COMMISSION SUPERIEURE DU NUMERIQUE ET DES POSTES

Avis n° 2025-09 du 29 septembre 2025
sur la mise en œuvre des dispositions relatives au Règlement (UE) 2024/2847 du Parlement européen et du conseil du 23 octobre 2024

Vu le Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 sur la cyber résilience, dit règlement CRA
Vu les articles l'article L. 43 et L. 125 du Code des postes et des communications électroniques
Vu l'article L2321-4-1 du Code de la défense

Après avoir auditionné les 17 et 18 septembre 2025 :

- M. Vincent Strubel, Directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)
- Mme Juliette Péron, Conseillère du directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)
- M. Alexandre Nègre, Conseiller juridique du secrétaire général de la défense et de la sécurité nationale (SGDSN)
- M. Gilles Brégant, Directeur général de l'Agence nationale des fréquences (ANFR)
- M. Christophe Digne, Directeur général adjoint de l'Agence nationale des fréquences (ANFR)
- M. Jean-Pierre Labe, Chef du service juridique de l'Agence nationale des fréquences (ANFR)

En application de l'article L. 125 du Code des postes et des communications électroniques (CPCE), la Commission supérieure du numérique et des postes (CSNP) a été saisie le 26 aout 2025 par le Secrétaire général de la défense et de la sécurité nationale (SGDSN) sur les dispositions de l'article 26 d'un projet de loi portant diverses dispositions d'adaptation au droit de l'Union européenne (DDADUE) visant à adapter le droit national au Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 sur la cyber résilience, dit règlement CRA.

Les dispositions soumises pour avis abrogent l'article L2321-4-1 du code de la défense et modifient l'article L. 43 du CPCE afin de confier à l'Agence nationale des fréquences (ANFR) de nouvelles prérogatives pour la mise en œuvre de ce règlement et l'autoriser à échanger, lorsque ses missions le nécessitent, des informations avec les services de l'Etat compétents.

Le bureau de la CSNP a désigné Mme Anne Le Hénanff, Députée du Morbihan et Vice-présidente de la CSNP, rapporteure de cet avis.

I. Eléments de contexte

Le règlement sur la cyberrésilience (CRA) vise à renforcer la cybersécurité dans toute l'Union européenne (UE) et établit un cadre pour garantir que les produits et services numériques sont sûrs dès leur conception, résilients contre les cybermenaces et capables de fournir une protection continue tout au long de leur cycle de vie.

Ce texte a pour vocation de relever les défis posés en matière de cybersécurité par la connectivité croissante des dispositifs numériques et l'augmentation des cyberattaques qui ont des répercussions importantes sur l'économie et la société.

Le règlement CRA s'applique à une large gamme de produits comportant des éléments numériques mis sur le marché de l'Union Européenne, quel que soit le lieu de leur fabrication, qui peuvent se connecter directement ou indirectement à d'autres dispositifs ou réseaux. Il s'applique notamment :

- aux produits matériels, notamment les dispositifs de l'internet des objets (IdO), les appareils domestiques intelligents, les systèmes de contrôle industriels, les micropuces,
- aux produits logiciels notamment les jeux vidéo, les applications, les programmes informatiques.

Le règlement CRA ne s'applique pas aux dispositifs médicaux déjà couverts par des règlements spécifiques de l'UE, aux produits destinés à l'aviation et à l'automobile régis par une législation sectorielle ainsi qu'aux équipements marins.

En application du CRA, les fabricants de ces produits et services couverts par le champ d'application, doivent intégrer la cybersécurité dans la conception et le développement des produits. Cela inclut, entre autres, des configurations de sécurité par défaut, des niveaux appropriés de mécanismes de chiffrement et de contrôle d'accès.

La mise en œuvre du CRA repose sur une évaluation des risques par les fabricants de produits et services entrant dans le champ d'application du CRA :

- Les fabricants sont tenus de procéder à une évaluation des risques et de la tenir à jour, et de mettre en œuvre des mesures pour remédier aux vulnérabilités identifiées au cours du cycle de vie du produit.
- Si les fabricants s'appuient sur des composants ou services tiers, ils doivent faire preuve de diligence raisonnable pour les intégrer dans leurs produits.
- Les fabricants doivent fournir une documentation claire et complète, comprenant une description des caractéristiques de cybersécurité du produit, des instructions pour une installation, une configuration et une utilisation en toute sécurité, des informations sur la

manière de signaler les vulnérabilités ainsi qu'une déclaration de conformité pour confirmer le respect du règlement.

- Les fabricants doivent signaler sans retard les incidents de cybersécurité graves et les vulnérabilités activement exploitées aux autorités nationales compétentes et à l'Agence de l'Union européenne pour la cybersécurité (ENISA) et informer les utilisateurs sur les risques potentiels et fournir des orientations pour les atténuer.
- Les fabricants sont tenus de fournir des mises à jour de sécurité pendant la période d'assistance du produit, qui doivent refléter la période d'utilisation prévue du produit.
- Les mises à jour doivent remédier aux vulnérabilités et garantir la sécurité continue du produit.

Le règlement confère également des responsabilités aux importateurs et aux distributeurs afin de s'assurer que les produits respectent les exigences en matière de cybersécurité :

- Les importateurs doivent vérifier que les fabricants ont respecté le règlement et s'assurer que les produits sont étiquetés et documentés correctement.
- Les distributeurs doivent s'assurer que les produits portent le marquage CE et que les informations et les instructions destinées aux utilisateurs ont été fournies, avant de les mettre à disposition sur le marché.
- Les produits porteront le marquage CE pour indiquer qu'ils sont conformes aux exigences du CRA.
- Les fabricants de pays non membres de l'UE doivent se conformer au règlement pour accéder au marché de l'UE, et pourraient ainsi influencer les normes mondiales en matière de cybersécurité.
-

La mise en œuvre du règlement est confiée aux autorités nationales de surveillance du marché qui contrôleront la conformité et effectueront des inspections.
Le règlement prévoit que la non-conformité pourra entraîner des sanctions importantes, dont:

- des amendes jusqu'à 2,5 % du chiffre d'affaires annuel mondial du fabricant;
- l'interdiction ou la limitation de la disponibilité d'un produit;
- la décision de retirer ou de rappeler un produit.

Le règlement CRA s'appliquera de manière progressive entre juin 2026 et décembre 2027 :

- la notification des organismes d'évaluation de la conformité s'appliquera à partir du 11 juin 2026.
- les obligations de signalement concernant les vulnérabilités activement exploitées et les incidents graves s'appliqueront à partir du 11 septembre 2026.
- les autres dispositions du CRA s'appliqueront le 11 décembre 2027.

II. Dispositions transmises pour avis à la CSNP

Article 26

I.- L'article L. 2321-4-1 du code de la défense est abrogé à compter du 11 septembre 2026.

II.- L'article L. 43 du code des postes et des communications électroniques est ainsi modifié :

1° Après le 3° du I quater, sont insérés deux alinéas ainsi rédigés :

« I quinquies. – L'Agence nationale des fréquences assure le contrôle du respect des dispositions du règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) n° 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828.

« Elle peut échanger avec les services de l'Etat compétents des informations, documents et données, dans la stricte mesure nécessaire à l'accomplissement de sa mission, sans que le secret des affaires ne soit opposable ni à l'agence, ni aux services de l'Etat concernés dans ce cadre. » ;

2° Au II :

a) Au premier alinéa, après les mots : « 34-9-3, », sont insérés les mots : « le contrôle de la mise sur le marché des produits mentionnés au I quinquies, » ;

b) Au 1°, après les mots : « 34-9-3 », sont insérés les mots : « ou des produits mentionnés au I quinquies » ;

c) A la première phrase du quatrième alinéa, après les mots : « 34-9-3 », sont insérés les mots : « , des produits mentionnées au I quinquies » ;

d) Au cinquième alinéa, après les mots : « 34-9-3 », sont insérés les mots : « ou des produits mentionnés au I quinquies » ;

3° Après le II bis du dernier alinéa, sont insérés cinq alinéas ainsi rédigés :

« II ter. – Lorsqu'elle constate un manquement aux dispositions mentionnés au I quinquies, l'Agence nationale des fréquences peut, après une procédure contradictoire, mettre en demeure, dans un délai qu'elle détermine, la personne responsable de se mettre en conformité avec ses obligations. Lorsque la personne responsable ne se conforme pas dans le délai imparti à la mise en demeure, l'agence peut, sans préjudice de la mise en œuvre des mesures de restriction ou d'interdiction prévues à l'article 54 du règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) n° 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828, prononcer à son encontre une amende administrative, dont le montant est proportionné à la gravité du manquement dans les conditions suivantes :

« 1° Le non-respect des exigences énoncées à l'annexe I du règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 précité et des obligations énoncées aux articles 13 et 14 du même règlement fait l'objet d'une amende administrative pouvant aller jusqu'à 15 millions d'euros ou, si l'auteur de l'infraction est une entreprise, jusqu'à 2,5 % de son chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent, le montant le plus élevé étant retenu ;

« 2° Le non-respect des obligations établies aux articles 18 à 23, à l'article 28, à l'article 30, paragraphes 1 à 4, à l'article 31, paragraphes 1 à 4, à l'article 32, paragraphes 1, 2 et 3, à l'article 33, paragraphe 5, et à l'article 53 du règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 précité fait l'objet d'une amende administrative pouvant aller jusqu'à 10 millions d'euros ou, si l'auteur

de l'infraction est une entreprise, jusqu'à 2 % de son chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent, le montant le plus élevé étant retenu ;

« 3° La fourniture d'informations inexactes, incomplètes ou trompeuses aux organismes notifiés et aux autorités de surveillance du marché en réponse à une demande fait l'objet d'une amende administrative pouvant aller jusqu'à 5 millions d'euros ou, si l'auteur de l'infraction est une entreprise, jusqu'à 1 % de son chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent, le montant le plus élevé étant retenu.

« Avant toute décision, l'agence informe par écrit la personne mise en cause de la sanction envisagée à son encontre, en lui indiquant qu'elle peut prendre connaissance des pièces du dossier et se faire assister par le conseil de son choix et en l'invitant à présenter, dans un délai qu'elle fixe qui ne peut être inférieur à un mois, ses observations écrites et, le cas échéant, ses observations orales. Passé ce délai, l'agence peut, par décision motivée, prononcer l'amende. La décision prononcée par l'agence peut être publiée aux frais de la personne sanctionnée. Toutefois, l'agence doit préalablement avoir informé cette dernière, lors de la procédure contradictoire mentionnée aux alinéas précédents, de la nature et des modalités de la publicité envisagée. Lorsque, à l'occasion d'une même procédure ou de procédures séparées, plusieurs sanctions administratives ont été prononcées à l'encontre du même auteur pour des manquements en concours passibles d'amendes dont le montant maximal excède 15 millions d'euros ou 2,5 % de son chiffre d'affaires pour une entreprise, ces sanctions s'exécutent cumulativement dans la limite du maximum légal le plus élevé. L'amende est recouvrée comme en matière de créances étrangères à l'impôt et au domaine. L'agence peut demander à la juridiction civile d'ordonner, le cas échéant sous astreinte, toute mesure de nature à mettre un terme aux manquements aux dispositions relatives à la mise sur le marché des produits mentionnés au I quinquies. Les modalités d'application du présent II ter sont fixées par décret en Conseil d'Etat. » ;

4° Au VII :

a) Le mot : « leur » est remplacé par le mot : « sa » ;

b) Les mots : « l'ordonnance n° 2021-650 du 26 mai 2021 portant transposition de la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen et relative aux mesures d'adaptation des pouvoirs de l'Autorité de régulation des communications électroniques » sont remplacés par les mots : « la loi n° XX du XX 202X portant diverses dispositions d'adaptation au droit de l'Union européenne en matière de XXX ».

III.- Les 1° et 2° du II entrent en vigueur le 11 juin 2026.

Le 3° du II entre en vigueur le 11 décembre 2027.

III. Discussion

L'article soumis pour avis à la CSNP poursuit plusieurs objectifs :

- Désigner les autorités nationales françaises en charge de notifier et de surveiller le marché des produits et services couverts par le règlement CRA. Le règlement CRA laisse en effet le choix à chaque pays membres de désigner ces autorités. Le gouvernement français a choisi de désigner l'ANSSI comme « autorité notifiante » et de désigner l'ANFR comme « autorité de surveillance du marché ».

- Préciser le plafond des amendes administratives applicables en cas de non-conformité des produits et services au règlement CRA.

- D'étendre l'application du règlement CRA en Nouvelle-Calédonie, en Polynésie française, dans les Terres australes et antarctiques françaises et à Wallis-et-Futuna, à Saint Barthélémy et Saint Pierre et Miquelon.

- D'abroger l'article L2321-4-1 du code de la défense dont les dispositions couvrent une partie des dispositions du règlement CRA et donc d'éviter de soumettre à deux textes différents les acteurs concernés.

➢ Sur la désignation de l'ANSSI en qualité d'autorité notifiante

Cette désignation n'appelle pas de réserve de la part des membres de la CSNP.

➢ Sur la désignation de l'ANFR en tant qu'autorité de surveillance de marché

Les membres de la CSNP s'interrogent sur la capacité de l'ANFR à exercer sa compétence de surveillance de marché dans un domaine, celui de la cyber-résilience, qui n'est pas son cœur de métier.

Les auditions ont mis en lumière que l'ANFR dispose déjà d'une solide expérience de surveillance de marché pour les objets radioélectriques (contrôles techniques, relevés de conformité, sanctions). Cette compétence pourrait être transposée au CRA, mais nécessitera un accompagnement important, notamment par l'ANSSI, ainsi que des moyens humains et budgétaires renforcés.

Les agents de l'ANFR disposent d'un profil technique reconnu, mais l'expertise juridique et cyber

devra être consolidée. À ce titre, la question des nouvelles compétences cyber confiées à l'ANFR mérite d'être clarifiée.

Il ressort que le choix du gouvernement qui a présidé à désigner l'Agence nationale des fréquences comme autorité de surveillance de marché est 1./ le fait qu'elle assure déjà une mission de surveillance de marché dans son champ de compétence et 2./ que le profil de ses agents, notamment des ingénieurs spécialisés dans le domaine des télécommunications, serait plus approprié que celui plus généralistes que celui des agents de la DGCCRF.

L'ANSSI a prévu un accompagnement des agents de l'ANFR pour l'exécution de ces missions de surveillance de marché.

En tout état de cause, ce choix pose la question des nouveaux moyens qui seront alloués à la bonne exécution de ces nouvelles missions.

- **Sur les moyens dont dispose l'ANFR pour exercer ces nouvelles compétences de surveillance du marché**

Ainsi que le mentionne l'étude d'impact transmise à la CSNP, ces nouvelles missions confiées à l'ANSSI et à l'ANFR vont générer un surcout et par conséquent des besoins financiers supplémentaires.

S'agissant des équipes dédiées à la surveillance du marché dans le cadre du CRA, l'ANFR évalue les besoins en Emplois temps plein entre 8 et 16 selon l'étendue des contrôles qui seront effectués.

En effet, lors des auditions, il a été indiqué que l'ANFR envisageait de cibler ses contrôles sur des « familles de produits », à raison de deux à cinq familles par an. Une telle approche est pragmatique mais suppose des moyens renforcés, car le nombre d'ETP proposé (8 à 16) semble très en deçà des besoins réels.

De plus, les réductions budgétaires et de personnel constatées ces deux dernières années interrogent sur la capacité effective de l'ANFR à assumer ces missions supplémentaires sans dotations nouvelles.

Aussi, ce nombre d'ETP parait sous-dimensionné au regard du nombre de produits à contrôler même dans l'hypothèse où ces contrôles seraient effectués en ciblant certaines familles de produits.

Le recours à des laboratoires privés pour effectuer tout ou partie des contrôles techniques à effectuer doit être également budgété.

- **Sur la nécessité d'une communication efficace auprès des fabricants, importateurs, distributeurs et usagers des produits et services soumis au CRA**

Les fabricants, fournisseurs et distributeurs de produits et services couverts par le champ d'application du CRA se comptent en milliers sur le seul territoire national.

Pour une application optimale du règlement CRA, il est essentiel qu'une campagne de communication soit mise en place dans les meilleurs délais pour informer ces acteurs du dispositif retenu par les autorités françaises.

Cette communication doit cibler non seulement les fabricants et distributeurs, mais aussi les consommateurs, afin de renforcer la confiance et la compréhension des enjeux de cybersécurité.

L'ANFR devra également travailler en articulation avec la DGCCRF, déjà impliquée dans des contrôles de conformité et de marquage CE, afin d'éviter les doublons et de mutualiser l'expertise.

- **Sur les plafonds des amendes établis par le projet de loi**

Le règlement prévoit que la non-conformité pourra entraîner des sanctions importantes, pouvant aller jusqu'à 2,5 % du chiffre d'affaires annuel mondial du fabricant.

Le projet de loi prévoit que le non-respect des dispositions du CRA peut faire l'objet d'une amende administrative pouvant aller jusqu'à 5,10 ou 15 millions d'euros selon la nature des infractions ou, si 'auteur de l'infraction est une entreprise, jusqu'à 1, 2 ou 2,5 % du chiffre d'affaires annuel mondial selon la nature de l'infraction.

Compte tenu des risques que font peser les produits ou services numériques ne répondant pas aux exigences du CRA sur le niveau de cyber-résilience global de nos sociétés, de nos concitoyens et de nos entreprises, ces montants paraissent appropriés dans la mesure où ils sont dissuasifs. Les auditions ont montré que la possibilité d'amendes substantielles est jugée comme un outil dissuasif important, notamment au regard des plafonds actuels de la directive RED (750 €). L'alignement sur les standards européens, en lien avec l'ANSSI, renforcera la crédibilité du dispositif français.

Néanmoins, les membres de la CSNP souhaitent attirer l'attention du gouvernement sur le fait que ces plafonds d'amendes vont constituer un changement d'échelle substantiel par rapport aux montants des amendes administratives actuellement décidées par l'ANFR et qu'il conviendra d'établir sans tarder des lignes directrices adaptées pour préciser les montants des amendes que pourra édicter l'ANFR.

- **Sur l'articulation avec les autorités compétentes de l'Union européenne**

Les membres de la CSNP considèrent que le règlement CRA constitue une avancée majeure dans la protection de nos concitoyens et de nos entreprises et considèrent que sa mise en œuvre doit

se faire avec diligence.

La possibilité de retrait du marché de produits ou services contrevenant aux dispositions du règlement CRA est une avancée substantielle. En effet, les auditions ont souligné l'importance d'agir face à l'arrivée massive de produits à bas coût, souvent importés, qui ne respectent pas les exigences cyber, ne sont pas mis à jour et inondent le marché. Leur retrait est un enjeu de sécurité mais aussi de crédibilité du dispositif.

Il a par ailleurs été rappelé que la décision de retrait d'un produit du marché, une fois prise par un État membre, est valable pendant trois mois sur l'ensemble du marché européen. Ce mécanisme constitue une avancée majeure mais suppose une coordination accrue entre autorités nationales pour éviter les incohérences.

Pour autant, les membres de la CSNP comprennent que tous les pays de l'Union européenne ne disposeront pas d'agences nationales opérationnelles comme le sont l'ANSSI et l'ANFR et qu'il serait inéquitable que l'application du règlement CRA repose sur quelques agences nationales pour contrôler les produits et services défectueux dans l'Union européenne.

- **Sur la suppression l'article L2321-4-1 du Code de la défense**

Les articles 13, 14 et le chapitre V du règlement CRA fixent des obligations en matière de communication de vulnérabilités contenues dans des produits qui sont susceptibles d'être notamment des logiciels qui ne sont pas compatibles avec le maintien l'article L. 2321-4-1 du Code de la défense. Cet article a en effet prévu une obligation d'information de l'ANSSI applicables aux éditeurs de logiciels constatant des vulnérabilités significatives sur leurs produits.

Dans la mesure ou le règlement CRA est d'harmonisation maximale, il n'est pas possible de maintenir de mécanismes et de faire peser sur les acteurs deux obligations parallèles de notification.

IV. Avis de la Commission supérieure du numérique et des postes

Sous réserve des observations formulées dans le présent avis, la CSNP rend un avis favorable sur l'article portant mise en œuvre des dispositions relatives au Règlement (UE) 2024/2847 du Parlement européen et du conseil du 23 octobre 2024