AVIS N° 2026-06 DU 6 MAI 2026

SUR LE CYBERSECURITY ACT 2

Vu le Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013 (règlement sur la cybersécurité) (Texte présentant de l'intérêt pour l'EEE)[1]

Vu la proposition de règlement relatif au règlement de l'UE sur la cybersécurité publiée le 20 janvier 2026[2]

Vu l'avis n°2024-05 du 4 septembre 2024 de la CSNP sur les enjeux politique et économiques du schéma européen de certification de sécurité des services cloud[3]

Vu les auditions de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et de la Direction générale des entreprises du ministère de l'Économie, des Finances et de la Souveraineté industrielle, énergétique et numérique (MEFSIEN)

Pour l'Agence nationale de la sécurité des systèmes d'information (ANSSI)
M. Vincent Strubel, Directeur général
Mme Laurence Begou, Directrice de cabinet adjointe

Pour la Direction générale des entreprises
M. Loic Duflot, Chef du service de l'économie numérique
M. Renaud Rodenas, Chef de projet réglementation du Cloud et de l'économie de la donnée
Mme Edith Guignabaudet, Chargée de mission Affaires européennes
Mme Shanna Leduc Morin, Chargée du cadre réglementaire du Cloud et de la donnée

Aux termes de ces consultations et de ses travaux, les membres de la Commission supérieure du numérique et des postes souhaitent formuler les recommandations suivantes :

Recommandation n°1 : exiger, lors des négociations au Conseil de l'Union européenne, l'intégration de clauses d'articulation explicites garantissant qu'une certification obtenue au titre du CSA2 vaut présomption de conformité pour les exigences techniques équivalentes des directives NIS 2, DORA et du CRA.

Recommandation n°2 : circonscrire le périmètre de la certification de la « cyber posture » des entités afin qu'elle ne se substitue pas aux prérogatives d'audit, de contrôle et de sanction des autorités de supervision nationales et sectorielles.

Recommandation n°3 : restreindre le périmètre du guichet unique de signalement (*Single Reporting Platform*) géré par l'ENISA afin de prévenir les risques d'engorgement et de compromission de la confidentialité liés au transit centralisé de données d'incidents critiques. Exiger, pour les acteurs relevant de la sûreté et de la sécurité nationale, une dérogation stricte garantissant que leurs déclarations d'incidents demeurent sous la prérogative exclusive de l'ANSSI.
.

[1] Règlement - 2019/881 - FR - EUR-Lex
[2] Proposition de règlement relatif au règlement de l'UE sur la cybersécurité | Bâtir l'avenir numérique de l'Europe
[3] Avis-n°2024-05-du-4-septembre-2024-sur-les-enjeux-politiques-et-economiques-du-schema-EUCS.pdf

Recommandation n°4 : demander à la Commission européenne de produire une étude d'impact détaillée évaluant la charge financière et administrative cumulée du CSA2, de NIS 2, de DORA et du CRA sur les entreprises européennes.

Recommandation n°5 : s'opposer fermement à l'article 16 du projet de règlement prévoyant la centralisation des vulnérabilités non corrigées au sein d'une base de données européenne gérée par l'ENISA, afin de préserver la maîtrise souveraine de l'ANSSI sur les failles affectant les infrastructures critiques nationales.

Recommandation n°6 : défendre un positionnement de l'ENISA strictement limité à la coordination et au partage d'informations, en bloquant tout transfert de compétences opérationnelles de réponse aux incidents au détriment des CSIRT nationaux.

Recommandation n°7 : garantir que l'adoption du CSA2 permette à la France d'assurer le maintien de la qualification SecNumCloud délivrée par l'ANSSI, sauf si un schéma européen de certification de sécurité offrant le même niveau de protection, notamment en termes d'immunité aux législations non européennes à portée extraterritoriale, était adopté.

Recommandation n°8 : amender les articles 19 à 23 pour imposer que la *Cybersecurity Skills Academy* s'appuie sur la reconnaissance mutuelle des référentiels nationaux existants, tels que SecNumedu en France, plutôt que sur la création d'un mécanisme européen d'autorisation directe des prestataires de formation.

Recommandation n°9 : exiger que l'introduction de nouvelles redevances prélevées directement auprès des acteurs économiques pour la délivrance d'autorisations et la maintenance des schémas de certification ne crée pas un effet d'éviction au détriment des budgets alloués aux agences nationales et que ce mécanisme n'alourdisse pas la charge financière des entreprises qui souhaitent renforcer leur niveau de sécurité et se mettre en conformité.

Recommandation n°10 : porter au niveau européen une définition de la cybersécurité ancrée sur les fondamentaux techniques (disponibilité, intégrité, confidentialité), en affirmant que toute législation étrangère permettant un accès secret aux données constitue une vulnérabilité technique à part entière.

Recommandation n°11 : refuser la dichotomie opérée par les considérants 77 et 129 du projet de règlement, qui exclut artificiellement l'exposition aux lois extraterritoriales du champ de l'évaluation technique de la conformité.

Recommandation n°12 : conditionner le soutien de la France au texte à la réintégration des risques de compromission légale d'origine étatique dans les grilles d'évaluation du Titre III relatif à la certification.

Recommandation n°13 : demander une révision de l'article 80, paragraphe 1, afin de clarifier la manière dont les fournisseurs soumis à des lois telles que le FISA américain peuvent légalement respecter l'obligation de « résister à tout événement » compromettant la confidentialité.

Recommandation n°14 : conditionner le soutien de la France à l'adoption de tout schéma de certification à la garantie que les fournisseurs certifiés ne soient pas soumis à des ordonnances de non-divulgation (*gag orders*), ces injonctions les rendant structurellement incapables de respecter l'obligation de signalement des accès non autorisés exigée à l'article 80, paragraphe 1, alinéa (d).

Recommandation n°15 : alerter le Conseil sur le risque juridique pesant sur les entreprises utilisatrices qui, en s'appuyant sur un certificat européen faussé, se retrouveraient en situation de non-conformité face à leurs propres obligations de gestion des risques au titre de NIS 2 et DORA.

Recommandation n°16 : démontrer l'inadéquation du Titre IV (logique de police administrative et de bannissement) pour le marché du cloud, et exiger la création de leviers de marché positifs permettant aux entreprises de choisir des solutions immunisées sans attendre une décision d'exclusion de la Commission.

Recommandation n°17 : modifier l'article 115 relatif aux sanctions pour s'assurer que les amendes pouvant atteindre 7 % du chiffre d'affaires mondial n'incombent pas aux seules entreprises utilisatrices, mais engagent conjointement la responsabilité des fournisseurs si une non-conformité étaient de leur fait.

Recommandation n°18 : réviser le mécanisme d'exemption de l'article 105 afin de réduire drastiquement le délai d'instruction de 9 mois et de définir des critères objectifs, garantissant ainsi la prévisibilité juridique des acteurs économiques, associé à un régime de maintien en conditions opérationnelles provisoire.

Recommandation n°19 : articuler le Titre IV avec le Titre III en établissant qu'un service disposant d'un certificat d'immunité validé est automatiquement exempté des restrictions liées à la chaîne d'approvisionnement.

Recommandation n°20 : déposer un amendement au Titre III visant à créer un label d'immunité aux législations extraterritoriales, conçu comme un module optionnel applicable de manière transversale aux niveaux d'assurance « basique », « substantiel » et « élevé ».

Recommandation n°21 : construire une coalition d'États membres favorables à cette approche modulaire, en démontrant qu'elle permet de sortir du blocage diplomatique sur le niveau « High+ » de l'EUCS tout en préservant l'ouverture du marché européen.

Recommandation n°22 : défendre le principe d'une adhésion volontaire à ce label modulaire, laissant à chaque entreprise ou administration la liberté de calibrer sa couverture juridique en fonction de sa propre analyse de risque au regard de la sensibilité de ses données.

Recommandation n°23 : garantir que ce label modulaire réponde par anticipation aux besoins des entités essentielles et importantes dans le cadre de la directive NIS2 et des organismes financiers soumis à DORA qui devront prouver l'étanchéité de leurs systèmes d'information dans le cadre des obligations futures imposées par le droit de l'Union.

I. Eléments de contexte

En avril 2019, l'adoption du règlement européen Cybersecurity Act (UE 2019/881) avait constitué une avancée majeure en définissant un cadre de certification de cybersécurité harmonisé à l'échelle européenne tant au niveau des méthodes d'évaluation que des différents niveaux d'assurance de certification.

Ce règlement permettait à l'ENISA[4], l'Agence de l'Union européenne pour la cybersécurité, créée en 2004, de :

- contribuer à la politique de l'Union européenne en matière de cybersécurité,
- renforcer la fiabilité des produits, des services et des technologies de l'information et de la communication (TIC) avec des systèmes de certification de cybersécurité,
- favoriser et coordonner la coopération avec les États membres et les organes de l'Union européenne grâce à un partage des connaissances, au renforcement des capacités et à la sensibilisation des autorités nationales et principalement les CSIRT nationaux,
- collaborer avec les principales parties prenantes pour renforcer la confiance dans l'économie connectée, accroître la résilience des infrastructures de l'Union européenne et donc de renforcer la sécurité numérique de la société et des citoyens européens.

Conformément au Cybersecurity Act, l'ANSSI est l'Autorité Nationale de Certification de Cybersécurité (ANCC) dans le cadre du Cybersecurity Act. A ce titre, l'ANSSI est en charge de surveiller la bonne application des différents schémas de certification européens en France.

En janvier 2026, la Commission a publié une proposition de révision du règlement sur la cybersécurité pour accroître les capacités et la résilience en matière de cybersécurité et prévenir la fragmentation du marché unique numérique de l'UE.

Cette révision propose également de renforcer la sécurité des chaînes d'approvisionnement des technologies de l'information et de la communication (TIC) de l'Union européenne.

Pour la Commission, ce projet de révision garantit que les produits auxquels ont accès les citoyens de l'Union européenne sont cybersécurisés dès la conception grâce à un processus de certification qui serait plus simple.

Le projet de révision renforce très sensiblement les pouvoirs de l'Agence de l'UE pour la cybersécurité (ENISA).

La Commission européenne a ouvert une phase de consultation qui prendra fin le 12 mai 2026.

Par le présent avis, la Commission supérieure du numérique et des postes a souhaité participer à cette consultation en formulant des recommandations et en attirant l'attention des autorités nationales et européennes sur plusieurs points de vigilance.

II. Historique du Cybersecurity Act et du Schéma européen de certification de sécurité des services cloud (EUCS)

L'élaboration du schéma européen de certification de sécurité des services cloud (EUCS) trouve son origine dans le règlement Cybersecurity Act (CSA1) de 2019. Ce projet avait pour mandat d'établir un référentiel garantissant la sécurité et la conformité des offres de services cloud sur le marché européen. La trajectoire de ce texte a été profondément modifiée par l'arrêt de la Cour de justice de l'Union européenne du 16 juillet 2020. En invalidant le Privacy Shield, la Cour a formellement exposé les pratiques de collecte massive permises par la section 702 du *Foreign Intelligence Surveillance Act* (FISA) américain. Si le *Data Privacy Framework* ratifié en juillet 2023 encadre désormais les données à caractère personnel, un vide juridique subsiste concernant la protection des données sensibles et stratégiques non personnelles des organisations européennes.

[4] European Union Agency for Cybersecurity, ENISA

Pour répondre à cette vulnérabilité, la première version de l'EUCS prévoyait un niveau de certification maximal baptisé "High+" sans poser de problème à aucun État européen jusqu'en 2023. Inspiré de la qualification SecNumCloud française, ce niveau de sécurité imposait des critères techniques, essentiellement de nature juridiques, d'immunité aux législations non européennes à portée extraterritoriale. L'objectif consistait à prémunir les données européennes contre les injonctions légales d'agences de renseignement étrangères, qu'elles soient américaines sous l'égide du FISA ou chinoises au titre de la loi sur le renseignement national de 27 juin 2017.

Ce projet a déclenché une offensive directe de la part de l'industrie et de l'administration des États-Unis. Le 25 mai 2023, la Computer & Communications Industry Association (CCIA) et la Business Software Alliance (BSA) ont adressé une requête à l'administration Biden. Ces groupements industriels ont dénoncé le niveau High+ comme une menace potentielle pour les intérêts économiques et la sécurité nationale des États-Unis. La pression diplomatique s'est concrétisée en septembre 2023 par l'intervention du Secrétaire d'État américain, Antony Blinken, qui a adressé une note à la Présidente de la Commission européenne, Ursula von der Leyen, l'avertissant que l'inclusion de ces critères d'immunité affecterait négativement les relations économique et sécuritaire entre les États-Unis et l'Union européenne. Sous cette pression, la Commission européenne a demandé à l'ENISA de revoir sa copie. Une nouvelle mouture, expurgée du niveau High+ et de toute exigence d'immunité, a été présentée au début de l'année 2024, et les services juridiques de la Commission ont justifié ce recul stratégique d'un argumentaire expliquant qu'un schéma de certification issu du CSA1 ne pouvait contenir que des critères techniques, sans préciser le sens de ce dernier terme.

Cet abandon génère une contradiction juridique flagrante avec le CSA1 de 2019. L'article 51 de ce règlement impose au schéma de certification de protéger les données contre l'accès non autorisé, d'identifier les dépendances connues et de garantir la traçabilité des consultations. Un référentiel validant des services cloud soumis aux injonctions secrètes du FISA contrevient à ces obligations légales. Les accès opérés par des services de renseignement tiers constituent à l'évidence des accès non autorisés au sens du droit européen, rendant la version actuelle de l'EUCS juridiquement défaillante.

C'est face à cette situation que la CSNP a adopté son avis du 4 septembre 2024. Ce document a alerté les pouvoirs publics sur le renoncement que représente la suppression du niveau High+. La CSNP y a rappelé que la confidentialité des données exige une protection contre les actes criminels isolés ainsi que contre les captations légales opérées par des puissances étrangères à des fins d'intelligence économique. L'avis a méthodiquement déconstruit l'argument selon lequel les critères d'immunité violeraient les règles de l'Organisation Mondiale du Commerce, la conformité aux traités s'appréciant au niveau de l'utilisation du référentiel dans les marchés publics, non dans sa définition technique.

Appuyée par les inquiétudes exprimées par la CNIL en juillet 2024, la CSNP a formellement demandé au Gouvernement d'exiger la suspension de l'adoption de cet EUCS affaibli. Elle a réclamé une analyse économique des conséquences de la dépendance à l'industrie américaine du cloud, positionnant la réintégration des critères d'immunité comme une condition non négociable pour l'émergence d'une industrie technologique européenne autonome.

C'est dans ce contexte que la Commission européenne a publié, le 20 janvier 2026, son projet de révision du Cybersecurity Act (CSA2).

Par ailleurs, cette publication intervient alors que la Commission Européenne prépare également le règlement sur le développement du Cloud et de l'IA (CADA), dont la présentation est attendue d'ici l'été 2026 et qui devrait traiter, entre autres, des conditions d'accès aux marchés publics européens dans ces secteurs.

La CSNP considère que ces deux chantiers sont indissociables : il convient d'anticiper les travaux du CADA en posant dès aujourd'hui le principe selon lequel les schémas de certification adoptés dans le cadre du CSA2 doivent intégrer explicitement une protection contre les législations à portée extraterritoriale auxquelles sont soumis les fournisseurs non européens, et que tout marché public relevant du périmètre de ces schémas devrait imposer à ces fournisseurs de s'y conformer.

III. Analyse du CSA2 : Une complexité accrue et des risques d'incohérence réglementaire

La proposition de révision du *Cybersecurity Act* (CSA2) constitue un texte d'une grande densité technique et juridique qui s'insère dans un écosystème législatif européen déjà saturé. Pour comprendre l'enjeu, il faut mesurer comment ce nouveau règlement s'articule ou se confronte à un nombre important d'autres textes majeurs. La Commission européenne elle-même souligne des risques d'incohérences, voire de contradictions directes, avec la directive NIS 2, qui fixe le cadre général de la gestion des risques pour les entités définies comme essentielles et importantes, et le *Cyber Resilience Act* (CRA), qui impose des règles de sécurité pour tous les produits numériques. Si le CSA2 n'est pas aligné avec DORA (*Digital Operational Resilience Act*), avec le CRA ou avec NIS2, pour ne retenir que ces trois textes essentiels, les dirigeants d'entreprises se retrouvent dans une insécurité juridique et pénale inacceptable face à leurs propres obligations.

L'inquiétude est d'autant plus forte que le CSA2 ne se limite plus à la seule certification de produits, services et processus comme le cloud. Le texte étend considérablement son périmètre en introduisant la certification des services de sécurité gérés (MSS) et, plus fondamentalement encore, la certification de la « cyber posture » des entités. Cette évolution majeure vise à permettre à une entreprise de prouver sa conformité globale à des textes comme NIS 2 ou DORA via un certificat. Or, en déplaçant la certification du produit vers l'organisation elle-même, le CSA2 percute directement les prérogatives d'audit et de contrôle des superviseurs sectoriels et nationaux. Ce basculement soulève une difficulté majeure. La « cyber posture » d'une organisation est par essence dynamique. Elle évolue quotidiennement pour s'adapter à de nouvelles vulnérabilités et à des menaces en mutation constante. À l'inverse, la délivrance d'un certificat atteste d'une conformité, valable à un instant T. Cet écart rend l'outil de la certification inadapté pour se substituer à la supervision continue et itérative exercée par les autorités nationales de contrôle, telles que l'ANSSI, dont la mission est précisément d'évaluer et de garantir la résilience opérationnelle des entités les plus sensible face à une menace en constante évolution technologique et géopolitique.

À ce socle s'ajoutent des textes en cours d'élaboration tels que le futur règlement sur le développement du Cloud et de l'IA (CADA) et le *Digital Networks Act* (DNA) pour les infrastructures de télécommunications. Pour une entreprise ou une administration, cette accumulation de couches réglementaires, chacune assortie de ses propres exigences de conformité, de reporting et de certification, menace de créer une insécurité opérationnelle majeure.

Certes, la Commission tente d'apporter une réponse à cette inflation normative en confiant à l'ENISA la création d'un guichet unique de signalement (*Single Entry Point* ou *Single Reporting Platform*). Si cette initiative va dans le sens d'une louable simplification en ambitionnant de permettre aux entreprises de déclarer leurs incidents cyber une seule fois pour l'ensemble des réglementations, elle ne résout pas le problème de fond. Si la coordination entre les exigences de certification du CSA2 et les obligations de gestion des risques dictées par ces autres textes n'est pas parfaitement fluide et dépourvue de contradictions, le risque demeure de voir les organisations s'épuiser dans une bureaucratie de la conformité au détriment de leur protection technique réelle.

Recommandation n°1 : exiger, lors des négociations au Conseil de l'Union européenne, l'intégration de clauses d'articulation explicites garantissant qu'une certification obtenue au titre du CSA2 vaut

présomption de conformité pour les exigences techniques équivalentes des directives NIS 2, DORA et du CRA.

Recommandation n°2 : circonscrire le périmètre de la certification de la « cyber posture » des entités afin qu'elle ne se substitue pas aux prérogatives d'audit, de contrôle et de sanction des autorités de supervision nationales et sectorielles.

Recommandation n°3 : restreindre le périmètre du guichet unique de signalement (*Single Reporting Platform*) géré par l'ENISA afin de prévenir les risques d'engorgement et de compromission de la confidentialité liés au transit centralisé de données d'incidents critiques. Exiger, pour les acteurs relevant de la sûreté et de la sécurité nationale, une dérogation stricte garantissant que leurs déclarations d'incidents demeurent sous la prérogative exclusive de l'ANSSI.

Recommandation n°4 : demander à la Commission européenne de produire une étude d'impact détaillée évaluant la charge financière et administrative cumulée du CSA2, de NIS 2, de DORA et du CRA sur les entreprises européennes.

IV. La préservation d'un équilibre des pouvoirs entre l'ENISA et les autorités nationales

Le Titre II du projet de règlement prévoit un élargissement substantiel du mandat et des moyens de l'Agence de l'Union européenne pour la cybersécurité, l'ENISA. Si le renforcement de la coopération européenne est une nécessité absolue, cette ambition ne doit pas se traduire par une centralisation excessive qui viendrait affaiblir les autorités nationales de sécurité, telles que l'ANSSI en France, ou les centres gouvernementaux de réponse aux incidents informatiques, les CSIRT nationaux, dont le CERT-FR. L'écosystème de la cybersécurité requiert avant tout de la réactivité et une fine connaissance du tissu économique et industriel local. Or, un transfert de compétences opérationnelles de l'échelon national vers l'échelon européen risquerait d'engendrer une lourdeur administrative et une perte d'efficacité inacceptable. À l'heure où les menaces s'intensifient de manière foudroyante, dopées par les usages malveillants de l'intelligence artificielle générative et, demain, par les capacités du déchiffrement quantique, notre résilience collective repose d'abord sur l'agilité de nos forces d'intervention de proximité.

Par ailleurs, l'article 16 du projet de règlement prévoit de confier à l'ENISA la maintenance d'une base de données européenne et le développement d'une capacité commune de gestion des vulnérabilités au niveau de l'union. Si cette initiative vise à renforcer la connaissance partagée de la menace, elle suscite de graves réserves quant à son application aux secteurs d'activité les plus protégés, tels que la défense ou les opérateurs d'importance vitale. Du point de vue de l'ANSSI, la centralisation de données techniques ultra-sensibles concernant des vulnérabilités non encore corrigées au sein d'une plateforme unique européenne constitue en soi une cible stratégique majeure. L'article 16, alinéa (b), charge en effet l'ENISA de développer une « capacité commune de gestion des vulnérabilités » au niveau de l'Union. Le Considérant 39 justifie cette centralisation par la volonté d'éviter la duplication des efforts, mais elle instaure paradoxalement un point de défaillance unique hautement stratégique pour les intérêts nationaux. L'existence d'un tel répertoire centralisé crée un risque de compromission globale qui pourrait exposer nos infrastructures critiques nationales avant même la mise en œuvre des mesures de remédiation. La maîtrise souveraine de l'information sur les vulnérabilités affectant les actifs les plus critiques doit impérativement rester sous le contrôle exclusif de l'autorité nationale de sécurité, afin d'éviter toute divulgation prématurée ou inappropriée susceptible de porter atteinte aux intérêts fondamentaux de la nation. Une telle centralisation risquerait de diluer les responsabilités et d'affaiblir l'efficacité de la réponse nationale en cas de crise cyber. Par ailleurs, et c'est un point essentiel d'incohérence, la création de cette base de données unique européenne va à l'encontre même de la philosophie de décentralisation et de proportionnalité promue par la directive NIS2.

Une inquiétude similaire entoure les nouvelles prérogatives de l'ENISA en matière de certification des compétences individuelles (*Cybersecurity Skills Academy*). Les articles 19 à 23 du projet confèrent à l'agence européenne le pouvoir de développer des schémas d'attestation des compétences et d'autoriser directement les prestataires de formation. Cette centralisation au niveau européen risque de court-circuiter les autorités nationales et les référentiels existants, à l'instar de SecNumedu en France, qui ont fait leurs preuves pour structurer les écosystèmes éducatifs et professionnels locaux. L'ENISA devrait s'appuyer sur les cadres nationaux plutôt que de chercher à réguler directement le marché de la formation et de la certification des professionnels au sein de chaque État membre.

Dans ce contexte, le rôle de l'ENISA doit demeurer celui d'un catalyseur facilitant la coordination et le partage d'informations entre les États membres, et non celui d'une autorité de substitution. L'agence européenne n'a pas vocation à diluer la compétence des entités nationales d'excellence pour pallier le sous-investissement chronique ou les politiques permissives de certains de nos partenaires européens. Comme l'ont amplement démontré les travaux récents de la Commission supérieure du numérique et des postes lors des auditions liées à la transposition de la directive NIS 2, les entreprises, les administrations et les collectivités territoriales expriment un besoin vital d'accompagnement au plus près du terrain. Cette réalité opérationnelle justifie au contraire un renforcement continu des moyens de l'ANSSI et de ses délégations régionales.

Enfin, une vigilance toute particulière doit être portée sur l'évolution du modèle de financement de l'agence européenne. Le projet estime le budget de l'ENISA à 341 millions d'euros sur la période 2028-2034, soit une moyenne annuelle de 49 millions d'euros. Cette forte augmentation budgétaire serait alimentée en partie par l'instauration de nouvelles redevances prélevées directement auprès des acteurs économiques pour la délivrance d'autorisations et la maintenance des schémas de certification. Il est impératif de s'assurer que ce nouveau mécanisme de taxation européenne ne crée pas un effet d'éviction au détriment des budgets alloués aux agences nationales, et surtout qu'il n'alourdisse pas la charge financière des entreprises qui cherchent vertueusement à élever leur niveau de sécurité et à se mettre en conformité.

Recommandation n°5 : s'opposer fermement à l'article 16 du projet de règlement prévoyant la centralisation des vulnérabilités non corrigées au sein d'une base de données européenne gérée par l'ENISA, afin de préserver la maîtrise souveraine de l'ANSSI sur les failles affectant les infrastructures critiques nationales.

Recommandation n°6 : défendre un positionnement de l'ENISA strictement limité à la coordination et au partage d'informations, en bloquant tout transfert de compétences opérationnelles de réponse aux incidents au détriment des CSIRT nationaux.

Recommandation n°7 : garantir que l'adoption du CSA2 permette à la France d'assurer le maintien de la qualification SecNumCloud délivrée par l'ANSSI, sauf si un schéma européen de certification de sécurité offrant le même niveau de protection, notamment en termes d'immunité aux législations non européennes à portée extraterritoriale, était adopté.

Recommandation n°8 : amender les articles 19 à 23 pour imposer que la *Cybersecurity Skills Academy* s'appuie sur la reconnaissance mutuelle des référentiels nationaux existants, tels que SecNumedu en France, plutôt que sur la création d'un mécanisme européen d'autorisation directe des prestataires de formation.

Recommandation n°9 : exiger que l'introduction de nouvelles redevances prélevées directement auprès des acteurs économiques pour la délivrance d'autorisations et la maintenance des schémas de certification ne crée pas un effet d'éviction au détriment des budgets alloués aux agences nationales

et que ce mécanisme n'alourdisse pas la charge financière des entreprises qui souhaitent renforcer leur niveau de sécurité et se mettre en conformité.

V. L'impératif de cohérence dans la définition des risques de cybersécurité

Pour comprendre l'enjeu, il convient de revenir aux fondamentaux de la doctrine en la matière : la sécurité numérique repose sur trois piliers indissociables, souvent désignés par le triptyque DIC, pour disponibilité, intégrité et confidentialité. La confidentialité garantit que seules les personnes autorisées ont accès aux données. L'intégrité assure que l'information n'est ni modifiée ni altérée de façon illégitime. La disponibilité, enfin, permet aux systèmes et aux données d'être accessibles au moment précis où l'utilisateur en a besoin. Dans le cadre de l'analyse de risques légitimement menée par une entreprise ou une administration, tout événement susceptible de compromettre l'un de ces trois piliers est traité comme une menace de sécurité quelle qu'en soit l'origine.

Or, le projet de texte de la commission européenne tente d'introduire une distinction déroutante entre les risques qualifiés de techniques et ceux qualifiés de non techniques. Selon cette logique, une faille logicielle exploitée par un pirate serait un risque technique, tandis qu'une injonction juridique étrangère obligeant un prestataire à livrer secrètement mais légalement des données, notamment dans le cadre d'une activité de renseignement d'intérêt économique, serait considérée comme un risque non technique. Du point de vue d'une organisation utilisatrice qui doit protéger ses secrets industriels ou ses données sensibles et stratégiques, cette séparation est une pure fiction juridique car la conséquence opérationnelle est strictement identique : dans les deux cas, la confidentialité est rompue et le préjudice pour l'entreprise est total. Il en va de même pour la disponibilité si un service est coupé unilatéralement par un fournisseur pour obéir à une mesure de rétorsion diplomatique de son état national : pour l'utilisateur européen, il s'agit d'une rupture technique de sa continuité d'activité. La certification européenne ne peut donc pas être vidée de sa substance en ignorant ces vecteurs d'insécurité sous prétexte qu'ils ont une origine juridique ou étatique.

Cette dichotomie artificielle est gravée dans l'architecture même du texte. Le Considérant 77 affirme que le cadre de certification, le Titre III, doit se concentrer sur les risques techniques, tandis que le Considérant 129 relègue l'exposition à la juridiction d'un pays tiers au rang de risque « non technique ». Cette séparation prive les utilisateurs de la capacité d'attester techniquement de la confidentialité réelle de leurs données face aux lois extraterritoriales. Au contraire, l'exposition d'un prestataire à des législations à portée extraterritoriale doit être analysée comme une vulnérabilité structurelle, au même titre qu'un défaut de conception logicielle, venant altérer la performance de sécurité globale du service. Pour une entreprise européenne, une législation étrangère à portée loi extraterritoriale telle que la section 702 du FISA américain ou de l'article 7 de la loi chinoise sur le renseignement du 27 juin 2017 crée évidemment une vulnérabilité dans la chaîne de dépendance technique du service numérique qui y est soumis, ce qui en fait un défaut de sécurité opérationnelle à part entière et non un simple sujet géopolitique qui pourrait être laissé, sans garantie juridique, à la seule appréciation des États ou de la Commission européenne.

Recommandation n°10 : porter au niveau européen une définition de la cybersécurité ancrée sur les fondamentaux techniques (disponibilité, intégrité, confidentialité), en affirmant que toute législation étrangère permettant un accès secret aux données constitue une vulnérabilité technique à part entière.

Recommandation n°11 : refuser la dichotomie opérée par les considérants 77 et 129 du projet de règlement, qui exclut artificiellement l'exposition aux lois extraterritoriales du champ de l'évaluation technique de la conformité.

Recommandation n°12 : conditionner le soutien de la France au texte à la réintégration des risques de compromission légale d'origine étatique dans les grilles d'évaluation du Titre III relatif à la certification.

VI. Le paradoxe de la conformité impossible de l'article 80-1

L'article 80-1 du projet de règlement définit les objectifs de sécurité que chaque futur schéma de certification européen devra obligatoirement poursuivre. Cet article constitue à ce titre le socle de confiance de l'ensemble du dispositif. L'alinéa (v) de cet article impose notamment à tous services certifiés de « résister à tout événement » susceptible de compromettre la confidentialité, l'authenticité, l'intégrité ou la disponibilité des données et des traitements associés. La portée de l'expression « tout événement » est ici fondamentale car, en l'absence de restriction explicite aux seuls incidents d'origine technologique, elle inclut de facto les injonctions administratives ou judiciaires.

Cette rédaction crée une impasse juridique insurmontable pour les prestataires soumis à des législations extraterritoriales comme la section 702 du FISA américain ou l'article 7 de la loi chinoise sur le renseignement national du 27 juin 2017. L'impasse est d'autant plus manifeste que le premier point du Considérant 137 reconnaît explicitement que certains pays tiers imposent aux entités sous leur juridiction de rapporter les vulnérabilités logicielles à leurs propres autorités avant toute divulgation publique. Cette disposition étrangère rend juridiquement impossible pour un fournisseur de respecter l'obligation de transparence sur les incidents posée à l'alinéa (d) de l'article 80-1. Il faut rappeler que la section 702 du FISA permet aux agences de renseignement américaines d'exiger l'accès aux données des « non-US Persons » auprès des fournisseurs de cloud soumis au droit américain, sans mandat judiciaire. En effet, ces acteurs sont légalement contraints de coopérer avec leurs autorités de renseignement et ne peuvent, sans enfreindre leur propre droit national, « résister » à une telle injonction de livraison de données ou à un mécanisme d'interruption unilatérale de service. Nous en avons eu un exemple très concret avec les sanctions ayant frappé en 2025 des magistrats de la Cour pénale internationale, et notamment notre concitoyen le juge Nicolas Guillou.

Cette contradiction est exacerbée par la distinction artificielle que tente d'opérer le texte entre les risques dits « techniques » et les risques « non techniques ». En classant arbitrairement l'exposition à une juridiction tierce dans cette seconde catégorie, la Commission occulte la réalité opérationnelle des organisations pour lesquelles un accès secret à leurs données constitue une rupture technique de la confidentialité aussi grave qu'une intrusion cybercriminelle. En ignorant ce conflit de lois, le règlement organise sciemment une impossibilité de conformité : soit le fournisseur obtient un certificat en dépit d'une vulnérabilité juridique documentée, soit le certificat est délivré sur la base d'une capacité de résistance que le prestataire est structurellement incapable d'offrir.

Un tel dispositif place les dirigeants d'entreprises et d'administrations dans une situation d'insécurité juridique majeure, car il leur ferait croire à une protection inexistante, tout en les privant de l'information nécessaire à leur propre conformité réglementaire, notamment au titre des directives NIS 2 ou DORA. En outre, cette opacité contredit frontalement l'alinéa (d) de l'article 80-1, qui exige le signalement des accès non autorisés : l'application d'ordonnances de non-divulgation étrangères, les fameux « *gag orders* », rendrait juridiquement impossible pour le prestataire de respecter cette obligation de transparence envers ses clients européens et les autorités de contrôle.

Recommandation n°13 : demander une révision de l'article 80, paragraphe 1, afin de clarifier la manière dont les fournisseurs soumis à des lois telles que le FISA américain peuvent légalement respecter l'obligation de « résister à tout événement » compromettant la confidentialité.

Recommandation n°14 : conditionner le soutien de la France à l'adoption de tout schéma de certification à la garantie que les fournisseurs certifiés ne soient pas soumis à des ordonnances de non-

divulgation (*gag orders*), ces injonctions les rendant structurellement incapables de respecter l'obligation de signalement des accès non autorisés exigée à l'article 80, paragraphe 1, alinéa (d).

Recommandation n°15 : alerter le Conseil sur le risque juridique pesant sur les entreprises utilisatrices qui, en s'appuyant sur un certificat européen faussé, se retrouveraient en situation de non-conformité face à leurs propres obligations de gestion des risques au titre de NIS 2 et DORA.

VII. Un mécanisme de sécurité des chaînes d'approvisionnement (Titre IV) à parfaire

Le nouveau Titre IV du projet de règlement introduit un cadre destiné à sécuriser les chaînes d'approvisionnement des technologies de l'information et de la communication (TIC) au sein de l'Union européenne. Ce dispositif repose sur une logique de « police administrative » activable à la seule discrétion de la Commission européenne : après avoir mené des évaluations de risques, celle-ci pourrait désigner certains fournisseurs comme étant « à haut risque » et, par conséquent, interdire ou restreindre l'usage de leurs produits et services par les entités essentielles européennes. Si un tel mécanisme apparaît légitimement conçu et potentiellement efficace pour la protection d'infrastructures matérielles tangibles, comme les équipements de réseaux de télécommunication, il s'avère en revanche totalement inopérant lorsqu'il est appliqué au domaine des services de cloud.

La contradiction majeure de ce dispositif réside dans son caractère binaire et politique. Tant qu'un fournisseur n'est pas officiellement banni par la Commission, aucune garantie juridique d'immunité ne peut être exigée par les utilisateurs. Or, une désignation de type « haut risque » visant les grands fournisseurs de cloud américains n'aurait aucun sens d'un point de vue économique et diplomatique. Personne, en Europe, ne souhaite l'éviction de ces acteurs dont l'apport technologique demeure essentiel à la compétitivité et à la transformation numérique de notre économie. Par ailleurs, dans le contexte actuel des relations avec nos partenaires stratégiques, une telle décision serait perçue comme une mesure de rétorsion diplomatique catastrophique que personne n'appelle de ses vœux.

En l'état, ce dispositif place donc les entreprises et les administrations publiques dans une impasse. Il maintient le *statu quo* d'une exposition subie à des législations extraterritoriales sans donner au marché le moindre levier à valeur légal pour s'en prémunir. Pour le cloud, le besoin des bénéficiaires finaux de la certification ne réside pas dans le bannissement politique de fournisseurs majeurs, mais dans la liberté de pouvoir exiger et choisir, pour leurs données les plus sensibles et stratégiques, des environnements offrant de strictes garanties juridiques de confidentialité et de disponibilité. Faute de fournir cette prévisibilité et ces leviers de marché, le Titre IV manque son objectif de renforcement de la sécurité des traitements de données au profit d'une gestion purement discrétionnaire des risques géopolitiques. Cette incertitude est aggravée par le régime d'exemption prévu à l'Article 105 : une entité contrôlée par un pays tiers peut demander à être exemptée des interdictions. Cependant, avec un délai de réponse de 9 mois laissé à la Commission et des critères d'évaluation discrétionnaires, ce mécanisme renforce l'insécurité économique là où un label d'immunité optionnel et immédiat prescrit dans le Titre III offrirait une prévisibilité de marché indispensable.

L'insécurité juridique dans laquelle ce dispositif plonge les entreprises est d'autant plus inacceptable qu'elle est assortie de sanctions financières d'une sévérité inédite. L'article 115 du projet de règlement prévoit en effet des amendes pouvant atteindre 7 % du chiffre d'affaires mondial total de l'entreprise qui enfreindrait les interdictions liées aux fournisseurs désignés comme étant à haut risque. Faire peser un tel risque pénal et financier sur les seules organisations utilisatrices, tout en les privant des moyens juridiques et des labels de certification clairs pour exiger l'immunité de leurs fournisseurs en amont, constitue à tout le moins un sérieux motif de perplexité.

Pour sortir de cette impasse, une articulation structurelle entre le Titre III, dédié à la certification, et le Titre IV, dédié à la sécurité des chaînes d'approvisionnement, s'avère indispensable. Le régime d'exemption prévu à l'article 105 exige d'une entité qu'elle prouve l'efficacité de ses mesures d'atténuation contre l'ingérence étrangère. Or, c'est précisément l'objet d'un schéma de certification technique rigoureux. Dès lors, la validation technique et auditée obtenue via un label d'immunité au titre du Titre III constitue une preuve objective et suffisante pour lever les doutes inhérents à la logique de police administrative du Titre IV. Établir qu'un service certifié avec ce niveau de garantie est d'office exempté des restrictions d'approvisionnement créerait une passerelle de simplification majeure. Ce mécanisme de procédure accélérée, de type *fast-track* redonnerait une prévisibilité immédiate aux acteurs économiques : la confiance serait garantie *a priori* par la conformité technique et le marché, plutôt que d'être suspendue à une décision politique et administrative *a posteriori*.

Recommandation n°16 : démontrer l'inadéquation du Titre IV (logique de police administrative et de bannissement) pour le marché du cloud, et exiger la création de leviers de marché positifs permettant aux entreprises de choisir des solutions immunisées sans attendre une décision d'exclusion de la Commission.

Recommandation n°17 : modifier l'article 115 relatif aux sanctions pour s'assurer que les amendes pouvant atteindre 7 % du chiffre d'affaires mondial n'incombent pas aux seules entreprises utilisatrices, mais engagent conjointement la responsabilité des fournisseurs si une non-conformité étaient de leur fait.

Recommandation n°18 : réviser le mécanisme d'exemption de l'article 105 afin de réduire drastiquement le délai d'instruction de 9 mois et de définir des critères objectifs, garantissant ainsi la prévisibilité juridique des acteurs économiques, associé à un régime de maintien en conditions opérationnelles provisoire.

Recommandation n°19 : articuler le Titre IV avec le Titre III en établissant qu'un service disposant d'un certificat d'immunité validé est automatiquement exempté des restrictions liées à la chaîne d'approvisionnement.

VIII. La modularité des schémas de certification au service de la confiance et du marché

Pour appréhender la portée de la proposition de révision du Titre III du *Cybersecurity Act*, il est nécessaire de comprendre l'architecture des schémas de certification européens. Le cadre actuel prévoit que chaque produit ou service numérique peut être certifié selon trois niveaux d'assurance croissants : « basique », « substantiel » et « élevé ». Le niveau « basique » s'attache à minimiser les risques cyber élémentaires, principalement par une revue de la documentation technique. Le niveau « substantiel » vise à contrer des attaquants disposant de compétences limitées via des vérifications approfondies des fonctions de sécurité. Enfin, le niveau « élevé » exige une résistance aux cyberattaques sophistiquées menées par des acteurs disposant de ressources significatives, validée par des tests d'intrusion rigoureux. Or, depuis 2021, le projet de schéma européen de certification de sécurité des services cloud (EUCS) se trouve dans une impasse qui entrave la transformation numérique de l'Union. La CSNP avait d'ailleurs, en septembre 2024, publié un avis pour présenter et documenter cette situation inacceptable au regard des enjeux croissant de sécurité numérique dans le cloud. Ce blocage découle d'une opposition binaire et injustifiée entre une approche limitant le schéma à des critères technologiques et une proposition intégrant des exigences d'immunité aux lois étrangères au seul niveau « élevé ». Cette polarisation s'est muée en un antagonisme stérile fin 2023, à la suite d'injonctions diplomatiques visant à supprimer toute garantie de confiance juridique du futur cadre européen.

Face à cette paralysie, la CSNP estime qu'une sortie de ces débats réside dans une approche modulaire consistant à décorréler strictement les niveaux d'assurance technologiques des critères d'immunité aux législations non européennes à portée extraterritoriale. Plutôt que de cristalliser le débat sur un niveau spécifique, il convient de créer un label d'immunité optionnel et transversal pouvant être associé à chacun des trois niveaux technologiques, basique, substantiel ou élevé. Cette modularité est la seule à même de redonner le choix au marché et de répondre à la diversité réelle des besoins des entreprises et des administrations.

Bien que l'Article 71, paragraphe 3, présente la certification comme volontaire, il prévoit des dérogations si le droit de l'Union l'exige. Pour des secteurs régulés par DORA ou NIS 2, par exemple, la certification deviendra de facto l'unique moyen de prouver une gestion rigoureuse des risques. Sans label d'immunité, ces entités seront contraintes par la loi de se certifier sur un cadre qui ignore sciemment le risque d'ingérence étrangère, alors que celui-ci, dans le contexte international dans lequel évoluent l'économie européenne, n'a jamais été aussi prégnant.

Une organisation pourrait ainsi, selon sa propre analyse de risques, choisir un service de niveau « basique » techniquement suffisant, mais y adjoindre le label d'immunité pour héberger des données personnelles sensibles en cohérence avec le RGPD. À l'inverse, une entité traitant des données industrielles stratégiques pourrait opter pour un niveau technique « substantiel » complété par ce même label pour se prémunir contre des accès secrets fondés sur la section 702 du FISA américain ou la loi chinoise sur le renseignement du 27 juin 2017. En inscrivant directement ce mécanisme de label optionnel dans le règlement, l'Europe s'affranchirait des débats sur un niveau « High+ » pour se doter d'un outil de marché flexible et robuste, seul capable de garantir l'autonomie stratégique et la résilience de nos organisations sans exclure les acteurs technologiques majeurs.

Recommandation n°20 : déposer un amendement au Titre III visant à créer un label d'immunité aux législations extraterritoriales, conçu comme un module optionnel applicable de manière transversale aux niveaux d'assurance « basique », « substantiel » et « élevé ».

Recommandation n°21 : construire une coalition d'États membres favorables à cette approche modulaire, en démontrant qu'elle permet de sortir du blocage diplomatique sur le niveau « High+ » de l'EUCS tout en préservant l'ouverture du marché européen.

Recommandation n°22 : défendre le principe d'une adhésion volontaire à ce label modulaire, laissant à chaque entreprise ou administration la liberté de calibrer sa couverture juridique en fonction de sa propre analyse de risque au regard de la sensibilité de ses données.

Recommandation n°23 : garantir que ce label modulaire réponde par anticipation aux besoins des entités essentielles et importantes dans le cadre de la directive NIS2 et des organismes financiers soumis à DORA qui devront prouver l'étanchéité de leurs systèmes d'information dans le cadre des obligations futures imposées par le droit de l'Union.