N° 110

SÉNAT

SESSION ORDINAIRE DE 2025-2026

13 mai 2026

RÉSOLUTION EUROPÉENNE PORTANT AVIS MOTIVÉ

sur la **conformité** *au* **principe** *de* **subsidiarité** *et de* **proportionnalité** *de la* **proposition** *de* **règlement** *du* **Parlement européen** *et du* **Conseil relatif** *à l'***Agence** *de l'***Union européenne** *pour la* **cybersécurité** (**ENISA**)*, au* **cadre européen** *de* **certification** *de* **cybersécurité** *et à la* **sécurité** *de la* **chaîne** *d'***approvisionnement** *des* **TIC***, et abrogeant le* **règlement** (**UE**) *2019/881* (**règlement** *sur la* **cybersécurité** *2*) - *COM*(*2026*) *11 final et de la* **proposition** *de* **directive** *du* **Parlement européen** *et du* **Conseil** *modifiant la* **directive** (**UE**) *2022/2555 en ce qui concerne l'***introduction** *de* **mesures** *de* **simplification** *et l'***alignement** *sur* [*la* **proposition** *de* **règlement** *sur la* **cybersécurité 2**] - *COM*(*2026*) *13 final*

Est devenue résolution du Sénat, conformément à l'article 73 octies *du Règlement du Sénat, la résolution adoptée par la commission des lois dont la teneur suit :*

Voir le numéro :

Sénat : 624 (2025-2026).

Vu l'article 88-6 de la Constitution,

Vu l'article 73 *octies* du Règlement du Sénat,

Vu la proposition de règlement du Parlement européen et du Conseil relatif à l'Agence de l'Union européenne pour la cybersécurité (ENISA), au cadre européen de certification de cybersécurité et à la sécurité de la chaîne d'approvisionnement des TIC, et abrogeant le règlement (UE) 2019/881 (règlement sur la cybersécurité 2), du 20 janvier 2026, COM(2026) 11 final,

Vu la proposition de directive du Parlement européen et du Conseil modifiant la directive (UE) 2022/2555 en ce qui concerne l'introduction de mesures de simplification et l'alignement sur [la proposition de règlement sur la cybersécurité 2], du 20 janvier 2026, COM(2026) 13 final,

Le Sénat émet les observations suivantes :

Le Sénat soutient l'objectif de renforcer la préparation et la résilience de la société et de l'économie de l'Union européenne en matière de cybersécurité, ainsi que l'objectif du développement et du renforcement de la main-d'œuvre dans le domaine de la cybersécurité ;

Cependant, il estime que – eu égard à l'importance de ces sujets pour la sécurité nationale – l'Union européenne doit veiller à agir de manière équilibrée et proportionnée ;

L'article 5 du traité sur l'Union européenne (TUE) stipule que l'Union européenne ne peut intervenir, en vertu du principe de subsidiarité, que « *si, et dans la mesure où les objectifs de l'action envisagée ne peuvent pas être atteints de manière suffisante par les États membres, mais peuvent l'être mieux, en raison des dimensions ou des effets de l'action envisagée, au niveau de l'Union* » ; il précise qu'en application du principe de proportionnalité, « *le contenu et la forme de l'action de l'Union n'excèdent pas ce qui est nécessaire pour atteindre les objectifs des traités* » ; ceci implique d'examiner, non seulement si l'objectif de l'action envisagée peut être mieux réalisé au niveau européen, mais également si l'intensité de l'action entreprise n'excède pas la mesure nécessaire pour atteindre l'objectif que cette action vise à réaliser ;

L'article 5 du protocole n° 2 sur l'application des principes de subsidiarité et de proportionnalité annexé au TUE et au traité sur le fonctionnement de l'Union européenne (TFUE) prévoit que « *les raisons permettant de conclure qu'un objectif de l'Union peut être mieux atteint au*

niveau de celle-ci s'appuient sur des indicateurs qualitatifs et, chaque fois que c'est possible, quantitatifs » ; ceci implique que les projets d'actes législatifs européens soient suffisamment motivés et circonstanciés ;

L'analyse d'impact qui précède la proposition de règlement COM(2026) 11 final précitée ne détaille pas les raisons du choix de l'option de « *réforme complète du mandat de l'ENISA* » en lieu et place d'amendements au mandat actuel défini dans 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) n° 526/2013 (règlement sur la cybersécurité). En conséquence, la motivation de cette proposition apparaît présenter des limites et ne permet pas la bonne compréhension des modifications envisagées au mandat de l'ENISA ;

Le Sénat rappelle, comme il l'avait fait dans sa résolution n° 25 (2017-2028), du 6 décembre 2017, portant avis motivé sur la conformité au principe de subsidiarité de la proposition de règlement relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) n° 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité), COM (2017) 477 final, ainsi que dans sa résolution n° 52 (2023-2024), du 19 janvier 2024, sur la proposition de règlement du Parlement européen et du Conseil établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir, COM(2023) 209 final, que la cybersécurité, de par l'importance qu'elle revêt pour la sécurité des États membres, relève par plusieurs aspects de la souveraineté nationale ;

La cybersécurité ne peut relever uniquement de l'article 114 du TFUE, qui porte sur le fonctionnement du marché intérieur. Dès lors qu'elle est fondamentale du point de vue de la sécurité nationale, elle relève également de l'article 4 du TUE qui stipule que l'Union européenne « *respecte les fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer son intégrité territoriale, de maintenir l'ordre public et de sauvegarder la sécurité nationale* » et précise : « *En particulier, la sécurité nationale reste de la seule responsabilité de chaque État membre* » ;

Pour atteindre les objectifs en matière de cyberrésilience et de renforcement des capacités des États membres, la Commission européenne propose de renforcer le mandat de l'ENISA (« *The European Union Agency*

for Cybersecurity » – « *ENISA* »), ce qui implique le renforcement de ses moyens financiers et humains ; Pour ce faire, demande est faite aux États membres de fournir chacun « *au moins deux agents de liaison* » en complément des experts nationaux détachés déjà mis à disposition auprès de l'ENISA (article 58). Ces agents étant issus des autorités nationales compétentes, et face au déficit d'experts techniques de la cybersécurité, cette mesure est de nature à centraliser l'expertise humaine au sein de l'ENISA, au détriment du renforcement de la main d'œuvre compétente dans les États membres, ce qui apparaît contraire à l'objectif poursuivi ;

Le Sénat estime que les États membres doivent tous disposer de capacités techniques et opérationnelles suffisantes en matière de cybersécurité et qu'il est bienvenu que l'ENISA les aide dans cette démarche, sans toutefois que l'ENISA se substitue aux capacités opérationnelles des États membres. Or, l'obligation de transferts de ressources humaines et de compétences du niveau national vers l'ENISA est de nature à contrarier les efforts de construction de capacités opérationnelles au sein des agences nationales ;

Le Sénat estime que le renforcement du mandat de l'ENISA ne doit pas se faire au détriment des prérogatives des États membres établies par les traités. Le rôle de l'ENISA doit ainsi rester cantonné à un soutien aux États membres, à la définition de standards techniques pour assurer qu'ils puissent appliquer les règles européennes et à l'animation des échanges d'information entre les États membres en matière de cybersécurité. En revanche, le mandat de l'ENISA ne saurait porter sur des compétences exercées par les autorités nationales, sur le plan opérationnel, notamment en matière de réponse aux incidents cyber, sans créer de la redondance et de la complexité, ni contrevenir aux principes de subsidiarité et de proportionnalité ;

À cet égard, le Sénat juge disproportionnée la proposition de créer un guichet unique au niveau de l'ENISA, en particulier eu égard à la menace des rançongiciels ;

Le Sénat estime en outre que certaines évolutions proposées en matière de certification (titre III) relèguent au second rang l'expertise des États membres et de leurs agences nationales compétentes, alors même que ce sont elles qui disposent de la connaissance des enjeux de terrain. À cet égard, le Sénat considère que l'ENISA devrait se fonder sur des référentiels nationaux existants qui – à l'instar du référentiel « SecNumedu » en matière de formation – ont fait leurs preuves, plutôt que de chercher à réguler directement les marchés concernés ;

Concernant la certification de sécurité des services *cloud*, compte tenu de l'impasse dans laquelle se trouve aujourd'hui le projet de schéma européen de certification de sécurité des services *cloud* (« *The European Union Cloud Services Scheme* » – « *EUCS* »), le Sénat estime que les référentiels nationaux existants (la qualification SecNumCloud, délivrée par l'Agence nationale de la sécurité des systèmes d'information – ANSSI –, pour la France) doivent pouvoir être préservés et pérennisés, dans l'attente de l'adoption d'un schéma européen de certification de sécurité offrant au moins le même niveau de protection, notamment en termes d'immunité aux législations non européennes à portée extraterritoriale ;

*

En conséquence, pour ces motifs, le Sénat considère que les propositions d'actes législatifs COM(2026) 11 final et COM(2026) 13 final précitées ne sont pas conformes à l'article 5 du TUE et au protocole n° 2 sur l'application des principes de subsidiarité et de proportionnalité annexé au TUE et au TFUE.

Devenue résolution du Sénat le 13 mai 2026.

Le Président,

Signé : Gérard LARCHER