIRT régionaux ».
- Silicon, « Ce que risque la France pour ne pas avoir transposé NIS 2 », juillet 2026.
- Next, suivi du calendrier de transposition NIS2, 2026.