



COMMISSION EUROPÉENNE

*Bruxelles, le 3.8.2018
C(2018) 5351 final*

*M. Gérard LARCHER
Président du Sénat
Palais du Luxembourg
15 rue de Vaugirard
F – 75291 PARIS CEDEX 06*

Monsieur le Président,

La Commission tient à remercier le Sénat pour son avis motivé sur la proposition de règlement du Parlement européen et du Conseil relatif à l'[Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information] 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.

Cette proposition s'inscrit dans le cadre d'un ensemble plus vaste de mesures ambitieuses qui visent à renforcer la cybersécurité globale de l'Union en s'attaquant à ce que la Commission considère comme les grandes priorités dans ce domaine: le renforcement de la résilience, la création d'un marché unique dans le domaine de la cybersécurité, une cyberdissuasion efficace au sein de l'Union européenne et le renforcement de la coopération internationale.

La proposition de doter l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information d'un mandat fort, permanent et ciblé s'appuie sur les principales réalisations de l'agence - dans le domaine de la coopération, du soutien au renforcement des capacités et de l'élaboration et de la mise en œuvre de politiques au niveau de l'Union - et sur les prescriptions du droit de l'Union, en particulier les missions importantes confiées à l'agence par la directive sur la sécurité des réseaux et des systèmes d'information (la «directive SRI»)¹. Parallèlement, l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information se voit confier plusieurs nouvelles responsabilités liées au cadre européen de certification de cybersécurité, à mettre en place, qui fait partie intégrante de la proposition.

¹ Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194 du 19.7.2016, p. 1).

Le renforcement de la confiance des utilisateurs dans le marché unique numérique par l'accroissement de la transparence des caractéristiques de sécurité des produits et services des technologies de l'information et de la communication est au cœur de la proposition formulée par la Commission concernant un cadre de certification à l'échelle de l'Union. Les nouvelles règles permettront aux entreprises européennes de ne soumettre chaque produit/service qu'à un seul processus de certification pour obtenir un certificat de cybersécurité qui serait valable dans toute l'Union européenne. L'approche volontaire épargnera des charges supplémentaires aux entreprises européennes et garantira la flexibilité nécessaire dans le secteur à l'évolution si rapide des technologies de l'information et de la communication.

La Commission se félicite que le Sénat partage son point de vue selon lequel il est nécessaire d'agir au niveau de l'Union pour renforcer les capacités européennes dans le domaine de la cybersécurité et de disposer d'un cadre européen unique pour la certification en matière de cybersécurité.

La Commission prend au sérieux les craintes exprimées par le Sénat au sujet du respect du principe de subsidiarité. Elle insiste sur le fait que les interdépendances entre les réseaux et les systèmes d'information sont telles que les mesures prises par les États membres à titre individuel sont très souvent insuffisantes pour réagir aux menaces et gérer les risques et les éventuelles conséquences de cyberincidents. Accroître la cyberrésilience de l'Union et susciter une plus grande confiance des utilisateurs dans le marché unique numérique, qui sont les principaux objectifs visés par la proposition, sont des questions d'intérêt commun pour l'Union.

Le champ d'application de la proposition est limité au fonctionnement du marché intérieur, dont sont explicitement exclues les questions relatives à la sécurité nationale, qui restent de la compétence exclusive des États membres. La Commission souligne également que sa proposition s'appuie sur les compétences et les expériences nationales et européennes existantes qui ont fait leurs preuves, lesquelles continueront de jouer un rôle fondamental à l'avenir.

L'avis du Sénat a été communiqué aux représentants de la Commission dans les négociations en cours avec les colégislateurs et servira à éclairer ces débats.

La proposition présentée par la Commission est actuellement soumise à la procédure législative associant le Parlement européen et le Conseil. La Commission a bon espoir qu'un accord pourra être conclu avant la fin de son mandat actuel, en 2019, sur la base des discussions constructives qui se déroulent actuellement avec les colégislateurs.

En réponse aux observations plus techniques figurant dans l'avis, la Commission vous invite à consulter l'annexe.

La Commission espère que ces précisions répondront aux questions soulevées par le Sénat et se réjouit, par avance, de la poursuite de notre dialogue politique.

Veillez agréer, Monsieur le Président, l'expression de notre haute considération.



Elzbieta Bienkowska
Membre de la Commission

Annexe

La Commission a examiné avec soin chacun des points soulevés par le Sénat dans son avis et a l'honneur d'apporter les précisions suivantes, groupées par thème.

En ce qui concerne l'objet de la proposition, les mesures relatives au mandat de l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information et à la mise en place du cadre européen de certification de cybersécurité visent des objectifs communs et sont étroitement liées. Au vu des nouvelles responsabilités que la proposition confie à l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information dans le domaine de la certification de cybersécurité, il est jugé essentiel que ce nouveau rôle de l'agence soit défini en liaison avec les dispositions relatives au cadre.

En ce qui concerne la compétence des États membres dans le secteur de la sécurité, la proposition exclut explicitement de son champ d'application les questions touchant à la sécurité nationale. Plus précisément, le mandat de l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information est établi sans préjudice des compétences des États membres en ce qui concerne la cybersécurité et, en tout état de cause, sans préjudice des activités relatives à la sécurité publique, à la défense et à la sûreté de l'État, et des activités de l'État dans les domaines du droit pénal (article 3, paragraphe 3, de la proposition). En outre, le cadre de certification proposé ne va pas à l'encontre des pratiques actuelles, ni ne les remet en question, pas plus qu'il n'abaisse les normes existantes. Les États membres conservent leur droit de réglementer le niveau de sécurité pour une catégorie de produits/services donnée qui n'est pas couverte par un système européen.

En ce qui concerne le mandat révisé de l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information, la proposition autorise l'agence à soutenir les travaux des États membres et des institutions de l'Union européenne en vue d'accroître la résilience collective de l'Union. Plus précisément, les missions confiées à l'agence en lien avec la coopération opérationnelle s'appuient sur les dispositions de la directive sur la sécurité des réseaux et des systèmes d'information [directive (UE) 2016/1148]. L'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information se voit confier a) le secrétariat du réseau des centres de réponse aux incidents de sécurité informatiques, b) la mise en œuvre des dispositions du règlement en vigueur concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information² (qui prévoit déjà la possibilité pour les États membres et l'Union européenne de demander de l'aide en cas d'atteinte à la sécurité ayant un impact significatif) et c) la mise en œuvre des nouvelles initiatives lancées au niveau de l'Union. Ces missions ne se substituent pas aux rôles et aux responsabilités des États membres ni ne les dupliquent. Au contraire, elles visent à aider les États membres à améliorer leur capacité à prévenir les incidents, à les déceler et à y faire face et à contribuer à la coopération

² Règlement (UE) n° 526/2013 du Parlement européen et du Conseil du 21 mai 2013 concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et abrogeant le règlement (CE) n° 460/2004, texte présentant de l'intérêt pour l'EEE (JO L 165 du 18.6.2013).

opérationnelle au niveau de l'Union, en particulier en ce qui concerne les questions transfrontières.

C'est dans ce même esprit que la proposition prévoit la possibilité pour deux États membres ou plus de demander à l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information d'apporter son concours ou de procéder elle-même à des enquêtes techniques ex post, dont la portée serait définie par les États membres concernés, en cas d'incidents ayant un impact important ou significatif.

En ce qui concerne les questions soulevées au sujet du cadre de certification de cybersécurité, la Commission a pleinement tenu compte des expériences nationales et européennes existantes qui ont fait leurs preuves et elle entend en tirer le meilleur parti dans le cadre à mettre en place à l'échelle de l'Union. La décision de confier à l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information un rôle important en matière de certification se fonde sur une analyse approfondie des options envisageables. La nécessité de disposer d'un organe de l'Union européenne indépendant, présent sur le terrain pour soutenir la mise en place et la gestion du cadre, est apparue clairement; il est également évident que l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information est le seul organe de l'Union européenne présentant ces caractéristiques. En outre, l'agence jouera certes un rôle dans l'élaboration des systèmes de certification, mais la mise en œuvre de ceux-ci, notamment les essais de produits en laboratoire, la délivrance des certificats, le suivi et le contrôle du respect des règles continueront de relever de la compétence des États membres et seront effectués au niveau national.

En ce qui concerne la gouvernance du cadre, la Commission propose que les États membres jouent un rôle fondamental par l'intermédiaire du Groupe européen de certification de cybersécurité institué dans la proposition, en proposant à la Commission l'élaboration des cadres de certification et en aidant l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information à élaborer et à contrôler les systèmes de certification, et dans le cadre de la procédure d'examen des actes d'exécution qui établiront chaque système.