



Conseil de
l'Union européenne

Bruxelles, le 20 avril 2021
(OR. en)

Dossier interinstitutionnel:
2018/0328(COD)

5628/2/21
REV 2 ADD 1

CYBER 13
TELECOM 25
COPEN 35
COPS 33
COSI 14
CSC 26
CSCI 13
IND 25
RECH 36
ESPACE 6
CODEC 92
PARLNAT 92

EXPOSÉ DES MOTIFS DU CONSEIL

Objet: Position du Conseil en première lecture en vue de l'adoption d'un
RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL établissant
le Centre européen de compétences industrielles, technologiques et de
recherche en matière de cybersécurité et le Réseau de centres nationaux
de coordination

- Exposé des motifs du Conseil
- Adoptée par le Conseil le 20 avril 2021

I. INTRODUCTION

1. Le 12 septembre 2018, dans le cadre de sa stratégie pour un marché unique numérique, la Commission a adopté et transmis au Conseil et au Parlement européen la proposition¹ de règlement du Parlement européen et du Conseil établissant le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination, qui a pour base juridique l'article 173, paragraphe 3, et l'article 188 du TFUE.
2. L'objectif de la proposition est d'aider l'UE à maintenir et à développer les capacités technologiques et industrielles en matière de cybersécurité nécessaires pour sécuriser son marché unique numérique. La proposition prévoit la création de structures à trois niveaux institutionnels: un Réseau de centres nationaux de coordination (niveau national), une communauté de compétences en matière de cybersécurité (au niveau des parties prenantes) et un Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité (au niveau de l'UE). Le Centre de compétences gèrera le soutien financier lié à la cybersécurité alloué au titre du budget de l'UE et facilitera les investissements conjoints de l'UE, des États membres et de l'industrie afin de renforcer la cybersécurité de l'UE.
3. Le 17 septembre 2018, la Commission a présenté la proposition au groupe horizontal "Questions liées au cyberspace" (ci-après "groupe"), qui a ensuite procédé, le 28 septembre 2018, à l'examen de l'analyse d'impact. L'examen de la proposition proprement dite au sein du groupe a débuté le 28 septembre 2018 sous la présidence autrichienne et s'est poursuivi sous les présidences roumaine, finlandaise, croate et allemande.
4. Le Comité économique et social européen (CESE) a adopté son avis² sur la proposition le 23 janvier 2019. Le CESE s'est félicité de l'initiative de la Commission, estimant qu'il s'agit d'une étape importante dans l'élaboration d'une stratégie industrielle en matière de cybersécurité et d'une mesure stratégique visant à parvenir à une autonomie numérique solide et globale.

¹ Document 12104/18.

² Document 5898/19.

5. Au sein du Parlement européen, le dossier a été attribué à la commission de l'industrie, de la recherche et de l'énergie (ITRE) et M^{me} Julia REDA (ITRE, Verts/ALE) a été nommée rapporteure. Le rapport a été adopté le 19 février 2019 par la commission ITRE et approuvé par le Parlement lors de la plénière de mars I 2019. Le 17 avril 2019, le Parlement a adopté sa position en première lecture, qui comportait 112 amendements à la proposition de la Commission, par 489 voix pour, 73 contre et 56 abstentions. À l'issue des élections européennes, M. Rasmus ANDRESEN (ITRE, Verts/ALE) a été nommé nouveau rapporteur.
6. Le 13 mars 2019, le Coreper a donné mandat³ pour entamer les négociations avec le Parlement européen. Cinq trilogues ont eu lieu depuis lors: les 13 et 20 mars 2019, sous la présidence roumaine, le 25 juin 2020, sous la présidence croate, et les 29 octobre et 11 décembre 2020, sous la présidence allemande.
7. Le premier trilogue s'est tenu le 13 mars 2019 à Strasbourg et n'a donné lieu à aucun débat de fond. Les deux parties ont présenté dans leurs propositions respectives leurs positions et les principales modifications proposées, et elles se sont mises d'accord sur les prochaines étapes et le calendrier. Les colégislateurs ont confirmé leur ferme volonté de parvenir à un accord dès que possible.
8. Au cours du deuxième trilogue, qui s'est tenu le 20 mars 2019 à Bruxelles, il a été procédé à l'examen des questions considérées comme politiques lors de la première réunion technique, à savoir principalement la mission et les tâches du Centre de compétences, le financement et le conseil de direction. La présidence roumaine a fondé son approche sur le mandat reçu pour le premier trilogue. Le deuxième trilogue a fait apparaître une attitude positive de part et d'autre, les colégislateurs ayant clairement fait preuve de flexibilité sur plusieurs questions et ayant donné des orientations au niveau technique pour que de nouveaux progrès puissent être réalisés sur le texte de compromis.

³ Document 7583/19.

9. Un mandat révisé de négociation avec le Parlement européen a été approuvé par le Coreper le 3 juin 2020⁴. Un troisième trilogue s'est tenu le 25 juin 2020, à la fin de la présidence croate, en vue d'informer le Parlement européen des principales modifications apportées au nouveau mandat du Conseil, l'accent étant mis sur 1) la mission, les objectifs et les tâches du Centre de compétences, 2) sa structure, 3) les dispositions financières et 4) la communauté de compétences en matière de cybersécurité.
10. Une question relative à la position du Conseil sur les droits de vote du conseil de direction du Centre qui était restée en suspens a été résolue au sein du Conseil sous la présidence allemande. Le 22 juillet 2020, le Coreper a adopté un mandat révisé clarifiant la portée du droit de veto de la Commission.
11. Une autre question en suspens concernant le siège du Centre de compétences a été résolue en marge du Coreper le 28 octobre 2020 par les représentants des gouvernements des États membres, qui se sont mis d'accord sur une procédure de sélection de ce siège⁵. La décision à cet égard a été prise par les représentants des gouvernements des États membres en marge du Coreper le 9 décembre 2020. Bucarest (Roumanie) a été choisie comme siège.
12. Dans le cadre du quatrième trilogue, qui s'est tenu le 29 octobre 2020, un large mandat a été donné au niveau technique pour que des compromis soient trouvés sur les questions en suspens. Lors de plusieurs réunions techniques, des compromis ont été trouvés sur la plupart des questions.
13. Au cours du cinquième et dernier trilogue, qui s'est tenu le 11 décembre 2020, le Conseil et le Parlement européen sont parvenus à un accord provisoire, conformément au mandat, qui a été renouvelé par le Coreper le 9 décembre 2020. Le 18 décembre 2020, le Coreper a approuvé le texte de compromis final tel qu'il a été approuvé lors du trilogue.

⁴ Document 8315/20.

⁵ Document 13405/20.

II. OBJECTIF

14. Cette proposition prévoit la création d'un Centre de compétences, qui serait le principal instrument de l'UE pour mettre en commun les investissements dans la recherche, la technologie et le développement industriel en matière de cybersécurité. Par ailleurs, il fournirait un soutien financier lié à la cybersécurité au titre du programme "Horizon Europe" et du programme pour une Europe numérique. Comme indiqué ci-dessus, la proposition prévoit également la création d'un Réseau de centres nationaux de coordination et d'une communauté de compétences en matière de cybersécurité.
15. Le Centre de compétences serait doté d'un conseil de direction composé de représentants des États membres et de la Commission, chargé de définir l'orientation générale des activités du Centre de compétences et de veiller à ce que celui-ci s'acquitte de ses tâches conformément au règlement. L'objectif du Centre serait d'assurer une coordination plus étroite entre la recherche et l'innovation ainsi que le déploiement de stratégies au niveau tant national que de l'UE, et de permettre aux États membres de prendre des décisions concernant leur contribution financière aux actions conjointes.
16. Le Centre de compétences serait en mesure:
 - i) de mettre en œuvre des actions de recherche et d'innovation (soutenues par le programme "Horizon Europe") ainsi que des actions de renforcement des capacités (soutenues par le programme pour une Europe numérique), dans le respect de la gouvernance susmentionnée (c'est-à-dire la Commission et les États membres);
 - ii) en liaison avec les États membres, de soutenir le développement et l'acquisition d'équipements, d'outils et d'infrastructures de données de cybersécurité avancés en Europe et d'assurer un large déploiement des dernières solutions de cybersécurité dans l'ensemble des secteurs économiques; à cette fin, le Centre de compétences serait également en mesure de faciliter l'acquisition partagée de capacités pour le compte des États membres.

III. ANALYSE DE LA POSITION DU CONSEIL EN PREMIÈRE LECTURE

A. PROCÉDURE

17. Le Parlement européen et le Conseil ont mené des négociations en vue de conclure un accord au stade de la position du Conseil en première lecture ("accord en deuxième lecture anticipée"). Le texte de la position du Conseil en première lecture reflète le compromis global auquel sont parvenus les deux colégislateurs, avec le soutien de la Commission.

B. SYNTHÈSE DES PRINCIPAUX POINTS

18. Les principales modifications par rapport à la proposition initiale de la Commission, qui ont été approuvées par les deux colégislateurs, sont les suivantes:
- 1) une formulation de compromis a été intégrée dans diverses dispositions afin d'aligner le texte sur les dispositions du règlement pour une Europe numérique et du règlement "Horizon Europe", étant donné que le Centre de compétences gèrera le soutien financier lié à la cybersécurité au titre du programme "Horizon Europe" et du programme pour une Europe numérique;
 - 2) la référence au siège du Centre de compétences qui avait été faite dans le dispositif du règlement (article 1^{er}) a été supprimée. En lieu et place de cette référence, un nouveau considérant (20) a été ajouté;
 - 3) un certain nombre de notions, assorties de définitions appropriées, ont été ajoutés, tels que "cybermenace", "action conjointe", "contribution en nature" et "pôle européen d'innovation numérique";
 - 4) une "stratégie" a été ajoutée, à savoir une stratégie globale et durable dans les domaines de l'industrie, des technologies et de la recherche en matière de cybersécurité, qui formule des recommandations stratégiques en vue du développement et de la croissance du secteur européen de la cybersécurité dans les domaines de l'industrie, des technologies et de la recherche et définit les priorités stratégiques pour les activités du Centre de compétences;

- 5) les tâches du Centre de compétences, qui étaient initialement définies dans un article unique, avec les objectifs, sont désormais énoncées dans un article spécifique et une distinction est établie entre les tâches stratégiques et les tâches de mise en œuvre dévolues au Centre;
- 6) le rôle de l'ENISA a été renforcé. L'ENISA sera observateur permanent au sein du conseil de direction du Centre de compétences et pourra fournir des avis et des contributions sur la rédaction de la stratégie et des programmes de travail annuel et pluriannuel;
- 7) de nouvelles dispositions ont été introduites en ce qui concerne les centres nationaux de coordination, notamment pour ce qui a trait à leur désignation et à l'évaluation réalisée par la Commission;
- 8) les tâches du conseil de direction ont été précisées, notamment en ce qui concerne l'adoption de la stratégie et des programmes de travail annuel et pluriannuel;
- 9) les règles de vote du conseil de direction du Centre de compétences ont été modifiées et le principe "un membre, une voix" a été établi, au lieu de la disposition initiale de la proposition de la Commission, qui prévoyait que l'UE devait détenir 50 % des droits de vote. Toutefois, pour certaines décisions liées à l'exécution du budget de l'Union, ainsi qu'en ce qui concerne le programme de travail annuel, le programme de travail pluriannuel et la méthode de calcul des contributions des États membres, la Commission disposera de 26 % des droits de vote. Le conseil de direction adoptera ses décisions à la majorité d'au moins 75 % des votes de l'ensemble de ses membres;
- 10) le comité consultatif industriel et scientifique est devenu le groupe consultatif stratégique, qui fournira des conseils sur la base d'un dialogue régulier entre le Centre de compétences et la communauté de compétences en matière de cybersécurité;
- 11) la communauté de compétences en matière de cybersécurité sera composée d'organismes/organisations collectifs et n'inclura pas de personnes; à titre de compromis, le Centre de compétences et ses organes pourront recourir à l'expertise de particuliers et de personnes physiques en tant qu'experts ad hoc;

12) de nouveaux articles ont été ajoutés sur l'équilibre entre les hommes et les femmes (article 35) et sur la personnalité juridique du Centre de compétences (article 39).

IV. CONCLUSION

19. La position du Conseil en première lecture reflète le compromis global auquel sont parvenus le Conseil et le Parlement européen, avec le soutien de la Commission.
 20. Le Conseil estime que sa position en première lecture représente un ensemble équilibré et que, une fois adopté, le nouveau règlement jouera un rôle essentiel dans la poursuite du développement des capacités technologiques, industrielles et de recherche de l'UE en matière de cybersécurité.
-