Parecer do Comité das Regiões – Estratégia para a Cibersegurança

(2013/C 280/05)

COMITÉ DAS REGIÕES

— acolhe favoravelmente a estratégia para a cibersegurança da Comissão e a diretiva sobre a segurança das redes e da informação (SRI) e secunda o objetivo da estratégia de assegurar um ciberespaço aberto, seguro e protegido e de tornar o ambiente em linha na UE o mais seguro do mundo;

— considera urgente a existência de um pacote que reúna os trabalhos propostos e em curso nesta matéria e que contribuirá para o desenvolvimento de uma visão coordenada e estratégica para a Europa. Um tal pacote merece o apoio do Comité na medida em que assegura a coordenação, encoraja a cooperação, produz ações claras e determinadas, alcança um nível comum de proteção contra ciberataques, melhora a resistência das redes e dos sistemas informáticos perante as novas e emergentes ameaças à cibersegurança e reduz a fragmentação na UE;

— recomenda à Comissão que publique um plano de ação explicando a forma como os objetivos ambiciosos descritos no pacote funcionarão na prática. O plano de ação necessitará também de uma orientação para a avaliação e o cálculo do impacto da estratégia, a fim de averiguar se a cooperação é uma realidade e se estão a ser feitos progressos;

— salienta que o novo pacote deve ajudar a melhorar a prevenção, a deteção e a resposta aos incidentes informáticos e conduzir a uma melhor partilha de informação e coordenação entre os Estados Membros e a Comissão contra grandes incidentes informáticos. Para tal, será necessária uma verdadeira partilha de esforços entre os Estados Membros, as instituições da UE, os órgãos de poder local e regional, o setor privado e a sociedade civil.

Relator	Robert BRIGHT (UK-PSE), membro do Conselho Municipal de Newport
Texto de referência	Comunicação conjunta — Estratégia da União Europeia para a cibersegurança (JOIN(2013) 1 final) Proposta de diretiva relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (COM(2013) 48 final)

I. **RECOMENDAÇÕES POLÍTICAS**

O COMITÉ DAS REGIÕES

1. acolhe favoravelmente a estratégia para a cibersegurança da Comissão e a diretiva sobre a segurança das redes e da informação (SRI) e secunda o objetivo da estratégia de assegurar um ciberespaço aberto, seguro e protegido e de tornar o ambiente em linha na UE o mais seguro do mundo;

2. espera que o novo pacote de cibersegurança, que inclui a estratégia e a diretiva, «aumente a fasquia» e dê um contributo importante para o desenvolvimento de normas de cibersegurança em toda a UE, diminuindo a insegurança jurídica, aumentando a confiança e a segurança dos serviços em linha e reduzindo os custos e os encargos administrativos desnecessários para, assim, apoiar o mercado único digital e os objetivos da Estratégia Europa 2020;

3. considera urgente a existência de um pacote que reúna os trabalhos propostos e em curso nesta matéria e que contribuirá para o desenvolvimento de uma visão coordenada e estratégica para a Europa. Um tal pacote merece o apoio do Comité na medida em que assegura a coordenação, encoraja a cooperação, produz ações claras e determinadas, alcança um nível comum de proteção contra ciberataques, melhora a resistência das redes e dos sistemas informáticos perante as novas e emergentes ameaças à cibersegurança e reduz a fragmentação na UE;

4. apela às organizações, incluindo às autoridades públicas, que reconheçam que o combate à cibercriminalidade é uma luta contínua e que deem prioridade à ameaça gerada pelas perturbações e pelos ataques informáticos através da identificação de pontos vulneráveis e do desenvolvimento das capacidades organizacionais para gerir infrações. À medida que a Internet se torna uma presença cada vez mais importante na vida das pessoas, também a ameaça da cibercriminalidade aumenta e se expande paralelamente. A cibercriminalidade, sob todas as suas formas, representa uma nova e sofisticada ameaça em rápido desenvolvimento para os Estados-Membros, bem como para as organizações e os cidadãos da UE no século XXI, que além de se estar a tornar cada vez mais frequente e complexa, não conhece fronteiras;

5. reconhece os principais progressos que a UE tem registado até à data para proteger melhor os cidadãos dos crimes em linha, incluindo as propostas legislativas sobre os ataques aos sistemas informáticos e o lançamento de uma aliança mundial contra os abusos sexuais de crianças em linha. O pacote deve promover as ações anteriores, nomeadamente as que constam na Agenda Digital para a Europa de 2010 [1], e visar a construção de uma política robusta de ciberdefesa na Europa. Para este efeito, insta os colegisladores que debatem presentemente a Proposta de diretiva relativa a ataques contra os sistemas de informação [2] a chegarem rapidamente a acordo sobre a mesma;

6. apoia a intenção ambiciosa da estratégia, uma vez que pretende não só harmonizar as capacidades de cibersegurança dos Estados-Membros e reunir as várias vertentes do trabalho proposto e em curso para estabelecer normas comuns e condições de concorrência equitativas, mas também coordenar e assegurar a coerência entre três domínios políticos: controlo da aplicação, Agenda Digital e política de defesa, segurança e relações externas, cujas competências têm estado separadas;

7. considera que o pacote poderia beneficiar de dados coligidos pelos governos nacionais e deveria propor um conjunto de normas harmonizadas no domínio da segurança das redes e da informação;

8. acolhe favoravelmente a abordagem multilateral adotada no pacote para a definição da política. O pacote reconhece a importância da cooperação entre os setores público e privado e do alcance de uma verdadeira parceria, munida dos recursos adequados. Além disso, aspira à realização do mercado único digital da UE, através da criação de um ambiente digital em linha protegido, seguro e próspero para as empresas, os governos e os cidadãos;

[1] COM(2010) 245, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:PT:HTML

[2] COM(2010) 517, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:PT:PDF

9. congratula-se com as medidas propostas na diretiva, incluindo a recomendação de que os Estados-Membros adotem obrigatoriamente uma estratégia nacional em matéria de segurança das redes e da informação (SRI), criem equipas de resposta a emergências informáticas (CERT) para trabalharem em parceira com a Agência Europeia para a Segurança das Redes e da Informação (ENISA) e estabeleçam um mecanismo de cooperação claro entre os Estados-Membros e a Comissão para comunicarem alertas rápidos sobre riscos e incidentes através de uma infraestrutura segura. Estas medidas e a abordagem regulamentar adotada na diretiva deverão contribuir amplamente para melhorar a coerência, estabelecer um grau de preparação mínimo a nível nacional comum a todos os países e fomentar a ciberdefesa em toda a UE;

10. insta o Parlamento Europeu e o Conselho a adotarem rapidamente a proposta de diretiva sobre um elevado nível comum de segurança das redes e da informação em toda a União;

11. considera que o pacote seria beneficiado se incluísse mais informações sobre as formas de notificação e recolha de dados em matéria de cibercriminalidade nos Estados-Membros, bem como informações mais específicas sobre a forma como tais medidas são aplicadas. Será crucial estabelecer sistemas de notificação comuns e uma maior clareza sobre requisitos de notificação para evitar a insegurança e a falta de coerência na forma como as autoridades competentes a nível nacional em matéria de SRI determinam e calculam os incidentes informáticos que têm «impacto significativo». Também é imperativo que a criação de uma autoridade competente a nível nacional em matéria de SRI tenha em conta a divisão de competências nos Estados-Membros, especialmente nos países com estruturas profundamente federalizadas ou descentralizadas;

12. manifesta, por conseguinte, algumas reservas quanto a certos aspetos regulamentares e jurídicos do pacote, nomeadamente no que diz respeito à falta de clareza na definição dos critérios a cumprir para que um Estado-Membro seja autorizado a participar num sistema seguro de troca de informações, a uma melhor especificação dos eventos desencadeadores de um alerta rápido e à definição das condições em que os operadores de mercado e as administrações públicas são obrigados a notificar os incidentes. A inexistência de regras claramente estabelecidas é um obstáculo à segurança jurídica;

13. manifesta-se apreensivo quanto à possibilidade de a diretiva vir a gerar encargos regulamentares desnecessários para as empresas e os órgãos públicos. Dever-se-ão empreender todos os esforços no sentido de evitar a duplicação de regulamentação e assegurar que todas as regulamentações adicionais respeitarão o princípio da proporcionalidade. Isto será particularmente importante para as organizações que já estejam sujeitas a uma obrigação de notificação substancialmente semelhante à que se pretende adotar;

14. recomenda à Comissão que publique um plano de ação explicando a forma como os objetivos ambiciosos descritos no pacote funcionarão na prática. O plano de ação necessitará também de uma orientação para a avaliação e o cálculo do impacto da estratégia, a fim de averiguar se a cooperação é uma realidade e se estão a ser feitos progressos;

15. apela a todos os Estados-Membros para que desenvolvam estratégias nacionais de cibersegurança que complementem a nova estratégia da UE (até 2012, apenas dez Estados-Membros o tinham feito). É importante que as estratégias nacionais complementem a estratégia da UE, a fim de assegurar coerência. Também é essencial que as ações da UE complementem as estruturas e as boas práticas existentes nos Estados-Membros;

16. congratula-se com as ações que a UE pretende realizar futuramente para desenvolver as capacidades da UE em matéria de cibersegurança, incluindo o lançamento de um projeto-piloto para combater os *botnets* e o *malware*, o empenho no sentido de melhorar a cooperação entre as CERT, a ENISA e o Centro Europeu da Cibercriminalidade, o desenvolvimento de uma rede de centros de excelência para a cibercriminalidade nacionais e o lançamento de uma plataforma público-privada sobre soluções SRI para criar incentivos à adoção de soluções TIC (tecnologias da informação e da comunicação) seguras. Apoia igualmente a intenção da estratégia de reunir todas as partes interessadas para avaliar os progressos efetuados ao cabo de 12 meses;

17. sublinha que uma estratégia bem-sucedida de cibersegurança passa pela cooperação estreita entre as autoridades competentes de SRI e as autoridades policiais e judiciais. Para tal é extremamente importante a notificação sistemática dos incidentes que se suspeite terem uma origem criminosa grave às autoridades responsáveis;

Participação dos níveis local e regional

18. crê que as prioridades apresentadas no pacote estabelecem um bom equilíbrio e são adequadas. Entre elas, a proteção dos direitos fundamentais, dos dados pessoais e da privacidade, uma governação multilateral eficiente e a partilha de responsabilidades para assegurar a segurança são domínios em que os municípios e as regiões devem desempenhar um papel central enquanto detentores de informação do setor público;

19. propõe que as regiões sejam reconhecidas, a par dos Estados-Membros, como principais promotoras de uma cooperação mais estreita entre utilizadores e fabricantes de inovações no domínio das TIC nos diferentes quadros governamentais e administrativos, incluindo no âmbito da cibersegurança e da proteção dos dados;

20. salienta que o novo pacote deve ajudar a melhorar a prevenção, a deteção e a resposta aos incidentes informáticos e conduzir a uma melhor partilha de informação e coordenação entre os Estados-Membros e a Comissão contra grandes incidentes informáticos. Para tal, será necessária uma verdadeira partilha de esforços entre os Estados-Membros, as instituições da UE, os órgãos de poder local e regional, o setor privado e a sociedade civil;

21. reconhece que a luta contra as ameaças informáticas requer maiores recursos e sensibilização para os perigos da cibercriminalidade e para a necessidade de uma cibersegurança eficiente e adequada. No que toca à governação multilateral, uma forte abordagem em matéria de cibersegurança deve ter conta os órgãos de poder local e regional, que devem ser implicados de forma plena e eficaz na gestão das iniciativas relacionadas com as TIC;

22. está convicto de que, tendo em conta a ameaça que as violações da segurança representam para os serviços de utilidade pública, como sejam o aprovisionamento de água e de energia a nível local, os órgãos de poder local e regional têm um papel crucial a desempenhar no combate à cibercriminalidade, na recolha de dados informáticos e na proteção da segurança dos dados, na medida em que são utilizadores e detentores de muitos produtos e serviços de informação digitais. Estes órgãos encarregam-se cada vez mais da prestação, por exemplo, de serviços digitais aos cidadãos e às comunidades e de formação nas escolas sobre SRI. Os governos, incluindo os locais e regionais, são responsáveis por salvaguardar o acesso e a abertura, respeitar e proteger os direitos fundamentais em linha e manter a fiabilidade e a interoperabilidade da Internet;

23. sugere que, a bem de uma melhor regulamentação, e dadas as competências e o papel fundamental dos órgãos de poder local e regional atualmente no planeamento e na aplicação de todas as medidas no domínio das TIC (particularmente no quadro da privacidade, da proteção de dados e da cibersegurança), estas entidades sejam sistematicamente consultadas pelas instituições da UE e pelos Estados-Membros durante a conceção e aplicação de medidas que visam concretizar a Agenda Digital para a Europa. É efetivamente lamentável que não se tenham empreendido esforços específicos para recolher os pontos de vista dos órgãos de poder local e regional durante a elaboração da proposta de diretiva. O CR já manifestou claramente a sua disponibilidade para assistir a Comissão nas consultas pré-legislativas, nomeadamente no Protocolo de Cooperação entre o CR e a Comissão ([3]);

24. recomenda que se incluam, no artigo 14.º, n.º 1, da diretiva, medidas aplicáveis ao nível local e regional, que contemplem, por exemplo, a criação de um processo de avaliação e gestão dos riscos, o cumprimento da política sobre a segurança da informação, o reforço da sensibilização para as questões da cibersegurança e a melhoria da literacia digital e das competências neste domínio;

25. salienta que importa incentivar e desenvolver parcerias a nível infranacional entre todos os intervenientes pertinentes, com vista a criar ações coordenadas em prol da cibersegurança, que contribuam para as iniciativas neste domínio realizadas a nível nacional e da UE, a fim de combater a cibercriminalidade e de minimizar as consequências do furto financeiro direto ou da propriedade intelectual, da perturbação nas comunicações e dos danos causados a dados comerciais críticos;

Subsidiariedade e proporcionalidade

26. assinala que, regra geral, a proposta parece cumprir ambas as condições que garantem o respeito do princípio da subsidiariedade, nomeadamente, o facto de ser necessária uma iniciativa da UE e o facto de a tomada de medidas a nível europeu trazer um valor acrescentado. As ações propostas são necessárias porque dizem respeito a aspetos transnacionais que não podem ser devidamente regulamentados de forma isolada pelos Estados-Membros ou pelos órgãos de poder local e regional. Além disso, espera-se que estas ações produzam um benefício claro, em comparação com iniciativas isoladas a nível nacional, regional ou local, uma vez que, por exemplo, os dados são transferidos entre fronteiras nacionais — tanto internas como externas — com uma velocidade cada vez maior. Além disso, as obrigações regulamentares a nível da UE contribuirão sem dúvida para criar condições equitativas e colmatar lacunas legislativas;

27. acolhe favoravelmente o compromisso de base da diretiva para com os princípios da subsidiariedade e da proporcionalidade. Dado o caráter transfronteiriço dos incidentes e riscos no domínio da SRI, a melhor forma de alcançar os objetivos apresentados na diretiva é a nível europeu, conforme ao princípio da subsidiariedade. A investigação indica que os cidadãos da UE confiam em instituições como a Comissão para abordar a questão da proteção dos dados pessoais ([4]). Além disso, a diretiva também respeita, em geral, o princípio da proporcionalidade, uma vez que garante que o texto não vai além do necessário para alcançar os objetivos fixados. Existem, no entanto, preocupações em relação à conformidade com o princípio da proporcionalidade e com as estruturas de governação internas dos Estados-Membros, uma vez que para cada Estado-Membro apenas se prevê uma autoridade competente ou uma equipa nacional de resposta a emergências informáticas (CERT);

28. entende que, apesar de a base jurídica do pacote de medidas ser constituída pelos artigos 26.º e 114.º do TFUE, as ações propostas excedem o âmbito destes artigos, uma vez que a proposta abrange todos os sistemas de informação da administração pública, incluindo sistemas de informação internos, como a Intranet;

Carta dos Direitos Fundamentais

29. acolhe favoravelmente o compromisso da diretiva para com a Carta dos Direitos Fundamentais da União Europeia. Devem aplicar-se no universo em linha as mesmas normas, princípios e valores que a UE defende para o mundo físico. As TIC devem ter em conta as necessidades de todos os membros da sociedade, incluindo as pessoas em risco de exclusão social. Todos os utilizadores da Internet devem poder contar com normas mínimas aplicáveis a todo um leque de necessidades, que assegurem a fiabilidade, segurança, transparência, simplicidade, interoperabilidade e redução dos riscos e dos encargos. No interesse da proteção efetiva dos direitos fundamentais, da segurança jurídica e da manutenção da reserva de exame parlamentar, o Comité insta a que a diretiva contemple regras mais concretas para a definição, em termos de direito

([3]) Protocolo de Cooperação entre a Comissão Europeia e o Comité das Regiões, assinado em 16 de fevereiro de 2012, R/CdR 39/2012, pt. 7.

([4]) http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

substantivo, dos padrões de segurança das redes e da informação. Em especial, importa formular requisitos em matéria de direitos fundamentais e de proteção e segurança de dados para criar a segurança das redes e da informação;

30. frisa que as tentativas de proteger e defender os cidadãos em linha devem ser adequadamente equilibradas com os direitos, liberdades e princípios concedidos aos cidadãos pela Carta. O Comité acolhe favoravelmente a importância dada ao facto de as políticas para a informática se inserirem num quadro de valores fundamentais da UE. Conforme se afirmou em pareceres anteriores ([5]), será essencial garantir o cumprimento de todos os requisitos de segurança, com vista a assegurar níveis máximos de privacidade e de proteção dos dados pessoais, evitando todas as formas de deteção de informação pessoal e de criação de perfis não autorizadas;

31. salienta que, apesar de os operadores privados serem cada vez mais responsáveis por importantes infraestruturas e serviços em linha, e apesar de ser necessário reconhecer o papel fundamental do setor privado, o Estado é, em última análise, o responsável por conservar a liberdade e proteger a segurança em linha dos cidadãos;

Simplificação

32. assinala que a introdução em toda a Europa do princípio de que as informações relativas a pessoas e a bens devem ser registadas uma só vez, sem necessidade de preencher formulários repetidamente, contribuirá em grande medida para reduzir a burocracia desnecessária para o público e os custos da administração pública em geral. Neste contexto, importa velar pelo respeito da legislação respeitante à proteção de dados;

Formação

33. chama a atenção para o facto de as defesas informáticas adequadas exigirem a formação e atualização de competências do pessoal, incluindo dos funcionários dos órgãos de poder local e regional. Importa prestar formação abrangente sobre questões de confiança e segurança a todo o pessoal, em particular aos técnicos especializados, ao pessoal diretamente responsável por procedimentos de segurança que requerem diversas metodologias e ao pessoal envolvido de forma geral ou indireta em iniciativas de inovação e modernização. A formação contínua é importante para o êxito da administração local em linha. Além disso, os órgãos de poder local e regional têm cada vez mais responsabilidades no que toca a prestar informações e orientações aos cidadãos sobre como utilizar adequadamente os sistemas e como reconhecer ameaças informáticas ([6]);

34. considera o «empenhamento da direção» um fator de êxito muito importante. Por este motivo, é essencial prever igualmente uma formação específica dirigida aos membros da direção e aos responsáveis pelo pessoal que lhes ministre os conhecimentos e a preparação necessários para criarem as bases de uma cultura da segurança nas suas organizações;

35. toma nota da melhoria da educação e da formação através da introdução de formação sobre SRI, bem como da criação de um campeonato de cibersegurança em 2014. Este trabalho deverá ter em conta alguns eventos já realizados nos Estados-Membros e estimular o intercâmbio de boas práticas. O CR congratula-se com a ambição de, através da Estratégia, introduzir nas escolas formação sobre SRI. Contudo, visto que a educação é da competência dos Estados-Membros, considera que serão necessários recursos significativos e muita planificação para alcançar este objetivo até 2014;

Apoiar as empresas, a inovação e as soluções técnicas

36. chama a atenção para o facto de que a proteção da privacidade depende de certos fatores, como a estrutura dos órgãos do setor público (a maior parte dos quais existe a nível local), a harmonização da legislação europeia, a promoção de uma cultura de inovação junto dos funcionários da administração pública (através, nomeadamente, de um código ético comum) e junto dos cidadãos (através da definição dos seus direitos enquanto consumidores digitais e da sensibilização para esses direitos) e a gestão de aplicações baseadas nas TIC;

37. é de opinião de que deve haver atividades adicionais que visem estimular e encorajar o desenvolvimento e a aplicação de soluções técnicas para o problema dos conteúdos ilícitos e prejudiciais em linha, e que promovam a cooperação e o intercâmbio das melhores práticas entre as mais diversas partes interessadas a nível local, regional, europeu e internacional. Neste contexto, é extremamente importante dispor de linhas de apoio para crianças, pais e educadores, linhas telefónicas para denunciar abusos, *software* que permita identificar melhor os conteúdos ilícitos e métodos fáceis e céleres para efetuar denúncias;

38. recomenda que se envidem todos os esforços para aumentar a pequena percentagem de empresas na UE (26% em janeiro de 2012) que têm uma política de segurança informática definida formalmente ([7]). Importa encorajar as empresas, independentemente da sua dimensão, a investir na cibersegurança, investimento esse que pode servir como ferramenta de *marketing* para potenciais clientes, ao mesmo tempo que reduz os efeitos catastróficos da cibercriminalidade. As empresas devem ponderar uma abordagem comercial às questões da cibersegurança, que se baseie na tecnologia e dê prioridade aos bens e processos mais importantes para a atividade comercial;

([5]) CdR 104/2010 fin.

([6]) http://www.enisa.europa.eu/publications/archive/scandinavian-approaches-survey

([7]) http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/ICT_security_in_enterprises

Potencial económico das TIC

39. salienta que, dado o enorme potencial económico das TIC na economia europeia (atualmente, o setor é responsável por quase 6% do PIB da UE ([8])), são necessárias medidas concretas para lidar com o fenómeno crescente da cibercriminalidade e para reconquistar a confiança dos cidadãos e das empresas na segurança da Internet (reduzindo o número de utilizadores europeus da Internet que têm receios quanto à segurança dos pagamentos em linha ([9]), por exemplo);

40. reafirma que são necessários esforços urgentes a nível local/regional, nacional e europeu para combater a cibercriminalidade, com vista a reduzir os enormes montantes perdidos devido a esta forma de criminalidade;

41. sugere que seria benéfico para a estratégia apresentar mais detalhes sobre como proteger e desenvolver a computação em nuvem, que tem um enorme potencial económico. O rápido aumento da utilização de dispositivos eletrónicos móveis não dá mostras de abrandar. Segundo um relatório da Gartner, até 2016, pelo menos 50% dos utilizadores de correio eletrónico para fins profissionais dependerão de um suporte móvel ([10]). Assim, é necessário examinar os novos problemas e oportunidades criados pelos dispositivos eletrónicos móveis e pela computação em nuvem. Além disso, esta forma de computação precisa de uma arquitetura adequada para que possa garantir níveis máximos de segurança ([11]). Na realidade, o Comité lamentou o facto de a recente comunicação da Comissão Europeia sobre a computação em nuvem não dar a atenção devida à relação entre a estratégia proposta e questões como a segurança efetiva dos dados, a regulamentação dos direitos de autor ou o desenvolvimento da acessibilidade e da portabilidade dos dados ([12]);

Cooperação internacional

42. entende que, face à ameaça da cibercriminalidade, que é mundial, interligada e transfronteiriça, há que encorajar também a cooperação internacional e o diálogo para lá das fronteiras da UE, com vista a assegurar uma abordagem verdadeiramente global e coordenada à cibersegurança. Neste sentido, importa incentivar todos os Estados a comprometer-se com a Convenção Internacional sobre a Cibercriminalidade (Convenção de Budapeste) ([13]). Igualmente importante é a cooperação continuada a nível bilateral, especialmente com os EUA, e a nível multilateral, com uma panóplia de organizações internacionais;

Ligações com os programas de financiamento da UE e o seu quadro orçamental

43. salienta a importância de melhorar a coordenação com os instrumentos de financiamento atuais e futuros, como o Horizonte 2020, o Quadro Europeu de Cooperação e o Fundo para a Segurança Interna, com vista a assegurar uma abordagem mais coordenada para os investimentos relacionados com a informática;

44. questiona se a afetação orçamental de 1,25 milhões de euros será suficiente para construir uma infraestrutura robusta e adequada para a SRI e manifesta a sua desilusão face à redução dos recursos orçamentais atribuídos ao Mecanismo Interligar a Europa, decidida por acordo do Conselho de 8 de fevereiro quanto ao Quadro Financeiro Plurianual 2014-2020. É necessário um orçamento robusto e acrescido para conceder apoio financeiro às infraestruturas TIC fundamentais, ligando as capacidades dos Estados-Membros em matéria de SRI e tornando assim mais fácil a cooperação em toda a UE.

II. RECOMENDAÇÕES DE ALTERAÇÃO

Alteração 1

Considerando 4

Texto da proposta da Comissão	Alteração proposta pelo CR
Deverá ser estabelecido um mecanismo de cooperação a nível da União, a fim de permitir o intercâmbio de informações e a deteção e resposta coordenadas a ameaças à segurança das redes e da informação («SRI»). Para que esse mecanismo seja eficaz e inclusivo, é indispensável que todos os Estados Membros tenham um mínimo de capacidades e uma estratégia que garanta um elevado nível de SRI no seu território. Deverão também aplicar-se requisitos mínimos de segurança às administrações públicas e aos operadores das infraestruturas críticas de informação, a fim de promover uma cultura de gestão dos riscos e assegurar a comunicação dos incidentes mais graves.	Deverá ser estabelecido um mecanismo de cooperação a nível da União, a fim de permitir o intercâmbio de informações e a deteção e resposta coordenadas a ameaças à segurança das redes e da informação («SRI»). Para que esse mecanismo seja eficaz e inclusivo, é indispensável que todos os Estados Membros tenham um mínimo de capacidades e uma estratégia que garanta um elevado nível de SRI no seu território. Deverão também aplicar-se requisitos mínimos de segurança às administrações públicas, **incluindo os órgãos de poder local e regional**, e aos operadores das infraestruturas críticas de informação, a fim de promover uma cultura de gestão dos riscos e assegurar a comunicação dos incidentes mais graves.

([8]) http://europa.eu/rapid/press-release_MEMO-13-71_en.htm
([9]) http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf
([10]) http://www.sophos.com/medialibrary/PDFs/other/SophosSecurityThreatReport2012.pdf
([11]) http://www.mcafee.com/hk/resources/reports/rp-sda-cyber-security.pdf
([12]) CdR 1673/2012.
([13]) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

Alteração 2

Considerando 9

Texto da proposta da Comissão	Alteração proposta pelo CR
A fim de atingir e manter um nível elevado comum de segurança das redes e dos sistemas informáticos, cada Estado-Membro deve dispor de uma estratégia nacional de SRI que defina os objetivos estratégicos e as ações estratégicas concretas a executar. É necessário desenvolver planos de cooperação SRI a nível nacional que cumpram os requisitos essenciais, a fim de alcançar níveis de capacidade de resposta que permitam uma cooperação eficaz e eficiente a nível nacional e da União em caso de ocorrência de incidentes.	A fim de atingir e manter um nível elevado comum de segurança das redes e dos sistemas informáticos, cada Estado-Membro deve dispor de uma estratégia nacional de SRI que defina os objetivos estratégicos e as ações estratégicas concretas a executar. É necessário desenvolver, **com a plena participação dos órgãos de poder local e regional**, planos de cooperação SRI a nível nacional que cumpram os requisitos essenciais, a fim de alcançar níveis de capacidade de resposta que permitam uma cooperação eficaz e eficiente a nível nacional e da União em caso de ocorrência de incidentes.

Alteração 3

Considerando 35

Texto da proposta da Comissão	Alteração proposta pelo CR
É particularmente importante que a Comissão proceda a consultas adequadas durante os seus trabalhos preparatórios, incluindo a nível de peritos. A Comissão, ao preparar e redigir atos delegados, deverá assegurar a transmissão simultânea, atempada e adequada dos documentos relevantes ao Parlamento Europeu e ao Conselho.	É particularmente importante que a Comissão proceda a consultas adequadas durante os seus trabalhos preparatórios, incluindo a nível de peritos. A Comissão, ao preparar e redigir atos delegados, deverá assegurar a transmissão simultânea, atempada e adequada dos documentos relevantes ao Parlamento Europeu e ao Conselho, **para que se completem ou alterem alguns elementos não essenciais do ato de base.**

Alteração 4

Artigo 14.º, n.º 1

Texto da proposta da Comissão	Alteração proposta pelo CR
Exigências de segurança e notificação de incidentes 1. Os Estados-Membros devem assegurar que as administrações públicas e os operadores do mercado adotem medidas técnicas e organizacionais adequadas para gerir os riscos que se colocam à segurança das redes e dos sistemas informáticos que controlam e utilizam na sua atividade. Tendo em conta os progressos técnicos, essas medidas devem garantir um nível de segurança adequado em função do risco existente. Em particular, devem ser tomadas medidas para impedir e minimizar o impacto dos incidentes que afetam a sua rede e sistema informático nos serviços essenciais oferecidos, assegurando assim a continuidade dos serviços assentes nessas redes e sistemas.	Exigências de segurança e notificação de incidentes 1. **Os** Estados-Membros devem assegurar que as administrações públicas e os operadores do mercado adotem medidas técnicas e organizacionais adequadas para gerir os riscos que se colocam à segurança das redes e dos sistemas informáticos que controlam e utilizam na sua atividade. **Estas medidas, aplicáveis a nível local e regional, podem contemplar a criação de um processo de avaliação e gestão dos riscos, o cumprimento da política sobre a segurança da informação, o reforço da sensibilização para as questões da cibersegurança e a melhoria da literacia digital e das competências neste domínio.** Tendo em conta os progressos técnicos, essas medidas devem garantir um nível de segurança adequado em função do risco existente. Em particular, devem ser tomadas medidas para impedir e minimizar o impacto dos incidentes que afetam a sua rede e sistema informático nos serviços essenciais oferecidos, assegurando assim a continuidade dos serviços assentes nessas redes e sistemas.

Justificação

Os órgãos de poder local e regional desempenham um papel crucial no combate à cibercriminalidade e esse facto deve ser plenamente reconhecido.

Alteração 5

Capítulo IV

Artigo 16.º

Texto da proposta da Comissão	Alteração proposta pelo CR
Artigo 16.º	*Artigo 16.º*
Normalização	Normalização
1. Para garantir a aplicação convergente do artigo 14.º, n.º 1, os Estados Membros devem encorajar a utilização das normas e/ou especificações pertinentes para a segurança das redes e da informação.	*1.* Para garantir a aplicação convergente do artigo 14.º, n.º 1, os Estados Membros devem encorajar a utilização das normas **harmonizadas** e/ou especificações pertinentes para a segurança das redes e da informação.
2. A Comissão estabelece, por meio de atos de execução, uma lista das normas referidas no n.º 1, que será publicada no *Jornal Oficial da União Europeia*.	*2.* A Comissão estabelece, por meio de atos de execução, uma lista das normas referidas no n.º 1, que será publicada no *Jornal Oficial da União Europeia*.

Justificação

A Comissão Europeia reconhece que a aplicação de normas divergentes nos diversos Estados-Membros constitui um desafio de monta. Por conseguinte, a harmonização das normas é essencial para assegurar um nível comum de segurança das redes e da informação em toda a UE.

Bruxelas, 3 de julho de 2013

O Presidente
do Comité das Regiões
Ramón Luis VALCÁRCEL SISO