Conselho da
União Europeia

Bruxelas, 17 de maio de 2016
(OR. en)

5581/1/16
REV 1 ADD 1

Dossiê interinstitucional:
2013/0027 (COD)

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

NOTA JUSTIFICATIVA DO CONSELHO

Assunto:	Posição do Conselho em primeira leitura com vista à adoção de uma DIRETIVA DO PARLAMENTO EUROPEU E DO CONSELHO relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União - Nota justificativa do Conselho - Adotado pelo Conselho em 17 de maio de 2016

I. INTRODUÇÃO

1. Em 12 de fevereiro de 2013, a Comissão apresentou uma proposta de diretiva do Parlamento Europeu e do Conselho relativa a *medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União* (adiante designada por "a diretiva"), que tem como base jurídica o artigo 114.º do TFUE.

2. O Comité Económico e Social Europeu e o Comité das Regiões votaram os seus pareceres em 22 de maio de 2013 e 3-4 de julho de 2013, respetivamente.

3. O Parlamento Europeu votou a sua resolução legislativa em primeira leitura a 13 de março de 2014[1], tendo adotado 138 alterações.

4. Em outubro de 2014, o Conselho e o Parlamento Europeu encetaram negociações no intuito de chegarem a acordo no início da segunda leitura. As negociações foram concluídas com êxito em 7 de dezembro de 2015, tendo o Parlamento Europeu e o Conselho alcançado um acordo provisório sobre um texto de compromisso.

5. Em 18 de dezembro de 2015, o Comité de Representantes Permanentes confirmou o texto de compromisso da diretiva, na versão acordada pelas duas instituições.

6. Em 28 de janeiro de 2016, a Presidente da Comissão IMCO do Parlamento Europeu endereçou ao Presidente do Comité de Representantes Permanentes uma carta na qual declarava que, caso o Conselho transmitisse formalmente ao Parlamento Europeu a sua posição acordada, sob reserva de ultimação pelos juristas-linguistas, ela própria recomendaria ao plenário que, aquando da segunda leitura do Parlamento, aceitasse a posição do Conselho sem alterações.

7. Em 29 de fevereiro de 2016, o Conselho confirmou o seu acordo político sobre o texto de compromisso da diretiva.

---

[1] Resolução legislativa do Parlamento Europeu, de 13 de março de 2014, sobre a proposta de diretiva do Parlamento Europeu e do Conselho relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação (SRI) em toda a União.

II. OBJETIVO

8. Decorre das negociações que a diretiva estabelece medidas destinadas a alcançar um elevado nível comum de segurança das redes e dos sistemas de informação na União Europeia a fim de melhorar o funcionamento do mercado interno.

III. ANÁLISE DA POSIÇÃO DO CONSELHO EM PRIMEIRA LEITURA

A. Considerações gerais

9. No seguimento da votação em plenário, o Parlamento Europeu e o Conselho entraram em negociações tendo em vista chegar a acordo em segunda leitura com base numa posição do Conselho em primeira leitura que o Parlamento considere aceitável. O texto da posição do Conselho em primeira leitura reflete inteiramente o compromisso alcançado entre os colegisladores.

B. Questões fundamentais

10. Especificam-se em seguida os principais elementos do compromisso alcançado com o Parlamento Europeu:

a. *Capacidades nacionais*

11. Nos termos do compromisso, os Estados-Membros têm determinadas obrigações no que respeita às suas capacidades nacionais no domínio da cibersegurança. Em primeiro lugar, têm a obrigação de adotar estratégias nacionais que definam os objetivos estratégicos e as medidas regulamentares e políticas adequadas com vista a alcançar e manter um elevado nível de segurança das redes e dos sistemas de informação.

12. Em segundo lugar, os Estados-Membros devem designar uma ou mais autoridades nacionais competentes em matéria de segurança das redes e dos sistemas de informação para controlar a aplicação da diretiva a nível nacional.

13. Em terceiro lugar, os Estados-Membros têm também de designar um ponto de contacto único nacional para a segurança das redes e dos sistemas de informação, ao qual caberá exercer uma função de ligação para assegurar a cooperação transfronteiras das autoridades dos Estados-Membros com as autoridades competentes de outros Estados--Membros e com o grupo de cooperação e a rede de CSIRT. O ponto de contacto único apresenta também ao grupo de cooperação um relatório anual sobre as notificações recebidas.

14. Por último, os Estados-Membros designam uma ou mais equipas de resposta a incidentes de segurança informática (CSIRT) responsáveis pelo tratamento de incidentes e riscos. No anexo I do texto de compromisso estão previstas as obrigações a cumprir e as tarefas das CSIRT.

b. *Cooperação*

15. A fim de apoiar e facilitar a cooperação estratégica entre os Estados-Membros, desenvolver a confiança e garantir um elevado nível comum de segurança das redes e dos sistemas de informação na União, o texto de compromisso institui um grupo de cooperação. O grupo, constituído por representantes dos Estados-Membros, pela Comissão e pela Agência da União Europeia para a Segurança das Redes e da Informação (ENISA), será incumbido das funções específicas enumeradas no texto, como o intercâmbio de boas práticas e informações sobre diversas questões ou a discussão das capacidades e do grau de preparação dos Estados-Membros.

16. De acordo com o compromisso, é também criada uma rede de CSIRT nacionais a fim de contribuir para o desenvolvimento da confiança entre os Estados-Membros e promover uma cooperação operacional célere e eficaz. A rede será composta por representantes das CSIRT dos Estados-Membros e da CERT-UE; a Comissão participará na rede na qualidade de observadora. A ENISA assegura os serviços de secretariado e apoia ativamente a cooperação entre as CSIRT. O texto prevê uma lista das tarefas a desempenhar pela rede, como proceder ao intercâmbio de informações sobre os serviços, as operações e a capacidade de cooperação das CSIRT, ajudar os Estados-Membros a fazer face a incidentes transfronteiras ou, em determinadas condições, proceder ao intercâmbio e à discussão de informações relacionadas com incidentes e riscos conexos.

c. *Requisitos de segurança e notificação*

17. A diretiva estabelece determinadas obrigações que recaem sobre duas categorias de intervenientes no mercado: os operadores de serviços essenciais e os prestadores de serviços digitais.

18. No anexo II da diretiva são enumerados vários setores importantes para a sociedade e para a economia, nomeadamente a energia, os transportes, o setor bancário, as infraestruturas do mercado financeiro, a saúde, o fornecimento e distribuição de água potável e a infraestrutura digital. Os Estados-Membros identificarão os operadores de serviços essenciais nestes setores com base em critérios precisos definidos na diretiva.

19. No anexo III da diretiva são enumerados três tipos de serviços digitais cujos prestadores terão de cumprir os requisitos da diretiva: os mercados em linha, os motores de pesquisa em linha e os serviços de computação em nuvem. Todos os prestadores de serviços digitais que fornecem os serviços enumerados terão de cumprir os requisitos da diretiva, com exceção das microempresas e das pequenas empresas.

20. As duas categorias de intervenientes no mercado terão de tomar medidas organizacionais e técnicas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação e para impedir e reduzir ao mínimo o impacto dos incidentes que afetam a segurança desses sistemas. Além disso, os incidentes que tenham um determinado nível de impacto nos serviços em questão terão de ser notificados às autoridades competentes nacionais ou às CSIRT. A diretiva estabelece critérios para determinar o nível de impacto de tais incidentes.

21. A diretiva segue uma abordagem diferenciada no que respeita às duas categorias de intervenientes. Os requisitos de segurança e notificação são mais aligeirados para os prestadores de serviços digitais do que para os operadores de serviços essenciais, o que reflete o grau de risco que a perturbação destes serviços pode representar para a sociedade e a economia. Além disso, tendo em conta que os prestadores de serviços digitais operam frequentemente em vários Estados-Membros e que é necessário garantir um elevado nível de harmonização, a diretiva impede os Estados-Membros de impor outros requisitos de segurança e notificação a esses prestadores.

22. O texto de compromisso prevê também a possibilidade de as entidades que não tenham sido identificadas como operadores de serviços essenciais e não sejam prestadores de serviços digitais notificarem, a título voluntário, determinados incidentes.

d. *Transposição*

23. Os Estados-Membros serão obrigados a transpor a diretiva no prazo de 21 meses após a data da sua entrada em vigor e disporão de mais seis meses para identificar os seus operadores de serviços essenciais.

IV. CONCLUSÃO

24. A posição do Conselho reflete inteiramente o compromisso alcançado nas negociações entre o Parlamento Europeu e o Conselho, com o acordo da Comissão. Este compromisso é confirmado pela carta enviada pela Presidente da Comissão IMCO ao Presidente do Comité de Representantes Permanentes em 28 de janeiro de 2016.