



ASSEMBLEIA DA REPÚBLICA

COMISSÃO DE ASSUNTOS EUROPEUS

Parecer

COM(2012)140

**COMUNICAÇÃO DA COMISSÃO AO CONSELHO E AO
PARLAMENTO EUROPEU - Luta contra a criminalidade na era
digital: criação de um Centro Europeu da Cibercriminalidade**



ASSEMBLEIA DA REPÚBLICA

COMISSÃO DE ASSUNTOS EUROPEUS

PARTE I - NOTA INTRODUTÓRIA

Nos termos do artigo 7.º da Lei n.º 43/2006, de 25 de agosto, alterada pela Lei n.º 21/2012, de 17 de maio, que regula o acompanhamento, apreciação e pronúncia pela Assembleia da República no âmbito do processo de construção da União Europeia, bem como da Metodologia de escrutínio das iniciativas europeias, aprovada em 20 de janeiro de 2010, a Comissão de Assuntos Europeus recebeu a COMUNICAÇÃO DA COMISSÃO AO CONSELHO E AO PARLAMENTO EUROPEU - Luta contra a criminalidade na era digital: criação de um Centro Europeu da Cibercriminalidade [COM(2012)140].

A supra identificada iniciativa foi enviada à Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, atento o seu objeto, a qual analisou a referida iniciativa e aprovou o Relatório que se anexa ao presente Parecer, dele fazendo parte integrante

PARTE II – CONSIDERANDOS

A Internet tornou-se parte integrante e indispensável da nossa sociedade e da nossa economia. Oitenta por cento dos jovens europeus ligam-se entre si e ao mundo através das redes sociais *online*¹. O comércio eletrónico faz com que mudem de mãos anualmente em todo o mundo cerca de 8 biliões de dólares². Mas, à medida que grande parte da nossa vida quotidiana e das nossas transações comerciais passam a ter lugar *online*, o mesmo sucede com as atividades criminosas. Todos os dias mais de um milhão de pessoas são vítimas da cibercriminalidade em todo o mundo³. As atividades criminosas *online* vão desde a venda de cartões de crédito furtados por valores irrisórios, a usurpação de identidade e o abuso sexual de crianças, até aos ciberataques em grande escala contra as instituições e as infraestruturas.

¹ Eurostat, «O acesso e a utilização da Internet», 14 de dezembro de 2010.

² Instituto Global McKinsey, «*Internet Matters: the Net's sweeping impact on growth, jobs and prosperity*». Relatório de maio de 2011, consultado em 8 de fevereiro de 2012.

³ Relatório Norton sobre o Cibercrime de 2011, 7 de setembro de 2011, consultado em 6 de janeiro de 2012.



ASSEMBLEIA DA REPÚBLICA

COMISSÃO DE ASSUNTOS EUROPEUS

Os custos globais da cibercriminalidade para as nossas sociedades são consideráveis. Um relatório recente revelou que as vítimas do cibercrime perdem anualmente cerca de 388 mil milhões de dólares em todo o mundo, o que torna este tipo de crime mais rentável que o conjunto do tráfico mundial de marijuana, cocaína e heroína⁴. Embora estes dados devam ser considerados com alguma cautela, pois as diferentes abordagens do conceito de cibercriminalidade podem fazer variar as estimativas dos custos, é geralmente reconhecido que esta forma de criminalidade é altamente rentável e apresenta riscos reduzidos, o que a torna cada vez mais comum e nociva.

A liberdade da Internet é o fator determinante que explica a revolução digital ocorrida nos últimos anos. A nossa Internet aberta não conhece fronteiras nacionais nem uma estrutura única de governação mundial. Mas, embora a promoção e a proteção da liberdade *online* seja conforme com a Carta dos Direitos Fundamentais da UE, é também nossa obrigação proteger os cidadãos contra os grupos criminosos organizados que tiram partido dessa abertura. Nenhum outro crime transpõe tão facilmente as fronteiras como o cibercrime, o que exige às autoridades responsáveis pela aplicação da lei que adotem uma abordagem coordenada e uma colaboração para além das fronteiras nacionais, que envolva igualmente todos os interessados, públicos ou privados. É neste aspeto que a UE pode trazer, e traz efetivamente, um importante valor acrescentado.

A União Europeia tem desenvolvido várias iniciativas para combater a cibercriminalidade. Entre estas figuram uma diretiva de 2011, relativa à luta contra a exploração sexual de crianças *online* e a pornografia infantil, e uma diretiva relativa a ataques contra os sistemas informáticos, ambas centradas na criminalização da utilização de instrumentos próprios à cibercriminalidade, designadamente as *botnets*⁵, e que devem ser adotadas em 2012.

⁴ Idem.

⁵ Proposta de diretiva do Parlamento Europeu e do Conselho relativa a ataques contra os sistemas de informação, COM (2010) 517 final, de 30 de setembro de 2010. As *botnets* são redes de computadores infetados por *software* maligno, que podem ser ativadas à distância, para desempenhar determinadas ações, incluindo ciberataques.



ASSEMBLEIA DA REPÚBLICA

COMISSÃO DE ASSUNTOS EUROPEUS

A luta contra o cibercrime, cujo principal instrumento jurídico é a Convenção sobre o Cibercrime do Conselho da Europa⁶, continua a ter a máxima prioridade. Foi tida em conta no ciclo de políticas da UE para lutar contra a criminalidade internacional grave e organizada⁷ e faz parte integrante dos esforços para definir uma estratégia global da UE em matéria de cibersegurança. A União Europeia começou igualmente a cooperar estreitamente com os seus parceiros internacionais, nomeadamente através do grupo de trabalho UE-EUA existente sobre cibersegurança e cibercriminalidade.

Não obstante os progressos efetuados, subsistem vários obstáculos a uma investigação e repressão eficaz do cibercrime a nível europeu, designadamente os limites jurisdicionais, a falta de partilha das informações, as dificuldades técnicas para detetar a origem dos criminosos informáticos, a disparidade das capacidades de investigação e da polícia científica, a escassez de pessoal qualificado e a falta de cooperação com outros interessados no domínio da cibersegurança. Através do Instrumento de Estabilidade, a UE também aborda o problema da rápida evolução das ameaças transnacionais relacionadas com o cibercrime nos países em desenvolvimento ou em transição, onde as capacidades para combater este tipo de crime são, muitas vezes, inexistentes.

Em resposta a estes desafios, a Comissão anunciou a sua intenção de criar um Centro Europeu da Cibercriminalidade, enquanto uma das prioridades da Estratégia de Segurança Interna⁸.

⁶ Convenção do Conselho da Europa sobre o Cibercrime, Budapeste, 23 de novembro de 2001, também designada por Convenção de Budapeste. A Convenção é acompanhada de um *protocolo adicional* relativo à incriminação de atos de natureza racista ou xenófoba praticados através de sistemas informáticos.

⁷ O ciclo de políticas da UE para lutar contra a criminalidade internacional grave e organizada, que abrange o período 2011/2013, estabeleceu oito prioridades, entre as quais, «intensificar a luta contra a cibercriminalidade e a utilização criminosa da Internet pelos grupos criminosos organizados».

⁸ «Até 2013, a UE estabelecerá [...] um centro de cibercriminalidade, através do qual os Estados Membros e as instituições da UE poderão desenvolver capacidades operacionais e analíticas para as investigações e a cooperação com parceiros internacionais». COM(2010) 673 final, de 22 de novembro de 2010.



ASSEMBLEIA DA REPÚBLICA

COMISSÃO DE ASSUNTOS EUROPEUS

Atentas as disposições da presente proposta, cumpre suscitar as seguintes questões:

a) Da Base Jurídica

Na luta contra o cibercrime, o principal instrumento jurídico é a Convenção sobre o Cibercrime do Conselho da Europa. A Convenção do Conselho da Europa sobre o Cibercrime, Budapeste, 23 de novembro de 2001, é também designada por Convenção de Budapeste. A Convenção é acompanhada de um *protocolo adicional* relativo à incriminação de atos de natureza racista ou xenófoba praticados através de sistemas informáticos

b) Do Princípio da Subsidiariedade

Por tratar-se de uma Comunicação da Comissão Europeia cuja iniciativa é não legislativa não há lugar à verificação do Princípio da Subsidiariedade.

c) Do conteúdo da iniciativa

Subscrever e adotar as considerações elaboradas pela Comissão Parlamentar competente na matéria, em especial os pontos 3 e 4 do Relatório, que se anexa ao presente Parecer.

PARTE III – PARECER

Em face dos considerandos expostos e atento o Relatório da comissão competente, a Comissão de Assuntos Europeus é de parecer que:

1. Relativamente à presente iniciativa não cabe a apreciação do cumprimento do Princípio da Subsidiariedade uma vez que se trata de matéria não legislativa;



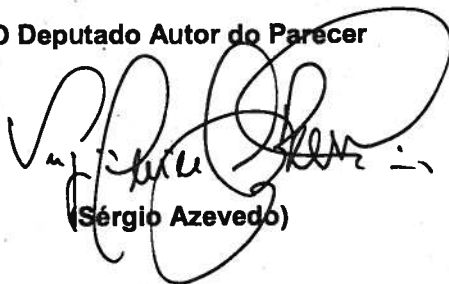
ASSEMBLEIA DA REPÚBLICA

COMISSÃO DE ASSUNTOS EUROPEUS

2. No que concerne as questões suscitadas nos considerandos, a Comissão de Assuntos Europeus prosseguirá o acompanhamento de futuros processos legislativos referente à presente iniciativa, nomeadamente através de troca de informação com o Governo.

Palácio de S. Bento, 8 de janeiro de 2013

O Deputado Autor do Parecer



(Sérgio Azevedo)

O Presidente da Comissão



(Paulo Mota Pinto)



ASSEMBLEIA DA REPÚBLICA

COMISSÃO DE ASSUNTOS EUROPEUS

PARTE IV – ANEXO

Relatório da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias

COMISSÃO DE ASSUNTOS CONSTITUCIONAIS, DIREITOS, LIBERDADES E GARANTIAS

RELATÓRIO

Iniciativa Europeia: COM (2012) 140 Final - Comunicação da Comissão ao Conselho e ao Parlamento Europeu – Luta contra a criminalidade na era digital: criação de um Centro Europeu da Cibercriminalidade

1. Nota Introdutória

A Comissão Parlamentar dos Assuntos Europeus, em conformidade com o disposto no nº 1 do artigo 7º da Lei nº 43/2006, de 25 de Agosto, referente ao acompanhamento, apreciação e pronúncia pela Assembleia da República, no âmbito do processo de construção da União Europeia, remeteu à Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, para esta se pronunciar sobre a matéria da sua competência, a COM (2012) 1140 FINAL – COMUNICAÇÃO DA COMISSÃO AO CONSELHO E AO PARLAMENTO EUROPEU sobre LUTA CONTRA A CRIMINALIDADE NA ERA DIGITAL: CRIAÇÃO DE UM CENTRO EUROPEU DA CIBERCRIMINALIDADE.

A COM(2012) 140 FINAL consagra a proposta da Comissão no sentido da criação de um Centro Europeu da Cibercriminalidade (EC3), que fará parte integrante da Europol e constituirá o futuro ponto de convergência da luta contra a cibercriminalidade na União Europeia.

2. Enquadramento

2.1. Segurança no ciberespaço

A presente proposta vem dar cumprimento a uma das ações inseridas no Objetivo 3 da COM (2010) 673 Final – **Estratégia de Segurança Interna da UE em Ação: cinco etapas para uma Europa mais segura.**

O objetivo 3 da COM (2010) 673 Final consiste no reforço dos níveis de segurança para os cidadãos e as empresas no ciberespaço, convergindo, nesta matéria, com a

estratégia delineada na **Agenda Digital para a Europa**¹, que elege, como um dos seus domínios-problema, a confiança e a segurança das tecnologias de informação, recomendando a *“aplicação rápida e eficaz do plano de ação da UE para a proteção das infraestruturas de informação críticas e do Programa de Estocolmo”* que *“espoletará uma vasta gama de medidas no domínio da segurança das redes e da informação e do combate ao cibercrime. Por exemplo, para reagir em tempo real, deve ser criada na Europa, inclusivamente para as instituições europeias, uma rede ampla e funcional de equipas de resposta a emergências informáticas (CERT). A cooperação entre essas equipas e as entidades judiciais/policiais é essencial, pelo que seria útil promover um sistema de pontos de contacto para ajudar a prevenir o cibercrime e responder às emergências, como no caso de ciberataques. A Europa necessita igualmente de uma estratégia para a gestão das identidades, nomeadamente para que os serviços de governo eletrónico possam dar garantias de segurança e eficácia”*².

¹ COM (2010) 245. A Agenda Digital para a Europa constitui, por seu turno, uma das sete iniciativas emblemáticas da **estratégia Europa 2020** e visa definir o papel que a utilização das tecnologias da informação e das comunicações (TIC) na concretização desta estratégia. O objetivo Agenda Digital para a Europa é definir um roteiro que maximize o potencial social e económico das TIC, com destaque para a Internet, um recurso fundamental da atividade económica e social: para os negócios, para o trabalho, para o lazer, para a comunicação e para a expressão livre das ideias.

² Para a concretização destes objetivos, a ADE estabelece as seguintes ações: Apresentação, em 2010, de medidas que visem pôr em prática uma política reforçada e de alto nível em matéria de segurança das redes e da informação, incluindo iniciativas legislativas, como a modernização da Agência Europeia para a Segurança das Redes e da Informação (ENISA), e outras medidas que permitam reagir mais rapidamente em caso de ataques informáticos, incluindo uma CERT para as instituições da UE; Apresentar, até 2010, medidas, nomeadamente iniciativas legislativas, que visem combater os ciberataques contra sistemas informáticos e, até 2013, regras em matéria de jurisdição do ciberespaço aos níveis europeu e internacional; Criar uma plataforma europeia para a cibercriminalidade até 2012; Até 2011, estudar a possibilidade de criar um centro europeu para a cibercriminalidade; Trabalhar com as partes interessadas a nível mundial, nomeadamente para reforçar a gestão mundial dos riscos na esfera digital e física e levar a cabo ações focalizadas, coordenadas a nível internacional, contra a criminalidade informática e os ataques à segurança; A partir de 2010, apoiar exercícios de preparação para a cibersegurança à escala da UE; No âmbito da modernização do quadro regulamentar da UE relativo à proteção dos dados pessoais, que visa torná-lo mais coerente e capaz de oferecer maior segurança jurídica, estudar a possibilidade de extensão das disposições sobre notificação das violações da segurança; Até 2011, publicar orientações para a aplicação do novo quadro das telecomunicações no que respeita à proteção da privacidade dos indivíduos e dos dados pessoais; Apoiar a criação de pontos de denúncia de conteúdos ilegais em linha (linhas diretas) e campanhas de sensibilização sobre a segurança das crianças em linha conduzidas a nível nacional, e melhorar a cooperação pan-europeia e a divulgação das melhores práticas neste domínio; Promover o diálogo entre as várias partes interessadas e a auto-regulação dos fornecedores de serviços europeus e mundiais (por exemplo, plataformas de redes sociais, operadores de comunicações móveis), em especial no que respeita à utilização dos seus serviços por menores. Por outro lado, os Estados-Membros devem estabelecer, até 2012, uma rede funcional de CERT a nível nacional que cubra toda a Europa, efetuar, a partir de 2010, e em cooperação com a Comissão, operações de simulação de ataques em grande escala e testar estratégias de mitigação, pôr a funcionar em pleno, até 2013, as linhas diretas para denúncia de conteúdos em linha ofensivos ou prejudiciais, organizar campanhas de sensibilização sobre a segurança das crianças em linha, prever para as escolas disciplinas sobre segurança em linha e ainda incentivar os fornecedores de serviços em linha a implementarem medidas de auto-regulação no que respeita à segurança das

Uma das preocupações da “Estratégia de Segurança Interna em Ação: cinco etapas para uma Europa mais segura” centra-se precisamente na necessidade de melhorar a capacidade de resposta aos ciberataques, aí se prevendo que até ao final de 2012 todos os Estados-Membros e as instituições da União Europeia devem dispor de uma equipa de emergência de resposta no domínio informático, cooperando entre si na prevenção e resposta (CERT).

Nos termos desta Estratégia, até 2013 a União Europeia “estabelecerá, no âmbito das estruturas existentes, **um centro de cibercriminalidade**, através do qual os Estados-Membros e as instituições da UEU poderão desenvolver capacidades operacionais e analíticas para as investigações e a cooperação com parceiros internacionais. Este centro melhorará a avaliação e o acompanhamento das medidas de prevenção e de investigação em vigor, apoiará o desenvolvimento da formação e a sensibilização nos domínios policial e judiciário, estabelecerá a cooperação com a Agência para a Segurança das Redes e da Informação (ENISA) e servirá de interligação com uma rede de equipas de emergência nacionais/governamentais de resposta no domínio informático (Computer Emergency Response Team – CERTs). O centro de cibercriminalidade deve tornar-se o ponto nevrálgico do combate europeu à cibercriminalidade”.

Ainda no âmbito da luta contra o cibercrime, a União Europeia tem como principal instrumento jurídico a Convenção sobre o Cibercrime do Conselho da Europa (Convenção de Budapeste).

2.2. Proteção das Infraestruturas Críticas

Importa ainda, neste contexto, referir que em 2006 a União Europeia lançou o **Programa Europeu de Proteção das Infraestruturas Críticas**, que deu origem à Diretiva 2008/114/CE, transposta para o nosso ordenamento jurídico através do Decreto-Lei nº 62/2011, de 09 de Maio³.

crianças em linha; e, até 2012, criar plataformas nacionais de alerta ou adaptá-las à plataforma para o cibercrime da Europol.

³ De acordo com o seu preâmbulo, “O presente decreto-lei estabelece os procedimentos de identificação e de proteção das infra-estruturas essenciais para a saúde, a segurança e o bem-estar económico e social da sociedade nos sectores da energia e transportes, transpondo a Directiva n.º 2008/114/CE, do Conselho, de 8 de Dezembro. Com o presente decreto-lei, estabelecem-se procedimentos para a identificação das diversas infra-estruturas com funções essenciais para a sociedade, cuja perturbação ou destruição teria um impacto significativo, porque implicaria que essa infra-estrutura deixasse de poder assegurar essas funções. Assim, com o regime agora criado, Portugal adquire uma maior capacidade de intervenção ao nível da segurança e resiliência das infra-estruturas que venham a ser sectorialmente consideradas críticas, no âmbito europeu, integrando o futuro Programa Europeu de Protecção de Infra-estruturas Críticas (PEPIC) suportado numa abordagem transversal dos riscos a que essas infra-estruturas possam estar expostas”.

Já aqui se salientava⁴ que esta Diretiva constituía *“a primeira etapa de uma abordagem faseada para identificar e designar as ICE [infraestruturas críticas europeias] e avaliar a necessidade de melhorar a sua protecção. Concentra-se, enquanto tal, nos sectores da energia e dos transportes, e deverá ser revista com o objectivo de avaliar o seu impacto e a necessidade de incluir no seu âmbito de aplicação outros sectores, designadamente o das Tecnologias da Informação e Comunicação (TIC)”*.

Em Março de 2009, a Comissão apresentou ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões a COM (2009) 149 - relativa à proteção das infraestruturas críticas da informação *“Proteger a Europa contra os ciberataques e as perturbações em grande escala: melhorar a preparação, a segurança e a resiliência”*.

Esta Comunicação centra-se na prevenção, preparação e sensibilização e define um plano de ações imediatas para reforçar a segurança e a resiliência das Infraestruturas Críticas de Informação.

Em conformidade, a COM (2009) 149 define cinco pilares de ação, nomeadamente a **preparação e prevenção** a todos os níveis, **deteção e resposta**, através da criação de mecanismos adequados de alerta rápido, a **mitigação e recuperação**, reforçando os mecanismos de defesa das ICI na UE, a **cooperação internacional**, promovendo internacionalmente as prioridades da EU e a definição de **critérios para o sector das TIC**, através da aplicação da diretiva relativa à identificação e designação das infraestruturas críticas europeias.

A avaliação das medidas propostas para cada um destes pilares e a definição de ações para o futuro foi objecto da COM(2011) 163 Final, que alerta para o facto de não ser possível, em matéria de tecnologias de informação e comunicação, efetuar uma abordagem europeia, sendo necessário envidar esforços no sentido de uma **gestão mundial de riscos**.

Nesta Comunicação releva-se a importância das equipas de resposta a emergências informáticas (CERT), a nível nacional, e que, em cooperação com a ENISA (Agência Europeia para a Segurança das Redes e da Informação), se constitua *“uma rede de CERT nacionais/governamentais totalmente operacionais em todos os Estados-Membros até 2012. Essa rede constituirá a espinha dorsal de um sistema europeu de partilha de informações e de alerta (SEPIA ou, na sigla inglesa, EISAS) para os cidadãos e as PME, que será construído até 2013 com recursos e capacidades nacionais”*.

⁴ Ponto 5 do Préâmbulo da Diretiva.

Apela igualmente aos Estados-Membros para conceberem “um plano de emergência europeu em caso de incidente informático, até 2012, e organizar exercícios pan-europeus regulares no domínio da cibersegurança. Os exercícios no domínio da cibersegurança são um elemento importante de uma estratégia coerente de planeamento da resposta a emergências e das acções de recuperação em caso de incidentes informáticos tanto ao nível nacional como europeu. Os futuros exercícios pan-europeus no domínio da cibersegurança deverão basear-se num plano de emergência europeu para incidentes informáticos que tire partido e se articule com os planos de emergência nacionais. Tal plano deverá prever os mecanismos e procedimentos de base para as comunicações entre Estados-Membros e, igualmente importante, contribuir para a definição do âmbito e para a organização dos futuros exercícios pan-europeus. A ENISA trabalhará com os Estados-Membros na elaboração desse plano europeu de emergência para incidentes informáticos, que deverá estar pronto até 2012. Nesse mesmo prazo, todos os Estados-Membros deverão elaborar planos nacionais de emergência e prever exercícios de resposta e de recuperação”.

De referir que sobre esta matéria, em termos de legislação, existe uma proposta de Diretiva do Parlamento e do Conselho, de 20 de Setembro de 2010, relativa a ataques contra os sistemas de informação⁵, justificada pela necessidade de intervenção da União Europeia neste domínio, pela necessidade de criminalizar certas formas de infrações não incluídas na atual Decisão-Quadro, em especial as novas formas de ciberataque, e ainda pela necessidade de eliminar obstáculos às investigações e ações penais nos processos transfronteiras⁶.

3. Objetivos e conteúdo da Comunicação

3.1. Contexto

⁵ E que vem revogar a Decisão-Quadro 2005/222/JAI do Conselho.

⁶ A proposta de Diretiva assinala que: “A principal causa da cibercriminalidade é a vulnerabilidade resultante de vários factores. Uma resposta insuficiente dos mecanismos de aplicação da lei contribui para a prevalência destes fenómenos e agrava as dificuldades, já que certos tipos de crimes têm carácter transfronteiriço. As denúncias relativas a este tipo de crime são muitas vezes inadequadas, em parte porque alguns crimes não são detectados e em parte porque as vítimas (operadores económicos e empresas) não os denunciam por temerem que a exposição pública das suas vulnerabilidades afecte a sua reputação e as perspectivas comerciais futuras. Além disso, as diferenças entre as legislações e procedimentos penais nacionais podem dar origem a diferenças a nível da investigação e das acções penais, conduzindo a discrepâncias no tratamento dado a estes crimes. A evolução no domínio das tecnologias da informação exacerbam estes problemas, facilitando a produção e distribuição de instrumentos («malware» e «botnets») e proporcionando ao mesmo tempo anonimato aos infractores e dispersando a responsabilidade por várias jurisdições. Dadas as dificuldades em levar a cabo uma acção penal, a criminalidade organizada consegue obter lucros consideráveis com riscos reduzidos. A presente proposta tem em conta os novos métodos utilizados para cometer cibercrimes, nomeadamente o recurso aos «botnets”.

A criação de um Centro Europeu da Cibercriminalidade é uma das prioridades da Estratégia de Segurança Interna da União Europeia, na medida em que a Internet se tornou “parte integrante e indispensável da nossa sociedade e da nossa economia”.

Com efeito:

- 80% dos jovens europeus ligam-se entre si e ao mundo através das redes sociais online;
- O comércio eletrónico movimenta atualmente oito biliões de dólares;
- Diariamente mais de um milhão são vítimas de cibercriminalidade em todo o mundo;
- As vítimas do cibercrime perdem anualmente cerca de 388 mil milhões de dólares, o que torna este tipo de crime mais rentável que o conjunto do tráfico mundial de marijuana, cocaína e heroína;
- Nenhum outro crime transpõe tão facilmente as fronteiras como o cibercrime.

3.2. Atividade do Centro Europeu da Cibercriminalidade (EC3)

Garantindo o respeito do princípio da subsidiariedade, o EC3 deve centrar a sua actividade em três áreas fundamentais:

- i) Cibercrimes praticados por grupos criminosos organizados, em especial os que geram grandes lucros, como a fraude online;
- ii) Cibercrimes que causem danos graves às vítimas, como a exploração sexual de crianças online; e
- iii) Cibercrimes (incluindo ataques informáticos) que afetem as infraestruturas críticas e os sistemas de informação da União.

Em conformidade, o EC3 deverá desempenhar quatro funções essenciais:

- i) Servir de ponto de convergência europeu de informações sobre a criminalidade, nomeadamente recolhendo informação sobre atividades, métodos e os suspeitos da prática de cibercrimes; neste âmbito, pretende-se estabelecer ligações adequadas ente as autoridades responsáveis pela aplicação da lei, a Equipa-de Resposta Informática de Emergência (CERT) e os especialistas do setor privado em matéria de segurança de tecnologias de informação e da comunicação, em observância das regras e acordos em matéria de confidencialidade, de modo a alcançar-se um retrato fiel da cibercriminalidade na Europa ao longo do tempo; A Comissão manifesta

nesta Comunicação o seu desejo de que os Estados-Membros estabelecessem a obrigatoriedade de notificação dos cibercrimes graves às autoridades nacionais responsáveis pela aplicação da lei;

- ii) Congregar os conhecimentos especializados europeus em matéria de cibercriminalidade para apoiar o reforço das capacidades nos Estados-Membros, ficando o EC3 com a função de ajudar os Estados-Membros a desenvolverem os conhecimentos especializados e a formação em matéria de luta contra a cibercriminalidade; neste âmbito, propõe-se a criação de um gabinete para a cibercriminalidade cuja tarefa será a de proceder ao intercâmbio de melhores práticas e conhecimentos, estabelecer contacto e dar resposta aos pedidos de informação apresentados pelas autoridades nacionais; o EC3 teria também como função o aconselhamento aos grupos de peritos em cibercriminalidade, incluindo a Task Force da União Europeia para a Cibercriminalidade e os peritos em matéria de luta contra a exploração sexual de crianças através da Internet, e estabelecer uma cooperação com a rede de centros de excelência contra a cibercriminalidade, designadamente a 2Centre e a comunidade de investigadores; o EC3 constituirá também um apoio aos Estados-Membros na elaboração e lançamento de uma aplicação online de notificação dos cibercrimes;
- iii) Prestar apoio às investigações dos Estados-Membros em matéria de cibercrime, em particular apoio operacional às investigações sobre cibercrime e assistência científica e de conhecimentos técnicos de cifragem no âmbito das investigações de cibercrimes;
- iv) Ser o interlocutor coletivo dos investigadores europeus de cibercrimes a nível das autoridades policiais e do poder judicial, atuando, neste âmbito, como ponto de encontro dos investigadores europeus (públicos e privados) sobre cibercrimes e colaborar com as diversas organizações, como a rede INSAFE (rede europeia de centros de sensibilização para uma utilização segura e responsável da Internet e dos telemóveis pelos jovens), na realização de campanhas de sensibilização do público.

3.3. Operacionalização do EC3

O Centro Europeu da Cibercriminalidade será integrado na Europol, ficando a estrutura com sede nas suas instalações.

A Comissão sugere que, para garantir a participação de outros intervenientes na direção estratégica do EC3, seja criado um conselho de administração presidido pelo diretor do Centro, nele incluindo o Eurojust, CEPOL, os Estados-Membros,



ASSEMBLEIA DA REPÚBLICA

representados pela Task Force da União Europeia para a Cibercriminalidade, a ENISA e a Comissão.

Em termos de recursos humanos, e tendo em conta as funções que podem vir a ser atribuídas à Europol, no contexto da revisão da sua base jurídica, e tendo em consideração a proposta de criação de um Fundo para a Segurança Interna, a Comissão admite que possa vir a ser necessário, no futuro, o recrutamento de pessoal.

Para garantir a capacidade operacional, a Comissão irá analisar, em colaboração com a Europol, as necessidades de recursos humanos e financeiros para a formação da equipa responsável pelo EC3.

4. Conclusões

- 4.1. A Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias apreciou e discutiu o conteúdo da COM (2012) 140 Final, com base no presente Parecer;
- 4.2. O reforço da capacidade de combate ao cibercrime e de proteção das infraestruturas críticas das tecnologias de informação e comunicação é fundamental para a segurança dos cidadãos e da economia global;
- 4.3. A criação de um Centro Europeu da Cibercriminalidade, no respeito pelo princípio da subsidiariedade e em observância das normas relativas à confidencialidade e acesso a base de dados pessoais, constitui um importante instrumento de combate à cibercriminalidade;
- 4.4. Face ao exposto, o presente Relatório sobre a COM (2012) 140 Final – Comunicação da Comissão ao Conselho e ao Parlamento Europeu sobre a LUTA CONTRA A CRIMINALIDADE NA ERA DIGITAL: CRIAÇÃO DE UM CENTRO EUROPEU DA CIBERCRIMINALIDADE deve ser remetido, para os devidos efeitos, à Comissão Parlamentar dos Assuntos Europeus.

Palácio de São Bento, 26 de Setembro de 2012

A Deputada Relatora

(Isabel Oneto)

O Presidente da Comissão

(Fernando Negrão)