Conseil de
l'Union européenne

Bruxelles, le 17 mai 2016
(OR. en)

Dossier interinstitutionnel:
2013/0027 (COD)

5581/1/16
REV 1 ADD 1

TELECOM 7
DATAPROTECT 6
CYBER 4
MI 37
CSC 15
CODEC 84
PARLNAT 154

EXPOSÉ DES MOTIFS DU CONSEIL

Objet:	Position du Conseil en première lecture en vue de l'adoption de la DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union - Exposé des motifs du Conseil - Adoptée par le Conseil le 17 mai 2016

dde/sc

I. INTRODUCTION

1. La Commission a présenté le 12 février 2013 sa proposition de directive du Parlement européen et du Conseil concernant des *mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union* (ci-après dénommée "la directive"), qui a pour base juridique l'article 114 du TFUE.

2. Le Comité économique et social européen a adopté son avis le 22 mai 2013 et le Comité des régions a adopté le sien les 3 et 4 juillet 2013.

3. Le Parlement européen a voté sa résolution législative en première lecture le 13 mars 2014[1], adoptant 138 amendements.

4. Le Conseil et le Parlement européen ont entamé des négociations en vue de parvenir à un accord en deuxième lecture anticipée en octobre 2014. Les négociations ont été clôturées avec succès le 7 décembre 2015, le Parlement européen et le Conseil parvenant à un accord provisoire sur un texte de compromis.

5. Le 18 décembre 2015, le Comité des représentants permanents a confirmé le texte de compromis de la directive, tel qu'il avait été approuvé par les deux institutions.

6. La présidence de la commission IMCO du Parlement européen a informé la présidence du Comité des représentants permanents par lettre du 28 janvier 2016 que, dans le cas où le Conseil transmettrait formellement sa position au Parlement européen dans les termes convenus, sous réserve de la vérification du texte par les juristes-linguistes, elle recommanderait à la plénière que la position du Conseil soit approuvée en deuxième lecture sans amendement.

7. Le 29 février 2016, le Conseil a confirmé son accord politique concernant le texte de compromis de la directive.

---

[1] Résolution législative du Parlement européen du 13 mars 2014 sur la proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information (SRI) dans l'Union.

II. OBJECTIF

8. Il ressort du résultat des négociations que la directive établit des mesures visant à assurer un niveau commun élevé de sécurité des réseaux et des systèmes d'information dans l'Union européenne afin d'améliorer le fonctionnement du marché intérieur.

III. ANALYSE DE LA POSITION DU CONSEIL EN PREMIÈRE LECTURE

A. Contexte général

9. À l'issue du vote en plénière, le Parlement européen et le Conseil ont mené des négociations en vue de conclure, sur la base de la position du Conseil en première lecture, un accord en deuxième lecture que le Parlement puisse approuver tel quel. Le texte de la position du Conseil en première lecture reflète tout à fait le compromis intervenu entre les colégislateurs.

B. Principaux éléments

10. Les principaux éléments du compromis trouvé avec le Parlement européen sont exposés ci-dessous:

a. *Moyens disponibles au niveau national*

11. En vertu du compromis, les États membres ont certaines obligations relatives aux moyens disponibles au niveau national en matière de cybersécurité. Premièrement, les États membres sont tenus d'adopter une stratégie nationale définissant les objectifs stratégiques et les mesures politiques et réglementaires appropriées en vue de parvenir à un niveau élevé de sécurité des réseaux et des systèmes d'information et de le maintenir.

12. Deuxièmement, les États membres désignent une ou plusieurs autorités nationales compétentes en matière de sécurité des réseaux et des systèmes d'information chargées de contrôler l'application de la directive au niveau national.

13. Troisièmement, les États membres sont également tenus de désigner un guichet unique national en matière de sécurité des réseaux et des systèmes d'information exerçant une fonction de liaison pour assurer une coopération transfrontière entre les autorités des États membres, ainsi qu'avec les autorités pertinentes des autres États membres, le groupe de coopération et le réseau des CSIRT. Le guichet unique fournira également au groupe de coopération un rapport annuel concernant les notifications reçues.

14. Enfin, les États membres désignent une ou plusieurs équipes de réactions aux incidents touchant la sécurité informatique (ci-après dénommées "CSIRT") chargées de la gestion des incidents et des risques. Le texte de compromis prévoit dans son annexe I des obligations et des tâches incombant aux CSIRT.

b. *Coopération*

15. Aux fins de soutenir et de faciliter la coopération stratégique entre les États membres, de renforcer la confiance et de parvenir à un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, le texte de compromis prévoit l'institution d'un groupe de coopération. Ce groupe sera composé de représentants des États membres, de la Commission et de l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ci-après dénommée "ENISA") et se verra confier des tâches spécifiques énumérées dans le texte, telles que l'échange de meilleures pratiques et d'informations sur un certain nombre de questions ou que l'examen des capacités et de l'état de préparation des États membres.

16. En outre, le compromis prévoit la mise en place d'un réseau des CSIRT nationales afin de contribuer au renforcement de la confiance entre les États membres et de promouvoir une coopération opérationnelle rapide et efficace. Le réseau sera composé de représentants des CSIRT des États membres et de la CERT-EU et la Commission participera au réseau en qualité d'observateur. L'ENISA assurera le secrétariat et soutiendra activement la coopération entre les CSIRT. Le texte définit une liste de tâches imparties au réseau, telles que l'échange d'informations sur les services, les opérations et les capacités de coopération des CSIRT, le soutien aux États membres dans la gestion d'incidents transfrontières ou, dans certaines conditions, l'échange et l'évaluation d'informations liées à des incidents et aux risques correspondants.

c. *Exigences en matière de sécurité et de notification*

17. La directive fixe certaines obligations à deux types d'acteurs du marché, à savoir aux opérateurs de services essentiels et aux fournisseurs de services numériques.

18. L'annexe II de la directive répertorie un certain nombre de secteurs importants d'un point de vue social et économique, dont ceux de l'énergie, des transports, de la banque, des infrastructures des marchés financiers, de la santé, de la fourniture et de la distribution d'eau potable et des infrastructures numériques. Dans ces secteurs, les États membres identifieront, sur la base de critères précis énoncés dans la directive, les opérateurs de services essentiels.

19. L'annexe III de la directive énonce trois types de services numériques dont les fournisseurs devront se conformer aux exigences de la directive: les places de marché en ligne, les moteurs de recherche en ligne et les services d'informatique en nuage. Tous les fournisseurs de services numériques offrant les services mentionnés devront satisfaire aux exigences de la directive, à l'exception des micro et petites entreprises.

20. Les deux types d'acteurs du marché seront tenus de prendre des mesures organisationnelles et techniques en vue de gérer les risques qui menacent la sécurité des réseaux et systèmes d'information, ainsi qu'en vue de prévenir les incidents qui compromettent la sécurité de ces systèmes et d'en limiter l'impact. Par ailleurs, les incidents ayant un certain degré d'impact sur les services en question devront être notifiés aux autorités nationales compétentes ou aux CSIRT. La directive prévoit des critères destinés à définir le degré d'impact de tels incidents.

21. La directive adopte une approche différentiée en ce qui concerne les deux catégories d'acteurs. Les exigences en matière de sécurité et de notification imposées aux fournisseurs de services numériques sont moins strictes que celles appliquées aux opérateurs de services essentiels, ce qui reflète le degré de risque que peut représenter une interruption des services de ces derniers pour la société et l'économie. De plus, compte tenu du fait que les fournisseurs de services numériques opèrent souvent dans de nombreux États membres et afin d'assurer un niveau élevé d'harmonisation, la directive empêche les États membres d'imposer à ces fournisseurs d'autres exigences liées à la sécurité et aux notifications.

22. Le texte de compromis prévoit également que des entités qui n'ont pas été recensées en tant qu'opérateurs de services essentiels et qui ne sont pas des fournisseurs de services numériques peuvent notifier, à titre volontaire, certains incidents.

d. *Transposition*

23. Les États membres seront tenus de transposer la directive dans un délai de 21 mois à compter de sa date d'entrée en vigueur et disposeront de 6 mois supplémentaires pour le recensement de leurs opérateurs fournissant des services essentiels.

IV. CONCLUSION

24. La position du Conseil reflète fidèlement le compromis dégagé à l'issue des négociations entre le Parlement européen et le Conseil, avec l'accord de la Commission. Ce compromis est confirmé par la lettre adressée le 28 janvier 2016 par la présidence de la commission IMCO du Parlement européen au président du Comité des représentants permanents.