COMMISSION EUROPÉENNE

Bruxelles, le 5.5.2024
C(2024) 3165 final

M. Jean-François RAPIN
Président de la commission
des affaires européennes du Sénat
Palais du Luxembourg
15, Rue de Vaugirard
F-75291 PARIS Cédex 06

cc. *M. Gérard LARCHER*
Président du Sénat
Palais du Luxembourg
15, Rue de Vaugirard
F-75291 PARIS Cédex 06

Monsieur le Président,

La Commission tient à remercier le Sénat pour son avis relatif à 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 (le «règlement sur la cybersolidarité») [COM(2023) 209 final].

Vu le contexte géopolitique actuel, l'Europe doit faire preuve d'unité, de solidarité et de détermination. Le paquet «cybersécurité» a été adopté le 18 avril 2023 afin de créer les mécanismes nécessaires pour garantir la cybersécurité et renforcer la coopération au niveau de l'Union face à l'augmentation des cybermenaces. Le règlement sur la cybersolidarité a pour objectif de mieux détecter les menaces et incidents de cybersécurité, de mieux s'y préparer et de mieux y réagir.

La Commission a examiné attentivement l'avis du Sénat et se félicite que ce dernier soutienne ces objectifs et partage le point de vue selon lequel il est nécessaire de doter l'Union européenne d'un cadre juridique solide et complet. La Commission se réjouit de pouvoir apporter des éclaircissements sur sa proposition.

Les débats entre la Commission et les colégislateurs, le Parlement européen et le Conseil, ont été conclus avec succès le 5 mars 2024. Bien que les précisions fournies portent sur la proposition initiale de la Commission, l'accord provisoire entre les colégislateurs a modifié certains des points soulevés dans l'avis du Sénat, qui avait été mis à la disposition des représentants de la Commission et alimenté les débats au cours des négociations des colégislateurs.

En espérant que les précisions fournies dans l'annexe répondront aux questions soulevées par le Sénat, la Commission se réjouit, par avance, de la poursuite du dialogue politique.

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

Maroš Šefčovič
Vice-président exécutif

Thierry Breton
Membre de la Commission

AMPLIATION CERTIFIÉE CONFORME
Pour la Secrétaire générale

Martine DEPREZ
Directrice
Prise de décision & Collégialité
COMMISSION EUROPÉENNE

Annexe

La Commission salue les observations détaillées formulées par le Sénat sur le règlement sur la cybersolidarité, qui ont apporté une contribution importante au dialogue en cours avec les États membres. La Commission souhaite formuler les remarques suivantes.

En ce qui concerne l'absence d'analyse d'impact au moment de son adoption, la Commission tient à souligner que le règlement sur la cybersolidarité proposé se fondait sur des actions de nature préparatoire ou temporaire qui ont déjà été lancées et sont déjà soutenues dans le cadre du règlement établissant le programme pour une Europe numérique, lequel a fait l'objet d'une étude d'impact spécifique[1]*. Il s'agit notamment de la demande de mise en place de centres d'opérations de sécurité nationaux et transfrontières au titre du programme pour une Europe numérique et du programme de soutien à court terme prévu par l'Agence de l'Union européenne pour la cybersécurité (ENISA) en matière d'action de soutien cyber à la préparation et la réaction aux incidents. Le règlement sur la cybersolidarité proposé permettrait de soutenir ces actions à long terme et de renforcer ainsi la solidarité et la coordination au niveau de l'UE. Les actions seront soutenues par le programme pour une Europe numérique et sont conformes à la gouvernance et au budget fixés dans le règlement relatif au programme pour une Europe numérique. Comme expliqué dans son exposé des motifs, la proposition de règlement sur la cybersolidarité n'avait pas d'incidences administratives ou environnementales notables au-delà de celles déjà évaluées dans le cadre de l'analyse d'impact du règlement relatif au programme pour une Europe numérique. La proposition ne visait pas à parvenir à une harmonisation ni à imposer de nouvelles obligations réglementaires, mais à diriger les financements de l'UE dans le domaine de la cybersécurité vers des actions à fort impact et à renforcer notre capacité collective à nous défendre contre les cybermenaces qui se font de plus en plus sérieuses.*

S'agissant des préoccupations du Sénat relatives aux compétences des États membres dans le domaine de la sécurité et de la défense nationales, il convient de noter que les actions proposées n'avaient pas d'incidence sur les responsabilités des États membres en matière de sécurité nationale ni sur leurs compétences en ce qui concerne la sécurité publique et la prévention et la détection des infractions pénales ainsi que les enquêtes et les poursuites en la matière. Il convient d'interpréter la proposition conformément aux dispositions du TFUE. L'expression «responsabilité première» dans le texte de la proposition faisait référence aux responsabilités et aux compétences en ce qui concerne la sécurité publique et dans le domaine de la prévention et de la détection des infractions pénales, ainsi que des enquêtes et des poursuites en la matière.

La proposition prévoyait une dérogation au principe d'annualité budgétaire énoncé dans le règlement (UE, Euratom) 2018/1046 du Parlement européen et du Conseil (le

[1] Règlement (UE) 2021/694 du Parlement européen et du Conseil du 29 avril 2021 établissant le programme pour une Europe numérique et abrogeant la décision (UE) 2015/2240 (JO L 166 du 11.5.2021).

«règlement financier»). Compte tenu du caractère imprévisible des cyberattaques, l'utilisation des ressources du mécanisme d'urgence dans le domaine de la cybersécurité est difficile à prévoir. La dérogation concerne toutes les actions relevant du chapitre III (mécanisme d'urgence dans le domaine de la cybersécurité) du règlement sur la cybersolidarité proposé. Les actions de préparation ont également été incluses dans cette dérogation, puisqu'il pourrait être nécessaire de les adapter afin d'améliorer la préparation aux nouveaux incidents et menaces en matière de cybersécurité.

La réaffectation des budgets entre les objectifs stratégiques du programme pour une Europe numérique, notamment l'objectif spécifique 4, aurait pour effet de limiter le nombre de certaines actions (mais pas de les annuler), notamment concernant les masters, en particulier ceux qui sont déjà couverts par Erasmus ou d'autres programmes. L'accord provisoire auquel les colégislateurs sont parvenus a réduit la réaffectation proposée à partir de l'objectif spécifique 4 du programme pour une Europe numérique.

En ce qui concerne l'éventuel double emploi entre le cyberbouclier européen proposé et le réseau des centres de réponse aux incidents de sécurité informatiques (CSIRT) déjà en place, ainsi que l'invitation du Sénat à renforcer les organes de coopération déjà en place, il convient de noter que le règlement sur la cybersolidarité proposé ne modifiait pas la gouvernance actuelle de l'écosystème de cybersécurité, mais s'insère plutôt dans celle-ci, en la renforçant. Cette gouvernance repose sur les acteurs existants et respecte pleinement leurs rôles et compétences en matière de gestion des crises de cybersécurité dans l'UE. Les actions du règlement sur la cybersolidarité compléteront les capacités nationales de détection des cybermenaces et des cyberincidents, ainsi que d'appréciation de la situation, de préparation et de réaction en la matière, sans faire double emploi avec celles-ci.

Les centres d'opérations de sécurité constituant le cyberbouclier européen, qui seront établis sur une base volontaire et au moyen de fonds de l'Union, ne feraient pas double emploi avec les structures d'échange d'informations et de coopération prévues par la directive révisée concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'ensemble de l'Union (SRI 2)[2]*, comme le réseau des centres de réponse aux incidents de sécurité informatiques. Le cyberbouclier européen a pour but d'améliorer l'appréciation de la situation dans l'UE en encourageant les centres d'opérations de sécurité nationaux et transfrontières à regrouper les informations et à partager les renseignements sur les cybermenaces de manière opérationnelle, en utilisant des outils et des infrastructures interopérables. Plutôt que de créer des doublons, le cyberbouclier européen compléterait le travail effectué par le réseau des centres de réponse aux incidents de sécurité informatiques, dont le principal objectif est d'assurer une coopération opérationnelle rapide et effective*

[2] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (JO L 333 du 27.12.2022).

entre les centres nationaux de réponse aux incidents de sécurité informatiques, notamment dans le domaine de la réponse aux incidents, comme souligné à l'article 15, paragraphe 3, point g), de la directive (UE) 2022/2555.

En ce qui concerne la sélection des fournisseurs de services de confiance, la proposition fixait un certain nombre de principes d'adjudication préliminaires à suivre lors de la passation de marchés de services pour la réserve de cybersécurité de l'UE. Elle établissait également un certain nombre de critères de sélection de ces fournisseurs de confiance, à inclure dans les documents de marché. Cela permettra de garantir que les entreprises sélectionnées pour fournir un service dans le cadre de la réserve de cybersécurité de l'UE respectent les niveaux les plus élevés possibles de sécurité et de confiance.

La Commission prend acte de la recommandation du Sénat d'inclure dans la réserve de cybersécurité de l'UE des prestataires ayant leur siège social dans un pays partie à l'accord sur les marchés publics de l'Organisation mondiale du commerce. À cet égard, il convient de noter que le programme pour une Europe numérique prévoit qu'en cas d'actions en matière de cybersécurité relevant de l'objectif spécifique 3 – Cybersécurité et confiance, pour des raisons de sécurité dûment justifiées, les appels d'offres peuvent être limités aux entités juridiques établies ou réputées établies dans les États membres et contrôlées par des États membres ou par des ressortissants d'États membres, ce qui, selon nous, est une disposition suffisamment souple mais qui garantit dans le même temps un niveau de sécurité approprié.

Le recours à des actes d'exécution prévu aux articles 12 et 13 concernant la réserve de cybersécurité de l'UE donnerait effet aux règles établies dans le règlement pour garantir des conditions de mise en œuvre uniformes. En particulier, les deux actes d'exécution proposés visent à déterminer les types et le nombre de services de réaction nécessaires pour la réserve de cybersécurité de l'UE et à détailler davantage les modalités d'attribution des services d'aide fournis par la réserve de cybersécurité de l'UE. Les deux actes d'exécution proposés ont pour but de garantir une application harmonisée et efficace des principales conditions nécessaires à la réalisation des objectifs de la réserve de cybersécurité de l'UE.

En ce qui concerne les préoccupations relatives aux doublons potentiels générés par le mécanisme d'analyse des incidents de cybersécurité, la Commission tient à souligner que la proposition ne prévoyait pas de nouvelle mission pour l'Agence de l'Union européenne pour la cybersécurité, mais fournit une description spécifique du format et des procédures de l'analyse. En particulier, l'action introduit la possibilité d'analyser des incidents de cybersécurité concrets en évaluant les causes et les conséquences de ces incidents ainsi que leur atténuation, après qu'ils se sont produits. En outre, le mécanisme s'appuiera sur la collaboration avec des acteurs du secteur privé, y compris des fournisseurs de services de sécurité gérés.
