COMISSÃO DAS COMUNIDADES EUROPEIAS

Bruxelas, 15.11.2006
COM(2006) 688 final

COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, AO CONSELHO, AO COMITÉ ECONÓMICO E SOCIAL EUROPEU E AO COMITÉ DAS REGIÕES

Combater o *spam*, o *spyware* e o *malware*

COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, AO CONSELHO, AO COMITÉ ECONÓMICO E SOCIAL EUROPEU E AO COMITÉ DAS REGIÕES

Combater o *spam*, o *spyware* e o *malware*

(Texto relevante para efeitos do EEE)

1. OBJECTIVO DA COMUNICAÇÃO

A sociedade está cada vez mais consciente do carácter essencial das redes e serviços de comunicações electrónicas para o nosso dia-a-dia, no trabalho ou em casa. Para que os serviços se possam implantar generalizadamente, são indispensáveis tecnologias de confiança, seguras e fiáveis. A Comunicação da Comissão "Estratégia para uma sociedade da informação segura"[1] tem por objectivo melhorar a segurança das redes e da informação em geral e insta o sector privado a encontrar soluções para as vulnerabilidades das redes e dos sistemas informáticos, que podem ser exploradas para difundir *spam* (correio não desejado) e *malware* (software maligno). A Comunicação da Comissão relativa à revisão do quadro regulamentar comunitário propõe novas regras para reforçar a segurança e a protecção da privacidade no sector das comunicações electrónicas[2].

A presente comunicação trata da evolução do *spam*[3] e de ameaças como o *spyware* (software espião) e o *malware* (software maligno). Nela se dá conta dos esforços realizados até à data para combater estas ameaças e se identificam outras acções que podem ser desenvolvidas, nomeadamente:

- o reforço da legislação comunitária

- a actuação repressiva

- a cooperação dentro de cada Estado-Membro e entre Estados-Membros

- o diálogo político e económico com os países terceiros

- iniciativas do próprio sector

- actividades de I&D.

---

1 COM(2006) 251 final
2 COM(2006) 334 final.
3 COM(2004) 28 final

2. O PROBLEMA – CARÁCTER EVOLUTIVO DAS AMEAÇAS

O *spam*[4] aumentou significativamente nos últimos 5 anos[5]. Segundo fontes do sector, o *spam* representa hoje 50-80 % das mensagens enviadas aos utilizadores finais[6]. Embora a maior parte do *spam* tenha origem fora da UE, os países europeus representam hoje 25 % das mensagens *spam* transmitidas[7]. O custo mundial do *spam* foi estimado em 39 000 M€ em 2005. Os custos do *spam* para as principais economias europeias foram estimados em cerca de 3 500 M€ na Alemanha, 1 900 M€ no Reino Unido e 1 400 M€ em França[8]. Enviar *spam* é considerado "um negócio" em si mesmo. Os comerciantes de *spam* alugam ou vendem às empresas, para fins de marketing, listas de endereços de correio electrónico por eles coligidos. O *spam* pela Internet, devido ao alcance deste meio de comunicação e ao baixo custo do envio de mensagens em massa, é especialmente lucrativo. Ao mesmo tempo, é possível também obter resultados significativos com investimentos modestos no combate ao *spam*. A título de exemplo, nos Países Baixos, conseguiu-se reduzir o *spam* neerlandês em 85 % investindo **570 000 €** em equipamento anti-*spam*.

De um mero incómodo, as mensagens de correio electrónico não solicitadas adquiriram um carácter cada vez mais fraudulento e criminoso. Um exemplo bem conhecido é a utilização do correio para a prática de *phishing*, que, de forma enganadora, leva os utilizadores finais a revelarem dados sensíveis através de falsos sítios Web que, pretensamente, representam empresas verdadeiras, o que coloca o problema de uma eventual fraude a nível da identidade e de danos causados à reputação das empresas. A disseminação de *spyware* pelo correio electrónico ou através de software com o fim de detectar e comunicar o comportamento em linha de um utilizador continua a aumentar. O *spyware* pode, nomeadamente, recolher informações pessoais, como senhas de entrada e números de cartões de crédito.

O envio de quantidades maciças de correio electrónico não solicitado é amplamente facilitado pela difusão de código maligno, como "vermes" e vírus. Uma vez instalados, permitem que um atacante assuma o controlo de um sistema informático infectado e o transforme num "botnet"[9], escondendo a identidade de quem, verdadeiramente, está na origem do *spam*. Os "botnets" são utilizados por quem se dedica a actividades de *spam*, de *phishing* e de venda de *spyware* para fins fraudulentos e criminosos. Os peritos do sector estimam que os "botnets" difundem mais de 50 % das mensagens de correio electrónico abusivas[10]. A difusão generalizada de *spyware* e de outros tipos de código maligno que atacam os consumidores e

---

4 O termo *spam* refere-se ao envio de comunicações não solicitadas – por exemplo, por correio electrónico - para fins comerciais. No entanto, as mensagens electrónicas não solicitadas podem também transportar software maligno (*malware*) e espião (*spyware*).

5 Em 2001 o *spam* representava 7% do tráfego mundial de correio electrónico.

6 Symantec 54 %; Messagelabs 68,6 %; MAAWG 80-85 %.

7 Primeiro trimestre de 2006 (Sophos) Ásia 42,8 %; América do Norte 25,6 %; Europa 25,0 %; América do Sul, 5,1 %; Australásia 0,8 %; África 0,6 %; outros 0,1 %.

8 Estudo Ferris, 2005.

9 "Botnets" são computadores "sequestrados" utilizados pelos difusores de *spam* para enviarem correio electrónico por grosso através da instalação de software oculto que transforma os computadores em servidores de correio sem o conhecimento dos utilizadores.

10 Países mais afectados pelos "botnets", segundo a Symantec, (3.º e 4.º trimestres de 2005): EUA 26 %, Reino Unido 22 %, China 9 %, França, Coreia do Sul, Canadá 4 %, Taiwan, Espanha, Alemanha 3 %, Japão 2 %.

as empresas tem um impacto económico considerável. O impacto financeiro global do *malware* foi estimado em cerca de 11 000 M€ em 2005[11].

3. MEDIDAS TOMADAS ATÉ À DATA – ACÇÕES REALIZADAS DESDE 2004

A UE adoptou em 2002 uma **Directiva relativa à privacidade e às comunicações electrónicas**, que **proíbe o *spam*[12]** e introduz o princípio do consentimento para o *marketing* destinado às pessoas singulares. Em Janeiro de 2004, a Comissão apresentou uma Comunicação relativa ao *spam* em que identificava acções que podiam complementar a Directiva[13]. A Comunicação sublinhava a necessidade de acção por parte de vários actores nos domínios da sensibilização, auto-regulação/medidas técnicas, cooperação e actuação repressiva. A Comissão começou a incluir a questão do combate ao *spam*, ao *spyware* e ao *malware* no diálogo com os países terceiros. Além disso, a Directiva relativa às práticas comerciais desleais[14] protege os consumidores contra as práticas comerciais agressivas. A cooperação transfronteiras para combater tais práticas está prevista no Regulamento relativo à cooperação no domínio da defesa do consumidor[15].

3.1. Acções de sensibilização

A Comunicação da Comissão contribuiu para aumentar a sensibilização para o problema do *spam* a nível nacional e internacional por todo o mundo. A nível da UE, o **programa Safer Internet *plus*** promove a utilização mais segura da Internet e das novas tecnologias em linha, em particular no respeitante às crianças, e insere-se numa abordagem coerente adoptada pela União Europeia.

Os Estados-Membros lançaram ou apoiaram **campanhas** destinadas a sensibilizar os utilizadores para o problema do *spam* e para o modo de lidar com ele. Regra geral, os FSI (fornecedores de serviços Internet) assumiram a responsabilidade de fornecerem aos seus clientes recomendações e assistência para se protegerem contra o software espião e os vírus. Em Fevereiro de 2004, a Comissão foi a anfitriã de um **seminário** da OCDE sobre *spam*. A Comissão também contribuiu activamente para o **Anti-*Spam* Toolkit** (à letra "estojo de ferramentas anti-*spam"*) da OCDE, que fornece um conjunto completo de opções regulamentares, soluções técnicas e iniciativas do sector para combater o *spam*.

A Cimeira Mundial das Nações Unidas sobre a Sociedade da Informação[16] **reconheceu** que o problema do *spam* devia ser tratado nas instâncias nacionais e internacionais competentes. A UIT realizou, em 2004 e 2005, conferências temáticas no âmbito da WSIS. A Agenda de Túnis da WSIS, adoptada em Novembro de 2005, apela à resolução eficaz dos problemas significativos e crescentes criados pelo *spam*[17].

---

11 Computer Economics: the 2005 Malware Report.
12 Art. 13.º da Directiva 2002/58.
13 Ver nota 3.
14 Directiva 2005/29/CE, anexo I, ponto 26.
15 Regulamento (CE) n.º 2006/2004.
16 WSIS, Genebra, Dezembro de 2003.
17 Agenda de Túnis, ponto 41.

3.2. Cooperação internacional

Sendo um problema que atravessa transfronteiras, o *spam* é já objecto de várias iniciativas de cooperação e para ele foram criados mecanismos transfronteiras de repressão. A Comissão criou a chamada **Contact Network of *Spam* Authorities** (CNSA) (rede de contacto das autoridades responsáveis pelo combate ao *spam*), que se reúne regularmente, divulga entre os seus membros as melhores práticas e coopera em matéria de actuação repressiva nos diversos países. A CNSA elaborou um procedimento de cooperação[18] para facilitar o tratamento transnacional das queixas relativas ao *spam*.

Os serviços da Comissão apoiam e participam como observadores no **Plano de Acção de Londres** (PAL), que reúne as autoridades policiais e judiciais competentes de 20 países e também adoptou um procedimento de cooperação transnacional. Em Novembro de 2005, realizou-se um seminário misto CNSA – PAL. A **OCDE** adoptou, em Abril de 2006, uma recomendação sobre cooperação transfronteiras na repressão do *spam*, que insta as autoridades policiais a partilharem informações e a trabalharem em conjunto[19].

A Comissão promove, além disso, **iniciativas a nível da cooperação internacional**. Os EUA e a UE acordaram em cooperar no combate ao *spam* através de iniciativas conjuntas a nível da actuação repressiva, e estudar os métodos de combate ao *spyware* e *malware* ilegais. A Comissão participa, além disso, no grupo de trabalho sobre *spam* da Canadian International Collaboration. O problema está a ser discutido com importantes parceiros internacionais, como a China e o Japão. Relativamente à Ásia, a Comissão elaborou uma Declaração Conjunta sobre cooperação internacional anti-*spam*, que foi adoptada em Fevereiro de 2005 na conferência da ASEM (Asia-Europe Meeting) dedicada ao comércio electrónico[20].

A Agenda de Túnis, adoptada pela Cimeira Mundial da Sociedade da Informação em Novembro de 2005, sublinha que a segurança da Internet é um domínio que requer maior cooperação internacional e que esta questão terá de ser abordada no quadro do modelo de cooperação reforçada para o governo da Internet, que será implementado na sequência da Cimeira[21].

3.3. Investigação e Desenvolvimento Tecnológico

No âmbito do Sexto Programa-Quadro de IDT, a Comissão lançou alguns projectos destinados a ajudar as partes interessadas a combater o *spam* e outras formas de software maligno. Estes projectos[22] incidiram em temas como a monitorização geral das redes e a detecção de ataques até ao desenvolvimento específico de tecnologias de filtragem que detectam *spam*, *phishing* e *malware*. Entre as realizações de sucesso desses projectos conta-se o estabelecimento de uma comunidade de investigadores dedicada à contenção do *malware* e o desenvolvimento de uma infra-estrutura europeia destinada a monitorizar o tráfego na Internet. Recentemente, iniciaram-se actividades de investigação em matéria de filtros para

---

18 http://europa.eu.int/information_society/policy/ecomm/doc/todays_framework/privacy_protection/*spam*/cooperation_procedure_cnsa_final_version_20041201.pdf

19 http://www.oecd-antispam.org/

20 http://www.asemec-london.org/

21 Agenda de Túnis, pontos 39-47. http://www.itu.int/wsis/docs2/tunis/off/6rev1.doc

22 www.diademhttp://cordis.europa.eu/fp6/projects.htm#search

phishing adaptativos, capazes de detectar ameaças desconhecidas, e de ciber-ataques. O esforço financeiro consagrado a estas actividades ascende a 13,5 M€.

3.4. Acções desenvolvidas pelo sector

A Comissão saúda o papel activo do sector no respeitante ao *spam*. Os fornecedores de serviços, de um modo geral, tomaram **medidas de carácter técnico** para resolver o problema do *spam*, incluindo melhores filtros. Os FSI criaram um **balcão de apoio** e fornecem aos utilizadores software anti-*spam*, *spyware* e *malware*. Muitos FSI instauraram **cláusulas contratuais** que proíbem as práticas fraudulentas em linha. Num processo judicial civil recente no Reino Unido, foi imposta uma coima de 68 800 € a um difusor de *spam* por violação de contrato. Grupos do sector adoptaram as melhores práticas para impedir o *phishing* em linha e melhorar os métodos de filtragem[23].

Os operadores de comunicações móveis também estão activos. Os códigos de conduta do sector prevêem a tomada de medidas contra as mensagens não solicitadas. A associação GSM publicou, em 2006, um Código de Práticas em matéria de *spam* móvel. Neste momento, a Comissão co-financia a iniciativa Spotspam (à letra "detectar o *spam"*), uma parceria entre entidades públicas e privadas, que visa construir uma base de dados para facilitar a investigação e a actuação repressiva em casos que envolvam *spam*[24].

3.5. Actuação repressiva

Não há dúvidas de que o combate ao *spam* produz resultados. As medidas de filtragem impostas na Finlândia reduziram a percentagem de *spam* nas mensagens de correio electrónico enviadas de 80 % para cerca de 30 %. Muitas autoridades reforçaram as medidas repressivas para travar os difusores de *spam*[25].

Existem, porém, diferenças significativas entre os Estados-Membros no respeitante ao número real de processos instaurados. Algumas autoridades iniciaram pelo menos uma centena de investigações bem sucedidas e que conduziram a uma penalização das actividades relacionadas com o *spam*. Noutros Estados-Membros, o número de processos investigados foi muito reduzido ou mesmo nulo.

A maioria das acções visou as **formas "tradicionais"** de *spam*; **outras ameaças detectadas foram praticamente ignoradas em termos de acção judicial**, apesar de criarem riscos importantes.

4. O QUE HÁ A FAZER DAQUI PARA A FRENTE

4.1. Medidas a nível dos Estados-Membros

A presente secção abrange as acções que devem ser desenvolvidas pelos governos e as autoridades nacionais no que respeita sobretudo à actuação repressiva e à cooperação.

---

23 http://www.maawg.org/home/

24 http://www.spotspam.net

25 Um inquérito da CNSA revelou que quinze dos dezoito membros que responderam instauraram processos no período compreendido entre 2003 e 2006.

4.1.1. Factores determinantes de sucesso

A persistência e a natureza evolutiva do problema exige um maior envolvimento e o estabelecimento de prioridades pelos Estados-Membros. As acções devem visar sobretudo os "profissionais" de *spam* e de *phishing* e a difusão de *spyware* e *malware*. Os factores determinantes de sucesso são:

– Um forte empenhamento dos governos centrais no combate às práticas ilícitas em linha

– Uma clara responsabilidade organizacional pelas actividades repressivas

– Recursos adequados para as autoridades policiais e judiciais competentes.

Actualmente, estes factores não estão presentes em todos os Estados-Membros.

4.1.2. Coordenação e integração a nível nacional

Nos termos da Directiva relativa à protecção da privacidade nas comunicações electrónicas e da Directiva relativa à protecção geral dos dados[26], as autoridades nacionais têm poderes para agir contra as seguintes práticas ilegais:

- envio de comunicações não solicitadas (***spam***)[27]**;**

- acesso ilícito a equipamentos terminais, quer para armazenar informações – como programas de ***adware*** (software de publicidade) e ***spyware*** – quer para aceder às informações armazenadas nesses equipamentos[28];

- infecção de equipamentos terminais através da introdução de ***malware***, como vermes e vírus, e da transformação dos computadores pessoais em ***botnets*** ou sua utilização para outros fins[29]**;**

- operação que consiste em levar os utilizadores a revelarem informações sensíveis[30], como senhas e dados sobre os cartões de crédito, através das chamadas mensagens de ***phishing***.

Algumas destas práticas estão também abrangidas pelo direito penal, incluindo a *Decisão-quadro relativa a ataques contra os sistemas de informação*[31]. De acordo com a Decisão, os Estados-Membros têm de prever uma pena de prisão máxima não inferior a três anos, ou cinco anos se se tratar de crime organizado.

A nível nacional, estas disposições podem ser aplicadas por órgãos administrativos e/ou pelas autoridades competentes em matéria penal. Se for este o caso, as **responsabilidades das** diferentes autoridades e os procedimentos de cooperação precisam de ser claramente definidos, o que pode exigir a tomada de decisões a um nível elevado da hierarquia dos governos nacionais.

---

26 Directiva 95/46/CE

27 Art. 13.º da Directiva "Privacidade e Comunicações Electrónicas".

28 N.º 3 do artigo 5.º da Directiva "Privacidade e Comunicações Electrónicas".

29 Ver nota 28.

30 N.º 1, alínea a), do artigo 6.º da Directiva relativa à protecção geral dos dados.

31 Decisão-Quadro do Conselho 2005/222/JHA.

Até à data, os aspectos penais e administrativos cada vez mais interligados do *spam* e de outras ameaças não se têm traduzido num crescimento correspondente dos procedimentos de cooperação nos Estados-Membros de forma a reunir as competências técnicas e investigativas dos diferentes organismos. São necessários protocolos de cooperação que abranjam domínios como a troca de informações e de informações secretas, dados de contacto, assistência e transferência de processos.

Uma estreita cooperação entre as autoridades policiais/judiciais, operadores de redes e FSI a nível nacional é também benéfica em termos de troca de informações, de aquisição de competências técnicas e de repressão de práticas ilícitas em linha. As autoridades da Noruega e dos Países Baixos forneceram informações que confirmaram a utilidade dessas parcerias público-privadas.

4.1.3. Recursos

Há que dispor de recursos para reunir provas, conduzir as investigações e instaurar processos. As autoridades precisam de dispor de recursos técnicos e legais e têm de familiarizar-se com o modo como os criminosos operam para poderem pôr fim às suas práticas.

Os mecanismos de apresentação de queixas em linha, com os sistemas associados de registo e análise das práticas ilícitas comunicadas, podem ser uma ferramenta importante. A experiência mostra que **investimentos modestos** podem produzir **resultados significativos**. A redução do *spam* nos Países Baixos foi conseguida através da criação de uma equipa específica composta por 5 funcionários a tempo inteiro da OPTA, a autoridade competente neerlandesa, dotados de equipamentos no valor de **570 000 €** para combaterem o *spam*. Com base neste investimento, a experiência adquirida em matéria de combate ao *spam* está agora a ser utilizada para atacar outros problemas.

4.1.4. Cooperação transfronteiras

O *spam* é um problema de dimensão mundial. As autoridades nacionais dependem muitas vezes das autoridades de outros países para processar os difusores de *spam*, ou, em sentido inverso, são solicitadas para prosseguir as investigações iniciadas noutros países.

Embora possa haver uma certa relutância em afectar recursos nacionais, que são escassos, à investigação dos problemas de terceiros, é importante que os Estados-Membros reconheçam que uma cooperação transfronteiras eficaz é um elemento essencial no combate ao *spam*. Recentemente, as autoridades australianas e neerlandesas responsáveis pelo combate ao *spam* cooperaram para fazer abortar uma grande operação de *spam*.

Até à data, 21 autoridades europeias subscreveram o procedimento de cooperação da CNSA (Contact Network of *Spam* Authorities)[32] para o tratamento transfronteiras de queixas; sugere-se às restantes autoridades que façam o mesmo nos próximos meses. Sugere-se aos Estados-Membros e às autoridades competentes, nomeadamente, que promovam activamente a utilização:

- dos documentos *pro forma* comuns CNSA-LAP (Plano de Acção de Londres)

[32] Ver nota 18.

- da Recomendação e do *Toolkit* (conjunto de ferramentas) da OCDE para o combate ao *spam*.

4.1.5 Acções propostas

Instam-se os Estados-Membros e as autoridades competentes a: - definirem claramente as responsabilidades dos organismos nacionais envolvidos no combate ao *spam*; - garantirem uma coordenação eficaz entre as autoridades competentes; - envolverem os intervenientes no mercado a nível nacional, tirando partido das suas competências especializadas e das informações de que dispõem; - garantirem a disponibilização de recursos adequados para a actuação repressiva; - subscreverem os procedimentos de cooperação internacional e darem resposta aos pedidos de ajuda transfronteiras.

4.2. Medidas a tomar pelo sector

Esta secção diz respeito às medidas que o sector pode tomar para promover a confiança dos consumidores e moderar o envio de mensagens de correio electrónico abusivas.

4.2.1. Envio e instalação de software

O software espião (*spyware*) constitui uma séria ameaça à privacidade dos utilizadores. As ofertas de software em linha tornaram-se num dos métodos mais utilizados para o **envio e instalação de *spyware*** no equipamento terminal do utilizador. O *spyware* pode também ser dissimulado em software distribuído através de outros meios, como CD-ROM para instalação num computador. Juntamente com o software adquirido pelo consumidor podem ser instalados programas espiões não desejados.

Indicam-se seguidamente algumas medidas destinadas a impedir que o software espião atinja os utilizadores finais.

4.2.2. Informar o consumidor

As ofertas de software podem incluir a instalação de outros programas. Quando este software adicional funciona como *spyware* controlando o comportamento dos utilizadores finais (para fins de marketing, por exemplo), estamos perante o tratamento de dados pessoais, que é ilegal sem o consentimento prévio do utilizador. Em muitos casos, o consentimento do utilizador para a instalação de tal software ou não é obtido ou é quase invisível no texto em letra muito pequena do longo acordo relativo à licença do utilizador final.

As empresas que oferecem produtos de software devem descrever clara e destacadamente todos os termos e condições da oferta, em particular se houver tratamento de dados pessoais por dispositivos de monitorização incluídos nos pacotes de software.

A auto-regulação e a utilização de uma espécie de "selo de aprovação" podem ser um meio eficaz de distinguir as empresas de confiança das que o não são. Os códigos de conduta, cujo

objectivo é informar o utilizador das condições que implicam o tratamento de dados pessoais, podem ser submetidos à aprovação do grupo de trabalho sobre protecção de dados (Grupo de Trabalho do artigo 29.º).

4.2.3 Cláusulas contratuais na cadeia da oferta

Muitas vezes, as empresas **não têm conhecimento** do modo como os anúncios aos seus produtos e serviços estão a ser tecnicamente transmitidos ao público. O software legítimo pode ir acompanhado de *spyware* utilizado para ganhar acesso a dados sensíveis, incluindo dados dos cartões de crédito, documentos confidenciais, etc.

As empresas que anunciam e/ou vendem produtos devem garantir que as actividades das suas partes contratantes são legítimas. Uma empresa precisa de compreender as relações na cadeia de contratantes, controlar a conformidade legal e impor a cessação do contrato por práticas ilícitas em qualquer ponto da cadeia, para que a relação contratual com empresas que se dedicam a práticas fraudulentas possa terminar imediatamente.

4.2.4. Medidas de segurança a tomar pelos fornecedores de serviços

Um inquérito efectuado pela ENISA em 2006[33] confirma que os fornecedores de serviços, em geral, tomaram medidas para combater o *spam*. O inquérito conclui, no entanto, que eles podem contribuir mais para a segurança geral da rede, e recomenda que se dê maior atenção à filtragem do correio electrónico que sai da rede de um fornecedor de serviços (**filtragem na saída)**. A Comissão insta os fornecedores de serviços a aplicarem essa recomendação.

O grupo de trabalho sobre protecção de dados, ou do artigo 29.º, adoptou um parecer sobre as questões da privacidade associadas à oferta de serviços de triagem do correio electrónico[34] que fornece orientações em matéria de confidencialidade das comunicações por correio electrónico e, mais especificamente, em matéria de filtragem das comunicações em linha contra vírus, *spam* e conteúdos ilícitos.

4.2.5. Acções propostas

A Comissão propõe:

- às empresas - que garantam que as informações-tipo para a aquisição de aplicações de software sejam conformes com a legislação em matéria de protecção de dados;

- às empresas - que proíbam contratualmente a utilização ilegal de software nos anúncios, controlem o modo como os anúncios chegam aos consumidores e estejam atentas às práticas ilícitas.

- aos fornecedores de serviços de correio electrónico - que apliquem uma política de filtragem que garanta a conformidade com a recomendação e as orientações sobre filtragem do correio electrónico.

33 http://www.enisa.eu.int/doc/pdf/deliverables/enisa_security_spam.pdf

34 Parecer 2/2006, WP 118.

4.3. Acções a nível europeu

A Comissão continuará a abordar as questões relacionadas com o *spam*, o *spyware* e o *malware* nos fóruns internacionais, nas reuniões bilaterais e, se necessário, através de acordos com países terceiros, e continuará a promover a cooperação entre as partes interessadas, incluindo os Estados-Membros, as autoridades competentes e as empresas do sector. A Comissão tomará também novas iniciativas no domínio da legislação e da investigação, destinadas a dar novo ímpeto à luta contra as práticas ilícitas que corroem a sociedade da informação. A Comissão tem neste momento em mãos o desenvolvimento de uma política coerente para o combate à cibercriminalidade, que será apresentada numa Comunicação cuja adopção está prevista para o início de 2007.

4.3.1. Revisão do quadro regulamentar

A Comunicação da Comissão[35] relativa ao quadro regulamentar das comunicações electrónicas propõe o reforço das regras em matéria de privacidade e de segurança. Nos termos da proposta, os operadores de rede e os fornecedores de serviços serão obrigados a:

- notificar a autoridade competente de um Estado-Membro de qualquer violação da segurança que tenha conduzido à perda de dados pessoais e/ou a interrupções na continuidade da oferta do serviço;

- notificar os seus clientes de qualquer violação da segurança que tenha conduzido à perda, modificação, acesso ou destruição dos seus dados pessoais.

As autoridades reguladoras nacionais terão poderes para garantir que os operadores implementam políticas de segurança adequadas e poderão ser estabelecidas novas regras que prevejam **remédios específicos** ou indiquem o **nível das sanções** expectável em caso de infracções.

4.3.2. Papel da ENISA

As propostas também incluem uma disposição que reconhece o papel de conselheira da ENISA (European Network and Information Security Agency) em questões de segurança. Está previsto a ENISA desempenhar outras tarefas, descritas na Comunicação da Comissão relativa a uma estratégia para a segurança[36], nomeadamente:

- construir uma parceria de confiança com os Estados-Membros e as partes interessadas com vista à criação de um **quadro adequado para a recolha de dados** sobre os incidentes de segurança e a confiança dos consumidores.

A ENISA coordenará cuidadosamente esse quadro com o Eurostat tendo em vista as estatísticas comunitárias sobre a sociedade da informação e o quadro de avaliação comparativa da iniciativa i2010[37].

---

35 http://europa.eu.int/information_society/policy/ecomm/tomorrow/index_en.htm

36 Ver nota 1.

37 Quadro de avaliação comparativa da iniciativa i2010 do Grupo de Alto Nível, de 20 de Abril de 2006.

- examinar a **viabilidade de um sistema europeu de alerta e partilha de informação** que facilite uma resposta eficaz às ameaças existentes e emergentes às redes electrónicas.

4.3.3. Investigação e desenvolvimento

O próximo programa-quadro (PQ7) visa o desenvolvimento contínuo dos conhecimentos e das tecnologias para tornar seguros os serviços e sistemas de informação, em estreita coordenação com as iniciativas políticas. Prevê-se que os temas de trabalho relativos ao *malware* incluam os *botnets* e os vírus escondidos, assim como os ataques aos serviços móveis e vocais.

4.3.4. Cooperação internacional

Sendo a Internet uma rede mundial, por todo o mundo tem de haver empenho em combater o *spam*, o *spyware* e o *malware*. Por conseguinte, a Comissão tenciona reforçar o diálogo e a cooperação com os países terceiros em matéria de luta contra estas ameaças e contra as actividades criminosas a elas associadas. Para isso, a Comissão procurará garantir que o *spam*, o *spyware* e o *malware* sejam objecto de acordos entre a UE e países terceiros, procurará obter o empenho firme dos países terceiros mais afectados pelo problema numa cooperação mais eficaz com os Estados-Membros da UE no combate a estas ameaças e acompanhará atentamente a efectiva consecução dos objectivos conjuntamente traçados.

4.3.5. Acções propostas

A Comissão:

- prosseguirá os seus esforços de sensibilização e de promoção da cooperação entre as partes interessadas;

- continuará a desenvolver acordos com países terceiros que incluam a questão do combate ao *spam*, ao *spyware* e ao *malware*;

- apresentará, no início de 2007, novas propostas legislativas que irão reforçar as regras em matéria de privacidade e de segurança no sector das comunicações, e uma política em matéria de cibercriminalidade;

- envolverá os especialistas em segurança da ENISA;

- apoiará as actividades de investigação e desenvolvimento no seu Sétimo Programa-Quadro.

5. CONCLUSÃO

Ameaças como o *spam*, o *spyware* e o *malware*, para além de terem um impacto financeiro significativo, minam a confiança na sociedade da informação e põem em causa a sua segurança. Embora alguns Estados-Membros tenham tomado iniciativas, na União Europeia em geral **as medidas tomadas são insuficientes para travar esta evolução**. A Comissão utiliza o seu papel de intermediária para alertar para a necessidade de aumentar o empenho político na luta contra estas ameaças.

Os esforços a nível da actuação repressiva têm de ser acelerados para cercear a actividade dos que conscientemente violam a lei. O sector deve tomar novas medidas

para complementar as acções repressivas. Tem de haver cooperação a nível nacional, tanto entre os órgãos dos governos, como entre os governos e o sector. A Comissão intensificará o diálogo e a cooperação com os países terceiros, estará atenta à situação para decidir da oportunidade de apresentar novas propostas legislativas e orientará as actividades de investigação para o reforço da privacidade e da segurança no sector das comunicações electrónicas.

A realização integrada e, sempre que possível, em paralelo, das acções identificadas na presente comunicação pode contribuir para reduzir as ameaças que actualmente põem em causa os benefícios da sociedade da informação e a economia.
A Comissão monitorizará a realização destas acções e avaliará, até 2008, a necessidade de outras acções.