COMISSÃO DAS COMUNIDADES EUROPEIAS

Bruxelas, 22.01.2004
COM(2004) 28 final

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

sobre as comunicações comerciais não solicitadas, ou "spam"

ÍNDICE

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

sobre as comunicações comerciais não solicitadas, ou "spam"

(Texto relevante para efeitos do EEE)

RESUMO

As comunicações comerciais não solicitadas por correio electrónico, também conhecidas por "spam", atingiram proporções preocupantes. Neste momento, estima-se que mais de 50% do tráfego mundial de correio electrónico é "spam". Mais preocupante ainda é a sua taxa de crescimento: em 2001, esse tipo de comunicações representava "apenas" 7% do tráfego mundial de correio electrónico.

O "spam" constitui um problema por várias razões: desrespeito da privacidade, engano dos consumidores, protecção dos menores e da dignidade humana, custos extraordinários para as empresas, perda de produtividade. A nível mais geral, o "spam" reduz a confiança dos consumidores, a qual constitui um requisito prévio para o êxito do comércio e dos serviços electrónicos e, naturalmente, para a sociedade da informação.

Prevendo esse perigo, a UE adoptou, em Julho de 2002, a Directiva 2002/58/CE, relativa à privacidade e às comunicações electrónicas, que introduziu em toda a UE o princípio do marketing baseado no consentimento prévio (*opt-in*) para o correio electrónico (incluindo as mensagens móveis SMS ou MMS) e salvaguardas complementares para os consumidores. O prazo para a transposição da referida directiva terminava em 31 de Outubro de 2003. Foram iniciados procedimentos de infracção contra uma série de Estados-Membros que não notificaram as medidas de transposição à Comissão.

Embora a adopção de legislação seja um primeiro passo necessário, esta constitui, no entanto, apenas uma parte da resposta. A presente comunicação define uma série de acções que devem necessariamente complementar as regras comunitárias, de modo a tornar a proibição do "spam" uma realidade.

Não existe, porém, uma solução milagrosa para o problema do "spam". A série de acções identificadas na presente comunicação centra-se sobretudo no controlo eficaz da aplicação da legislação pelos Estados-Membros e as autoridades públicas, nas soluções técnicas e auto-reguladoras da indústria e na sensibilização dos consumidores. A dimensão internacional também é focada, dado que muito do "spam" provém de fora da União Europeia.

Embora estas acções reflictam amplamente o consenso surgido ao longo de 2003, como confirmado numa reunião de trabalho pública realizada em Outubro de 2003, será igualmente essencial estabelecer um consenso sobre a sua implementação. Apenas será possível pôr cobro à proliferação do "spam", se todos os envolvidos, desde os Estados-Membros e autoridades públicas até aos consumidores e utilizadores da Internet e das comunicações electrónicas, passando pelas empresas, desempenharem o seu papel.

Algumas destas acções têm um custo óbvio. Mas é o preço a pagar pela sobrevivência do correio e dos serviços electrónicos enquanto ferramenta de comunicação eficaz.

A implementação das acções definidas na presente comunicação contribuirá fortemente para reduzir a quantidade de "spam", em benefício da sociedade da informação, dos cidadãos e da economia.

Contexto e objectivo

As comunicações comerciais não solicitadas recebidas por correio electrónico[1], também conhecidas por "spam", são, reconhecidamente, um dos problemas mais importantes com que a Internet se defronta hoje em dia. O "spam" atingiu proporções preocupantes. Neste momento, existe o risco de os utilizadores do correio electrónico ou do SMS deixarem pura e simplesmente de o utilizar – apesar de ser uma das aplicações preferidas da Internet – ou de utilizar os serviços móveis, ou de deixarem de os utilizar tanto quanto o fariam noutras circunstâncias. De um modo mais geral, atendendo a que se espera que a Internet e outras comunicações electrónicas (por exemplo, os serviços de banda larga, o acesso sem fios, as comunicações móveis) sejam um elemento determinante para o crescimento da produtividade nas economias modernas, o "spam" exige um olhar ainda mais atento.

Embora seja consensual que é necessário agir antes que os benefícios que o correio electrónico e outros serviços electrónicos trazem para as empresas e os cidadãos sejam anulados pela proliferação do "spam", o modo de o combater não é imediatamente evidente. Sobretudo, não existe uma solução milagrosa para o problema. Apenas será possível combater eficazmente o "spam", se todos os envolvidos, desde os Estados-Membros e autoridades públicas até aos consumidores e utilizadores da Internet e das comunicações electrónicas, passando pelas empresas, desempenharem o seu papel.

A presente comunicação identifica as acções a realizar nas diversas frentes, jurídica, técnica e de sensibilização, com base na Directiva 2002/58/CE, estabelecendo um regime baseado no consentimento prévio ("opt-in"), que os Estados-Membros tinham de implementar para as comunicações comerciais até 31 de Outubro de 2003[2].

Esta série de acções centra-se, em particular, na aplicação e controlo efectivo do cumprimento da referida directiva pelos Estados-Membros, nas medidas técnicas, na auro-regulação pelo sector, na sensibilização dos consumidores e na cooperação internacional. A dimensão internacional é, na verdade, fundamental, dado que grande parte do "spam" parece provir de fora da União Europeia e, em particular, da América do Norte[3].

---

1 A presente comunicação não abrange as comunicações não solicitadas não electrónicas, como, por exemplo, o correio postal não solicitado.

2 Ver, nomeadamente, o artigo 13º da Directiva 2002/58/CE relativa à privacidade e às comunicações electrónicas (ver secção 2, mais adiante).

3 Por exemplo, as iniciativas 'spam box', organizadas em 2002 pela 'Commission Nationale Informatique et Libertés (CNIL)' (francesa) e pela 'Commission de la Protection de la Vie Privée (CPVP)' (belga), pareceram confirmar que os Estados Unidos e, em menor escala, o Canadá, eram a principal fonte das mensagens "spam". As conclusões da CPVP podem ser consultadas em http://www.privacy.fgov.be/publications/spam_4-7-03_fr.pdf; o relatório da CNIL encontra-se disponível no seguinte endereço URL: http://www.cnil.fr/thematic/docs/internet/boite_a_spam.pdf. Ver também: UNCTAD, E-Commerce and Development Report 2003, New York and Geneva, 2003, p. 27.

As acções reflectem amplamente o consenso surgido ao longo de 2003[4]. O consenso nesta matéria é tanto mais importante quanto compete sobretudo a essas partes interessadas, com o apoio da Comissão, quando possível, implementar as acções identificadas, para benefício da sociedade da informação, da indústria e dos utilizadores.

Estrutura do documento

O documento identifica os aspectos específicos do problema do "spam" e propõe acções específicas de resposta a cada um deles. Apontam-se também, sempre que se considerou útil, as melhores práticas.

A estrutura de apresentação das acções propostas é a seguinte:

- **Acções a nível da aplicação e controlo do cumprimento da legislação** para os governos e as autoridades públicas em particular, em domínios como a reparação judicial e as sanções, os mecanismos de apresentação de queixas, a apresentação de queixas a nível transnacional, a cooperação com os países terceiros e a monitorização (Secção 3).

- **Acções a nível da auto-regulação e da tecnologia** para os intervenientes no mercado em particular, em domínios como as disposições contratuais, os códigos de conduta, as práticas de marketing aceitáveis, os rótulos, os mecanismos alternativos de resolução de litígios, as soluções técnicas, como, por exemplo, a filtragem e a segurança (Secção 4).

- **Acções de sensibilização**, que abrangem a prevenção, a educação dos consumidores, os mecanismos de comunicação de ocorrências, a desenvolver pelos governos e as autoridades públicas, os intervenientes no mercado e as associações de consumidores e afins (Secção 5).

No final da comunicação, apresenta-se um quadro que sistematiza estas acções. As acções estão interrelacionadas em vários aspectos, pelo que devem ser, tanto quanto possível, implementadas em paralelo e de uma maneira integrada.

Antes de se abordarem as acções propriamente ditas, analisa-se sucintamente, nas próximas secções, o "spam" (Secção 1) e recapitulam-se as novas regras aplicáveis desde 31 de Outubro de 2003 (Secção 2).

---

[4] Antes da reunião de trabalho, foi distribuído um documento temático sobre as comunicações não solicitadas, ou "spam". O documento baseou-se, ele próprio, em discussões prévias no contexto do Comité das Comunicações (COCOM) e do Grupo de Trabalho do "Artigo 29.º" para a Protecção dos Dados. Os membros deste comité e do grupo de trabalho forneceram informações em resposta a um questionário. Também se obtiveram reacções de uma série de associações industriais e de empresas individuais, desde FSI (fornecedores de serviços Internet) a fabricantes de computadores e software, passando por empresas de marketing directo e publicitários.

1. SPAM – O PROBLEMA

Spam: O que é?

O termo "spam" é mais vezes usado do que definido. O termo sucinto é normalmente utilizado para designar as mensagens electrónicas não solicitadas, muitas vezes a mesma mensagem para uma multiplicidade de destinatários. A nova directiva não define nem utiliza o termo "spam". Utiliza os conceitos de "comunicações não solicitadas" "por correio electrónico", "para fins de comercialização directa", os quais, no seu conjunto, cobrem efectivamente a maior parte das espécies de "spam". O conceito de "spam" é, por conseguinte, utilizado na presente comunicação como a designação sucinta de correio electrónico comercial não solicitado.

Note-se que o próprio conceito de "correio electrónico" abrange não só o correio electrónico tradicional baseado no SMTP, mas também o SMS, o MMS e, na realidade, qualquer forma de comunicação electrónica para a qual não é exigida a participação simultânea do remetente e do destinatário (ver Secção 2, adiante).

1.1. A dimensão do problema

O correio electrónico comercial não solicitado, ou "spam", atingiu números preocupantes. Apesar das estatísticas variarem, estima-se em geral que mais de 50% do tráfego mundial de correio electrónico seja "spam".

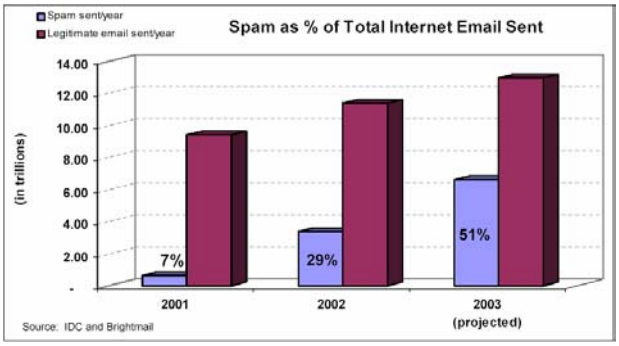

Figura 1: Percentagem de "spam" no total do correio electrónico enviado pela Internet

A sua taxa de crescimento é ainda mais preocupante. Em 2001, estimou-se que o "spam" constituía "apenas" 7 % do tráfego mundial de correio electrónico. Em 2002, foi estimado em 29 %. As projecções para 2003 apontam para 51 %.

Pode haver variações significativas entre as diversas categorias de utilizadores e entre as regiões do mundo. (Na Comissão Europeia, por exemplo, estima-se que 30% das mensagens electrónicas provenientes do exterior sejam "spam".) No geral, porém, os números mais recentes referentes à UE não são menos preocupantes que os números mundiais[5].

Embora as comunicações não solicitadas, ou "spam", nas redes móveis, através, por exemplo, das mensagens em texto do Serviço de Mensagens Curtas (Short Message Service (SMS)), pareçam não constituir actualmente um problema grave, a evolução para o correio electrónico em redes móveis permite prever um aumento do volume de "spam". A experiência em países onde se regista uma elevada taxa de utilização dos serviços de Internet móvel *I-mode* (no Japão, por exemplo) confirma essa ameaça.

---

[5] Em Setembro de 2003, o "spam" foi estimado em 49 % na UE, ao passo que, no mesmo período, essa percentagem era de cerca de 54 % a nível mundial (Fonte: Brightmail, 2003).

1.2. Por que razão o "spam" constitui um problema

Do ponto de vista das pessoas, o "spam" é uma invasão da privacidade. Esta preocupação está no centro das novas regras para as comunicações não solicitadas descritas na próxima secção. Além disso, o "spam" é, muitas vezes, fraudulento ou enganador. Uma percentagem importante do "spam" parece pretender seduzir os consumidores através de declarações falsas ou enganosas[6]. Infelizmente, há demasiados consumidores a responder efectivamente a estas mensagens falsas ou enganadoras[7]. As mensagens pornográficas podem igualmente causar grande mal-estar[8]. A limpeza das caixas de correio para eliminar o "spam" consome tempo e aumenta os custos para o consumidor quando são necessários meios de filtragem e outros recursos de software.

As pessoas importam-se?

O número de queixas apresentadas é um dos indicadores das procupações expressas pelos utilizadores. Em 3 meses, o Spam Box francês recebeu 325 000 mensagens. Uma experiência semelhante na Bélgica conduziu à apresentação de 50 000 queixas em dois meses e meio[1]. A "spam box" permanente da FTC, a chamada base de dados UCE, estava a receber 130 000 mensagens por dia nos primeiros meses de 2003[1].

O "spam" atingiu um ponto em que também cria custos consideráveis para as empresas. Em termos de custos directos, os funcionários são também obrigados a limpar as caixas de correio, o que provoca uma diminuição da eficiência ou da produtividade no trabalho. Os departamentos de informática gastam tempo e dinheiro a tentar solucionar o problema. Os fornecedores de serviços Internet (FSI) e os fornecedores de serviços de correio electrónico (FSCE) têm de comprar mais largura de banda e mais capacidade de armazenagem para as mensagens electrónicas não desejadas. Existe também o risco de o "spam" suscitar a atribuição de responsabilidades a quem o recebe (por exemplo, conteúdos nocivos nos computadores pessoais dos trabalhadores) ou simplesmente - e

---

6 De acordo com um relatório recente da FTC, 22% do "spam" analisado continha informações falsas no campo "assunto"; em 42% o "assunto" era enganador, dando a entender que o remetente tinha qualquer relação comercial ou pessoal com o destinatário; 44% do "spam" continha informações falsas no campo "remetente" ou no campo "assunto"; mais de metade do "spam" relativo a finanças continha falsos remetentes ou falso "assunto"; 40% de todo o "spam" continha sinais de falsidade na mensagem; 90% das oportunidades de investimento e de negócio continhamafirmações provavelmente falsas; 66% do "spam" continha informações falsas no campo "remetente", no campo "assunto" ou no próprio texto da mensagem. (False Claims in Spam, A report by the FTC's Division of Marketing Practices, 30 de Abril de 2003, disponível em: http://www.ftc.gov/reports/spam/030429spamreport.pdf).

7 De acordo com a Pew Internet, 7% dos utilizadores do correio electrónico declararam ter feito uma encomenda na sequência de uma mensagem não solicitada e 33% dos utilizadores do correio electrónico clicaram numa ligação de uma mensagem não solicitada para obterem mais informações. Ainda que a percentagem de consumidores burlados se mantenha relativamente baixa, as economias de escala fenomenais que os comerciantes sem escrúpulos podem conseguir através do "spam" falso ou enganoso vieram conferir maior gravidade ao problema da "extorsão" dos consumidores. Ver: "Spam–How It Is Hurting Email and Degrading Life on the Internet", Outubro de 2003', Relatório de Deborah Fallows para o Pew Internet & American Life Project. Este relatório encontra-se disponível no endereço URL: http://www.pewinternet.org/reports/pdfs/PIP_Spam_Report.pdf. Um autor de correio electrónico multi-destinatários testemunhou recentemente no Spam Forum da FTC, organizado em Abril-Maio de 2003, que lucrava mesmo que a taxa de resposta fosse inferior a 0,0001%. (Observações de Timothy J. Muris Chairman, Federal Trade Commission, cimeira de Aspen, "Cyberspace and the American Dream", The Progress and Freedom Foundation, 19 de Agosto de 2003, Aspen, Colorado).

8 As mensagens "spam" também incluem, por vezes, violência gratuita ou incitamento ao ódio com base na raça, sexo, religião ou nacionalidade.

inconscientemente – o reenvia (por exemplo, inclusão errada na lista negra, danos à reputação). Existem também custos indirectos: algumas mensagens de correio electrónico comerciais ou empresariais legítimas não são entregues devido às actuais técnicas de filtragem anti-"spam" (as chamadas medidas falsamente positivas), ou simplesmente deixam de ser lidas devido à sua associação ao "spam". O "spam" é cada vez mais utilizado como veículo para espalhar vírus, o que pode revelar-se muito oneroso para as empresas.

Medir os custos do "spam" continua a ser uma tarefa difícil, em particular para os indivíduos, sobretudo porque é difícil atribuir um valor monetário a alguns dos danos causados. As estimativas, no entanto, são em geral inquietantes. A título ilustrativo, a Ferris Research calculou que, em 2002, o "spam" custou às empresas europeias 2 500 milhões de euros apenas em termos de perda de produtividade[9]. E, como atrás indicado, a quantidade de "spam" aumentou consideravelmente desde 2002. Segundo o fornecedor de software MessageLabs Ltd, em Junho de 2003, o custo do "spam" para as empresas britânicas foi de cerca de 3 200 milhões de libras[10]. As implicações do "spam" também podem variar em função dos sectores em causa. Por exemplo, o sector jurídico pode ser particularmente vulnerável aos efeitos do "spam", dadas as informações confidenciais e sensíveis com que lida.

Uma das consequências mais preocupantes do "spam" é o facto de reduzir a confiança dos utilizadores, a qual constitui um requisito prévio para o êxito do comércio electrónico e da sociedade da informação em geral. A percepção de que um sector retalhista é afectado por comerciantes "vigaristas" pode ter efeitos profundamente negativos na reputação dos comerciantes idóneos desse sector. Números recentes referentes aos Estados Unidos, onde a experiência com o "spam" é maior do que na UE, confirmam que muitas pessoas têm agora menos confiança no correio electrónico devido à enorme quantidade de "spam" que recebem[11].

Em termos mais gerais, prevê-se que a Internet e outras comunicações electrónicas – acesso em banda larga, acesso sem fios – sejam um elemento fundamental para o crescimento da produtividade nas economias modernas. No entanto, algumas características atraentes desses serviços –ligação permanente, acesso sem fios – são características passíveis de fazer aumentar a quantidade de "spam" recebido ou reenviado, se não se adoptarem medidas de segurança adequadas. Perversamente, porém, o crescimento de tais serviços poderá conduzir a um aumento do "spam", caso não sejam rapidamente implementadas medidas eficazes.

---

9 Fonte: Ferris Research, 2003.

10 Este número e outras estimativas vêm mencionados em: '"Spam"; Report of an Inquiry by the All Party Internet Group', Londres, Outubro de 2003, p. 8; este relatório pode ser consultado no seguinte endereço URL: http://www.apig.org.uk .

11 De acordo com o recente inquérito da Pew Internet acima mencionado, 25% dos entrevistados estavam a utilizar menos o correio electrónico devido à quantidade de "spam" que recebiam.

2. RESUMO DAS REGRAS RELATIVAS ÀS COMUNICAÇÕES COMERCIAIS NÃO SOLICITADAS

2.1. O regime de consentimento prévio ("opt-in")

A Directiva 2002/58/CE relativa à privacidade e às comunicações electrónicas (data-limite para a transposição: 31 de Outubro de 2003) exige que os Estados-Membros proíbam o envio de mensagens comerciais não solicitadas por correio electrónico ou outros sistemas de mensagens electrónicas (como o SMS e o Multimedia Messaging Service (MMS)) sem o consentimento prévio do assinante desses serviços de comunicações electrónicas (n.º 1 do artigo 13.º da directiva) [12]. Trata-se do sistema de "opt-in", até agora apenas aplicável aos faxes e aos aparelhos de chamadas automáticas[13].

Três regras básicas do novo regime:

Regra nº 1: As propostas comerciais por correio electrónico estão sujeitas ao consentimento prévio dos assinantes. Há uma pequena excepção para o correio electrónico (ou SMS) enviado aos clientes pela mesma pessoa sobre serviços ou produtos similares que tenha para oferecer. Este regime aplica-se aos assinantes que são pessoas singulares, mas os Estados-Membros podem optar por alargá-lo às pessoas colectivas.

Regra nº 2: É ilegal dissimular ou ocultar a identidade do remetente em nome do qual é efectuada a comunicação.

Regra nº 3: Todas as comunicações de correio electrónico para fins de comercialização devem incluir um endereço válido para o qual o destinatário possa comunicar que não deseja receber mais comunicações desse tipo ("opt-out").

No entanto, nem todas as comunicações de correio electrónico não solicitadas são proibidas. A regra prevê uma excepção nos casos em que, no contexto de uma venda, se tenham obtido as coordenadas para o envio de mensagens de correio electrónico ou SMS. Essa situação é muitas vezes designada por "soft opt-in". No âmbito dessa relação comercial com o cliente, a empresa que obteve os dados de um seu cliente pode utilizá-los para comercializar produtos ou serviços semelhantes aos já vendidos a esse mesmo cliente. Esta excepção foi harmonizada a nível comunitário e os Estados-Membros são obrigados a implementá-la. No entanto, esta excepção tem de ser redigida com rigor para evitar perverter efectivamente o regime de "opt-in". Não obstante, mesmo nessas circunstâncias, a empresa é obrigada a indicar claramente, da primeira vez que recolhe os dados, que eles podem ser utilizados para marketing directo (e, quando pertinente, que os dados poderão ser transmitidos a terceiros para esse efeito) e deverá oferecer ao cliente a possibilidade de rejeitar esta modalidade "gratuitamente e através de um meio simples". Além disso, cada mensagem comercial subsequente deve incluir um meio fácil para o cliente pôr termo, gratuitamente e com facilidade, a quaisquer mensagens posteriores ("opt-out").

---

12 Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva «Privacidade e Comunicações Electrónicas») JO L 201 de 31.7.2002.

13 Para as chamadas telefónicas comerciais, distintas das efectuadas com aparelhos de chamadas automáticas, os Estados-Membros podem optar por uma abordagem "opt-in" (consentimento prévio) ou "opt-out" (opção de exclusão).

O sistema de consentimento prévio ("opt-in") é obrigatório para qualquer mensagem de correio electrónico ou SMS dirigida a pessoas singulares para fins de marketing directo. Os Estados-Membros podem alargar esse sistema às comunicações que têm por destinatários as empresas (pessoas colectivas). Os Estados-Membros que tivessem optado por um sistema de "opt-out" para mensagens comerciais entre empresas, incluindo listas de "opt-out", podem continuar a fazê-lo. A aplicação de um regime diferenciado em função da natureza do assinante de um serviço de correio electrónico pode criar dificuldades específicas para os remetentes quando se tratar de distinguir as pessoas colectivas das singulares.

Para todas as categorias de destinatários, quer se trate de pessoas colectivas ou singulares, a directiva proíbe as mensagens de marketing directo que dissimulem ou escondam a identidade do remetente. Além disso, essas mensagens devem conter um endereço válido para o qual os destinatários possam enviar um pedido para lhes pôr termo[14].

O Grupo de Trabalho do Artigo 29.º para a protecção dos dados, criado para aconselhar a Comissão e que reúne as autoridades responsáveis pela protecção dos dados na UE, está a estudar alguns desses conceitos mais aprofundadamente para contribuir para uma aplicação uniforme das medidas nacionais adoptadas em conformidade com a Directiva 2002/58/CE[15]. O consenso sobre estas questões evitará diferenças de interpretação que poderão prejudicar o funcionamento do mercado interno. Outros aspectos das comunicações não solicitadas foram abordados em documentos anteriores do Grupo de Trabalho[16].

2.2. Disposições de execução

As disposições da directiva geral relativa à protecção dos dados referentes à reparação judicial, à responsabilidade e às sanções são aplicáveis às disposições da directiva relativa à privacidade e às comunicações electrónicas, incluindo as disposições sobre as

---

14 Nº 4 do artigo 13.º da Directiva 2002/58/CE.

15 Nos termos do nº 3 do artigo 15.º da Directiva 2002/58/CE, em conjugação com o artigo 30.º da Directiva 95/46/CE.

16 Ver, por exemplo, Parecer 7/2000 sobre a proposta de directiva do Parlamento Europeu e do Conselho relativa ao tratamento dos dados pessoais e à protecção da privacidade no sector das comunicações electrónicas, de 12 de Julho de 2000; Recomendação 2/2001 sobre certos requisitos mínimos para a recolha de dados pessoais em linha na União Europeia. A recolha de dados foi também examinada no documento de trabalho de 21 de Novembro de 2000 intitulado "Privacidade na Internet - Uma abordagem integrada da UE no domínio da protecção de dados em linha". Estes documentos podem ser consultados no seguinte endereço URL: http://europa.eu.int/comm/internal_market/privacy/workingroup_en.htm.

comunicações não solicitadas[17].

Em síntese, os Estados-Membros devem garantir que a legislação preveja sanções e reparação judicial para os casos de infracção. Deve prever-se o direito individual a reparação judicial para os casos de violação dos direitos previstos na legislação nacional. Embora essa reparação judicial não deva prejudicar quaisquer procedimentos administrativos (eventualmente anteriores), não existe a exigência harmonizada de prever tais procedimentos administrativos. Tem de prever-se o direito individual a indemnização pelos danos sofridos em resultado de qualquer processamento ou acto ilícitos. Devem impor-se sanções em caso de infracção que garantam a plena aplicação da directiva.

Por outras palavras, embora uma directiva, pela sua própria natureza, dê aos Estados-Membros margem de manobra para escolherem as medidas a prever – incluindo reparação judicial e sanções – aquando da transposição da directiva, tais medidas devem obrigatoriamente garantir a "plena aplicação" das disposições sobre comunicações comerciais não solicitadas.

Como geralmente acontece com uma directiva, as disposições de execução são, antes de mais, da competência dos Estados-Membros, não da Comissão. Por exemplo, não compete à Comissão intentar acções ou impor coimas aos infractores dos direitos e obrigações previstos na directiva[18].

2.3. Outras disposições aplicáveis ao "spam"

Uma prática frequentemente relacionada com o "spamming" é a "colheita" de endereços de correio electrónico, ou seja, a recolha automática de dados pessoais em sítios públicos relacionados com a Internet, como a Web, as salas de conversa, etc. Tal prática é ilícita por força da directiva "geral" relativa à protecção dos dados (Directiva 95/46/CE), quer a recolha seja ou não efectuada automaticamente por software[19].

---

17 O artigo 15.º da Directiva 2002/58/CE remete para o Capítulo III da Directiva 95/46/CE relativo aos recursos judiciais, responsabilidade e sanções:
Artigo 22.º – Recursos
Sem prejuízo de quaisquer garantias graciosas, nomeadamente por parte da autoridade de controlo referida no artigo 28º, previamente a um recurso contencioso, os Estados-Membros estabelecerão que qualquer pessoa poderá recorrer judicialmente em caso de violação dos direitos garantidos pelas disposições nacionais aplicáveis ao tratamento em questão.
Artigo 23.º – Responsabilidade
1. Os Estados-Membros estabelecerão que qualquer pessoa que tiver sofrido um prejuízo devido ao tratamento ilícito de dados ou a qualquer outro acto incompatível com as disposições nacionais de execução da presente directiva tem o direito de obter do responsável pelo tratamento a reparação pelo prejuízo sofrido.
2. O responsável pelo tratamento poderá ser parcial ou totalmente exonerado desta responsabilidade se provar que o facto que causou o dano lhe não é imputável.
Artigo 24.º – Sanções
Os Estados-Membros tomarão as medidas adequadas para assegurar a plena aplicação das disposições da presente directiva e determinarão, nomeadamente, as sanções a aplicar em caso de violação das disposições adoptadas nos termos da presente directiva.

18 Ao contrário do que acontece, por exemplo, com agências como a Federal Trade Commission dos Estados Unidos.

19 Ver igualmente o documento de trabalho do Grupo de Trabalho do Artigo 29.º para a protecção dos dados intitulado "Privacidade na Internet - Uma abordagem integrada da UE no domínio da protecção de dados em linha" (Documento nº WP 37, adoptado em 21 de Novembro de 2000).

O "spam" fraudulento e enganoso pode ser particularmente ultrajante. Por força das regras comunitárias em vigor sobre publicidade enganosa e práticas comerciais desleais (por exemplo, a Directiva 84/450/CEE relativa à publicidade enganosa)[20] estas práticas já são ilegais. As legislações nacionais prevêem também, em geral, sanções mais pesadas para os casos mais graves, incluindo sanções penais.

Determinadas categorias de "spam" podem ser ainda mais incomodativas, como o "spam" pornográfico ou o "spam" que contém violência gratuita, sobretudo se as crianças estão expostas a esse género de conteúdos[21]. Embora o conteúdo de algumas dessas mensagens seja lesivo, mas não ilícito em si, a sua distribuição indiscriminada a adultos e crianças é, em geral, ilícita à luz do direito nacional, que prevê, muitas vezes, sanções bastante pesadas. As mensagens "spam" poderão igualmente conter conteúdos ilícitos, como o incitamento ao ódio com base na raça, no sexo, na religião ou na nacionalidade. De qualquer modo, a partir do momento em tais mensagens tenham por finalidade o marketing directo – o que será muitas vezes o caso – estarão abrangidas pela proibição do "spam" ("*ban on spam*") como outras categorias de comunicações de correio electrónico não solicitadas.

Há igualmente que referir a exigência constante da Directiva 2000/31/CE, relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico, no mercado interno (Directiva «Comércio Electrónico»), de que as "comunicações comerciais" sejam claramente identificáveis como tal (ver artigo 6.º, alínea a), da directiva relativa ao comércio electrónico)[22].

Acresce ainda que actividades como a pirataria informática ou o roubo de identidades são muitas vezes perpetradas em apoio das actividades de "spam", com a finalidade de enviar "spam" ou de obter acesso a bases de dados de endereços ou a computadores. Muitas dessas actividades passarão a estar abrangidas pela Decisão-Quadro sobre os ataques a sistemas informáticos, que prevê sanções penais. Esta Decisão-Quadro, baseada numa proposta da Comissão, foi acordada a nível político em Fevereiro de 2003, devendo em

---

20 Directiva 84/450/CEE do Conselho, de 10 de Setembro de 1984, relativa à aproximação das disposições legislativas, regulamentares e administrativas dos Estados-Membros em matéria de publicidade enganosa; JO L 250 de 19/9/1984, p. 17-20. A Comissão apresentou recentemente uma proposta de substituição e actualização da directiva relativa à publicidade enganosa (COM(2003) 356 final).

21 Em 24 de Setembro de 1998, o Conselho adoptou a recomendação relativa ao desenvolvimento da competitividade da indústria europeia de serviços audiovisuais e de informação através da promoção de quadros nacionais conducentes a um nível comparável e eficaz de protecção dos menores e da dignidade humana (98/560/CE). A recomendação foi o primeiro instrumento jurídico a nível comunitário relativo ao conteúdo dos serviços audiovisuais e da informação, abrangendo todas as formas de entrega, desde a radiodifusão até à Internet.

22 Directiva do Parlamento Europeu e do Conselho de 8 de Junho de 2000, JO nº L 178 de 17.7.2000. Como regra geral, as "comunicações comerciais" devem obedecer às regras que lhes são aplicáveis no Estado-Membro de estabelecimento do prestador de serviços. Esta regra, no entanto, não se aplica à permissibilidade de comunicações de correio electrónico não solicitadas (ver artigo 3.º da directiva relativa ao comércio electrónico e o seu anexo). Nos (poucos) casos em que as pessoas singulares não estejam protegidas pela Directiva 2002/58/CE (por exemplo, as pessoas singulares que não são assinantes) contra comunicações comerciais não solicitadas, os Estados-Membros devem igualmente garantir, nos termos da directiva relativa ao comércio electrónico, que os fornecedores de serviços que enviam comunicações comerciais não solicitadas por correio electrónico consultem regularmente e respeitem os registos das "exclusões" ("opt-out"), no qual se podem inscrever as pessoas singulares que não desejam receber esse tipo de comunicações comerciais (ver artigo 7.º da directiva relativa ao comércio electrónico).

breve ser oficialmente aprovada[23]. Em muitos Estados-Membros, o acesso ilegal aos servidores ou computadores pessoais ou a sua utilização abusiva são já considerados delitos, passíveis de acção judicial.

3. APLICAÇÃO E EXECUÇÃO EFECTIVAS PELOS ESTADOS-MEMBROS E AS AUTORIDADES PÚBLICAS

A presente secção abrange as acções propostas a realizar especificamente pelos governos e autoridades públicas, em domínios como a reparação judicial e as sanções, os mecanismos de apresentação de queixas, as queixas transnacionais, a cooperação com os países terceiros e a monitorização.

Antes, porém, de se debruçar sobre a efectiva aplicação da legislação, a Comissão assinala que alguns Estados-Membros ainda não transpuseram a Directiva «Privacidade e Comunicações Electrónicas», incluindo as disposições sobre as comunicações comerciais não solicitadas efectuadas por correio electrónico, directiva essa que faz parte do novo quadro regulamentar mais vasto para as comunicações electrónicas[24]. O Parlamento Europeu manifestou recentemente a sua preocupação quanto a este atraso[25]. Terminado o prazo para a transposição da Directiva «Privacidade e Comunicações Electrónicas», 31 de Outubro de 2003, a Comissão deu início, em Novembro de 2003, a procedimentos de infracção contra alguns Estados-Membros por não-notificação das medidas de transposição[26].

3.1. Introdução

Embora contribua para reduzir o "spam", a legislação só por si não será suficiente. A aplicação efectiva do regime de consentimento prévio ("opt-in") deve ser uma prioridade em todos os Estados-Membros. Para além da obrigatoriedade da existência de pessoal e recursos suficientes, há que dispor de mecanismos de execução adequados, incluindo mecanismos transfronteiras. A cooperação com os países não pertencentes à UE é também fundamental. A monitorização é igualmente importante, quanto mais não seja para determinar as prioridades a nível da execução.

A eficácia dos mecanismos de execução parece depender de uma série de factores:

– a possibilidade de impor o cumprimento da legislação através da aplicação de multas ou outras sanções. Algumas autoridades reguladoras parecem não dispor ainda de poderes de execução (efectivos);

– a natureza dos mecanismos de apresentação de queixas e os meios de reparação ao dispor das pessoas e das empresas;

---

23 Proposta de decisão-quadro do Conselho relativa a ataques contra os sistemas de informação, COM(2002) 173 final, de 19.4.2002.

24 Ver também o Nono Relatório sobre a implementação do pacote regulamentar das telecomunicações, disponível no seguinte endereço URL: http://europa.eu.int/information_society/topics/ecomm/all_about/implementation_enforcement/annualreports/9threport/index_en.htm.

25 A importância da aplicação plena, efectiva e atempada do novo quadro regulamentar das comunicações electrónicas, incluindo esta directiva, foi sublinhada pela Comissão na sua Comunicação "Comunicações electrónicas: A Via para a Economia do Conhecimento (COM(2003) 65 de 11 de Fevereiro de 2003).

26 Foram enviadas cartas de notificação para cumprir em 25 de Novembro de 2003 (ver IP/03/1663).

– a necessidade de clareza e a coordenação entre as autoridades nacionais, tendo em conta as suas funções muitas vezes sobrepostas nesta matéria;

– o nível de conhecimento que os utilizadores têm dos seus direitos e do modo de os fazer valer. É preciso informar os utilizadores sobre o local/entidade a que devem apresentar queixa, o que será ou não investigado, os tipos de medidas de execução que podem ser tomadas e quais as informações que precisam de fornecer para as autoridades iniciarem uma investigação;

– a coordenação e a cooperação entre Estados-Membros e entre estes e os países terceiros sobre a legislação nacional aplicável a determinados casos;

– os meios disponíveis para localizar os autores de "spam" activos na UE ou fora dela e que escondem a sua identidade, nomeadamente utilizando a identidade, o endereço ou os servidores de outros.

Na secção 2.2 descreveram-se as disposições de execução aplicáveis às disposições relativas a comunicações não solicitadas. O modo como os procedimentos relativos às comunicações não solicitadas efectuadas por correio electrónico são organizados e tratados tem sido até agora muito diversificado[27]. Embora uma directiva comunitária seja um instrumento que confere aos Estados-Membros uma certa margem de manobra na aplicação das suas disposições, é necessário que o controlo do seu cumprimento seja eficaz, independentemente do método utilizado.

Diversidade nos Estados-Membros

A autoridade responsável pela execução das disposições relativas às comunicações comerciais não solicitadas não é a mesma em todos os Estados-Membros. Na maioria dos casos, é a autoridade responsável pela protecção dos dados a principal responsável. Nalguns países, porém, é a autoridade reguladora nacional (ARN) das comunicações electrónicas que desempenha essa função. Noutros países ainda, o controlo da aplicação das regras compete principalmente às autoridades responsáveis pela protecção dos consumidores (incluindo o provedor dos consumidores).É frequente haver várias autoridades envolvidas na execução das disposições relativas às comunicações não solicitadas. Além disso, o « spam » implica, em inúmeros casos, práticas enganosas ou fraudulentas. (Uma minoria de Estados-Membros não dispõe de autoridade para a protecção dos consumidores e o controlo da aplicação das regras está a cargo das associações de consumidores ou dos próprios consumidores.) As actividades de « spamming » estão frequentemente associadas a infracções às regras sobre a protecção dos dados, como a recolha de endereços electrónicos, quando não a actividades de cibercriminalidade, como a intrusão ilícita nos PC ou nos servidores. Não são necessariamente as mesmas autoridades que velam pelo cumprimento das disposições correspondentes, muito menos a uma escala transfronteiras.

Excepto num pequeno número de Estados-Membros , uma queixa não dá necessariamente origem a uma investigação. Recorre-se por vezes a contactos «pré-infracção», que incluem conselhos e orientações às empresas, com algum êxito. Por vezes, essa fase anterior à queixa é deixada a cargo do consumidor, que deve contactar a sociedade em causa antes de introduzir uma queixa. Alguns países, como o Reino Unido, recorrem à auto-regulação para organizar essa primeira fase de acção. Em alguns Estados-Membros já existem mecanismos de depósito de queixas no âmbito da auto-regulação. Também é frequente as autoridades agirem por sua própria iniciativa. O facto de uma autoridade administrativa estar especialmente encarregada destas questões não exclui, em princípio, o recurso directo ao sistema judicial.

Nem todas as autoridades responsáveis pela protecção dos dados têm poder para agir contra pessoas colectivas. Também nem todas (até agora) têm a possibilidade de impor sanções. Para isso, têm de

[27] Note-se que as queixas muitas vezes também dizem respeito a questões conexas, como o direito de acesso a dados pessoais e o direito de objecção ao processamento de dados.

introduzir um processo junto das autoridades judiciais. Em França, a experiência com a caixa de correio de « spam » («boîte à spam») levou a autoridade responsável pela protecção dos dados a seleccionar alguns casos e a remetê-los para as autoridades judiciais, sem grande sucesso.

Na Bélgica, uma experiência semelhante levou a uma troca de pontos de vista com os remetentes suspeitos e, nos casos transfronteiras, à sua remissão para as autoridades correspondentes de outros Estados da UE ou para a FTC dos Estados Unidos.

Uma abordagem equilibrada que inclua a legislação, o controlo da aplicação das regras e a auto-regulação é muitas vezes descrita como o meio mais eficaz de executar o regime de «opt-in». Convida-se os Estados-Membros a avaliarem a eficácia dos seus mecanismos de execução, nomeadamente à luz das diversas acções a seguir propostas (ver Secções 3.2 a 3.6).

Convida-se também os Estados-Membros a desenvolverem estratégias nacionais destinadas a garantir a cooperação entre as autoridades responsáveis pela protecção dos dados, as autoridades encarregadas da protecção dos consumidores e as autoridades reguladoras nacionais (ARN) e a evitarem as sobreposições de competências e as duplicações de tarefas entre autoridades.

Para facilitar e coordenar as trocas de informações e de melhores práticas sobre a execução eficaz da legislação (por exemplo, no que respeita a queixas, meios de reparação, sanções, cooperação internacional) os serviços da Comissão criaram, com o apoio dos Estados-Membros e das autoridades responsáveis pela protecção dos dados, um **grupo informal em linha para as comunicações comerciais não solicitadas**. O grupo facilitará e coordenará igualmente os trabalhos sobre as restantes acções identificadas na presente comunicação, como a sensibilização e as soluções técnicas.

Os documentos redigidos na sequência dos debates no seio do grupo serão, em geral, transmitidos ao Comité das Comunicações (COCOM) criado ao abrigo do quadro regulamentar para as redes e serviços de comunicações electrónicas e/ou ao Grupo de Trabalho do Artigo 29.º para a protecção dos dados, com vista a uma acção apropriada. O grupo pode, nomeadamente, elaborar critérios de aferição de desempenhos para as várias medidas a propor.

Este grupo em linha inclui as administrações nacionais competentes e as autoridades para a protecção dos dados, para além dos serviços da Comissão. O grupo em linha determinará o modo de garantir a participação de outras partes interessadas.

3.2. Reparação judicial e sanções eficazes

3.2.1. Discussão

Neste momento, a reparação judicial inclui geralmente multas ou mandados de injunção para fazer cessar o processamento ilícito de dados, implicando, por vezes, o bloqueio dos sítios Web envolvidos. Nalguns Estados-Membros, os "mandados de injunção para cessar" precedem ou acompanham as multas em caso de não-cumprimento. No entanto, nem todas as autoridades são competentes para tratar toda a gama de infracções relacionadas com o "spam", nem dispõem das mesmas ferramentas. Muitas vezes, os casos também são remetidos para as autoridades judiciais. Nem todos os Estados-Membros prevêem sanções judiciais para as infracções.

Nem todos os Estados-Membros prevêem reparação judicial e multas/sanções no seu direito administrativo ou penal. As sanções penais variam de Estado-Membro para Estado-Membro e incluem, por vezes, penas de prisão.

Além disso, há, em geral, a possibilidade de pedir uma reparação de danos (indemnização) nos termos do direito civil.

Embora se faça frequentemente a distinção entre crimes "menores" e crimes "graves" (por exemplo, mensagens multi-destinatários (*bulk e-mails*), publicidade e práticas comerciais enganosas ou fraudulentas), as próprias sanções variam acentuadamente de um Estado-Membro para outro.

Em muitos casos, as actividades de "spam" podem igualmente dar origem a reparações judiciais previstas na legislação geral sobre protecção de dados (por exemplo, não-cumprimento da obrigação de notificação, desrespeito do direito de acesso, não-cumprimento da obrigação de designar um representante num Estado-Membro da UE, etc.) ou em legislação específica (por exemplo, sobre publicidade enganosa, técnicas de marketing fraudulentas, etc.). Foram utilizados, nomeadamente antes da introdução do regime de consentimento prévio ("opt-in"), vários fundamentos jurídicos para combater certas formas de "spam" (por exemplo, campanhas de publicidade electrónica multi-destinatários, utilização ilegítima de dados pessoais, perturbações na rede, utilização abusiva de contratos de correio electrónico (*e-mail accounts*), fraude e interpretação errónea de contratos).

Em termos gerais, a reparação judicial não é considerada um mecanismo de execução suficiente. Em geral, as autoridades para a protecção dos dados (APD), as autoridades para a protecção dos consumidores (APC) e/ou as ARN podem aplicar multas administrativas, mas os montantes variam. Os Estados-Membros que não prevêem essa possibilidade estão, em geral, a ponderar a sua introdução. Comparadas com a reparação judicial, as sanções administrativas parecem ser particularmente adequadas a um sector de tal modo dinâmico. As APD, APC e ARN recorrem, muitas vezes, elas próprias, a ferramentas complementares de execução. Os procedimentos administrativos podem revelar-se pouco dispendiosos e céleres (segundo dados da APD italiana, concluídos em cinquenta dias ou menos).

3.2.2. Acções propostas

Como requisito prévio, a Comissão insta os Estados-Membros que ainda não transpuseram a directiva e, em particular, as disposições sobre comunicações não solicitadas, a concluírem essa tarefa sem demora. Os serviços da Comissão prontificam-se a dar assistência aos Estados-Membros, se necessário.

Pede-se aos Estados-Membros que avaliem a eficácia do seu sistema de reparação judicial e sanções em caso de infracções e que criem condições adequadas para as vítimas pedirem a reparação dos danos.

Os Estados-Membros e as autoridades competentes que não prevêem uma reparação administrativa devem considerar a hipótese de a preverem para combater o "spam", como ferramenta para garantir um processo rápido, pouco dispendioso e eficaz de aplicar o regime de "opt-in".

A Comissão verificará se as medidas nacionais de transposição prevêem sanções efectivas em caso de incumprimento das exigências nesta matéria por parte dos intervenientes no mercado, incluindo, se necessário, sanções financeiras e penais.

Neste contexto, a Comissão investigará igualmente em que medida as autoridades competentes dispõem dos poderes de investigação e execução necessários.

3.3. Mecanismos de apresentação de queixa

3.3.1. Discussão

A execução efectiva das regras implica a existência de mecanismos de apresentação de queixas. Algumas APD criaram caixas de correio electrónico para onde os utilizadores podem reenviar o correio electrónico comercial não solicitado e comprometeram-se a tomar medidas em determinados casos.

Alguns Estados-Membros parecem preferir os procedimentos administrativos normais e/ou os contactos com os FSI (fornecedores de serviços Internet), ou equipas de resposta a emergências informáticas (*Computer Emergency Response Teams (CERTs)*) no caso de perturbações da rede. Outros Estados-Membros favorecem os procedimentos mais tradicionais (pedidos de indemnização ao abrigo do direito civil/processos administrativos). A co-regulação ou a auto-regulação são, por vezes, defendidas como alternativas mais eficazes às medidas de execução directas.

Melhores práticas

A França e a Bélgica utilizaram, em finais de 2002, caixas de correio electrónico específicas para receberem queixas concretas relativas a "spam" e os resultados são bastante interessantes. Os relatórios dessas iniciativas encontram-se ao dispor do público[28]. Prevê-se que a França estabeleça a título permanente uma caixa de correio electrónico ao abrigo das novas regras que transpõem a Directiva «Privacidade e Comunicações Electrónicas». A "Federal Trade Commission" (FTC) dos EUA gere uma caixa de correio semelhante e utiliza as mensagens que nela dão entrada para intentar acções judiciais com fundamento em práticas comerciais desleais e enganosas[29].

Uma das vantagens das caixas de correio electrónico é o facto de, aparentemente, encorajarem os consumidores a comunicar as infracções, tornando, por conseguinte, mais efectiva a execução da legislação adoptada. Além disso, permitem dispor de estatísticas essenciais sobre a dimensão e a natureza dos problemas registados num dado país ou região, fornecendo uma perspectiva clara, o que, por sua vez, constitui uma ferramenta valiosa para as autoridades estabelecerem as prioridades em matéria de execução ou mesmo para adaptarem essas prioridades. Por outro lado, podem conceber-se acções preventivas com base nos conhecimentos adquiridos. A título ilustrativo, a CNIL, ou seja, a APD francesa, utilizou as informações reunidas durante o funcionamento da sua

---

28 O relatório de 24 de Outubro de 2002 adoptado pela 'Commission National Informatique et Libertés' (CNIL), a APD francesa, encontra-se disponível no seguinte endereço URL : http://www.cnil.fr/frame.htm?http://www.cnil.fr/thematic/internet/spam/spam_sommaire.htm
O relatório de Julho de 2003 elaborado pela 'Commission de Protection de la Vie Privée', a autoridade belga responsável pela protecção dos dados, pode ser consultado no seguinte endereço URL: http://www.privacy.fgov.be/publications/spam_4-7-03_fr.pdf.

29 Ver, por exemplo. http://www.ftc.gov/bcp/conline/pubs/online/inbox.pdf As mensagens não desejadas ou enganosas podem ser enviadas para o seguinte endereço URL: uce@ftc.gov.

'boîte à spams' para conceber pacotes de informações preventivas destinados aos utilizadores e aos responsáveis comerciais.

A utilidade de uma caixa de correio electrónico para monitorizar e medir a escala e o âmbito do "spam" depende, como é óbvio, da capacidade para investigar cabal e rapidamente as queixas apresentadas.

Embora exista, em geral, um interesse pela experiência de outros Estados-Membros com as caixas de correio electrónico, apenas alguns Estados-Membros parecem ter planos ou ponderar a hipótese de utilizar uma caixa de correio específica. As razões indicadas são, em geral: a existência da possibilidade de apresentar queixa por correio electrónico, normalmente através do sítio Web da autoridade responsável; a necessidade de pessoal especializado e de equipamentos suplementares ou ainda a necessidade de alterar os procedimentos legais existentes.

3.3.2. Acções propostas

Os Estados-Membros e as autoridades competentes deverão avaliar a eficácia do seu sistema jurídico para lidar com as queixas dos utilizadores e prever adaptações, se necessário.

Os Estados-Membros e as autoridades competentes são convidados a criar caixas de correio electrónico específicas, apoiadas por campanhas de informação.

Essas caixas de correio electrónico específicas terão de ser concebidas de modo a permitir uma pesquisa e uma análise simples, para que se possa compreender melhor o problema e estabelecer prioridades em matéria de execução das regras.

Os serviços da Comissão facilitarão a partilha de informações sobre as experiências com as caixas de correio electrónico.

3.4. Queixas transfronteiras e cooperação em matéria de execução dentro da UE

3.4.1. Discussão

O tratamento eficaz das queixas transfronteiras é uma forma de proteger devidamente os consumidores neste domínio. Será muito importante garantir que os mecanismos nacionais de apresentação de queixas, independentemente das suas modalidades, estejam ligados de modo a garantir que as queixas dos utilizadores de um Estado-Membro relativas a mensagens originadas noutro Estado-Membro também recebam um tratamento eficaz (ver secção 3.5 mais adiante, relativa à cooperação com os países terceiros).

Presentemente, nem todos os Estados-Membros dispõem de um procedimento formal para lidar com as queixas transfronteiras. As soluções actuais incluem contactos com a autoridade competente do outro Estado-Membro e a eventual transferência da queixa para a autoridade competente do país de origem da ou das mensagens.

A nível europeu, as APD (incluindo as dos países do EEE e dos países candidatos) estão a procurar trocar informações sobre as queixas transfronteiras, por intermédio do

'*Complaints handling workshop*', um grupo criado no âmbito da Conferência Europeia de comissários responsáveis pela protecção dos dados.

É possível recorrer a esse grupo para as queixas transfronteiras relativas ao "spam", nomeadamente para a tarefa de determinar qual a legislação aplicável a determinados casos. Ao mesmo tempo, convém saber que nem todas as APD têm poderes de execução para as disposições relativas às comunicações não solicitadas.

No domínio da protecção dos consumidores, a Comissão propôs recentemente um regulamento relativo à cooperação no domínio da defesa do consumidor, que estabelece uma rede de autoridades públicas responsáveis pela protecção do consumidor para lidar com os problemas transfronteiras[30]. O regulamento instaura procedimentos de assistência mútua e prevê uma cooperação operacional profunda entre as autoridades nacionais. O regime proposto abrange o "spam" fraudulento ou enganoso ou que viola outras regras de protecção dos consumidores, mas não todo o "spam" proibido pela directiva relativa à privacidade e às comunicações electrónicas. O regulamento está neste momento a ser discutido no Conselho e no Parlamento.

3.4.2. Acções propostas

Os Estados-Membros e as autoridades competentes são convidados a avaliar a eficácia dos seus procedimentos actuais em matéria de tratamento das queixas transfronteiras (por exemplo, acordos de assistência mútua).

Encoraja-se a coordenação entre as autoridades nacionais competentes. Tal inclui a coordenação e as trocas de informações entre as autoridades responsáveis pela execução das novas disposições, e entre essas mesmas autoridades e outras responsáveis por formas específicas de "spam" (como o "spam" fraudulento ou os "scams", o "spam" pornográfico, as mensagens relativas a produtos para a saúde ilegalmente distribuídos).

No que respeita ao "spam" fraudulento e enganoso, pede-se ao Conselho e ao Parlamento que dêem o seu acordo à proposta de regulamento relativo à cooperação em matéria de protecção dos consumidores tão rapidamente quanto possível, de modo a garantir que as autoridades responsáveis pela protecção dos consumidores da UE disponham de todos os instrumentos necessários para lidar com o "spam" fraudulento e enganoso. Pede-se também ao Conselho e ao Parlamento que considerem a possibilidade de alargar o âmbito deste regulamento à Directiva «Privacidade e Comunicações Electrónicas».

Pede-se aos Estados-Membros que estudem os meios de eliminar os obstáculos existentes à troca de informações e à cooperação e a possibilidade de pedirem a outros Estados-Membros que tomem medidas. Na prática, poderia ser útil dispor de um mecanismo de ligação (ver iniciativa das APD atrás mencionada) através do qual as autoridades reguladoras nacionais pudessem cooperar com vista à execução das regras a nível transfronteiras. O estabelecimento de uma rede de apoio à cooperação poderá tirar partido de programas actuais da Comissão, como o IDA[31].

A Comissão tenciona facilitar e promover esses esforços de coordenação entre as autoridades nacionais competentes, nomeadamente através do recentemente criado grupo

---

30 COM(2003) 443 final.

31 Para informações sobre o programa IDA, consultar o endereço URL: http://europa.eu.int/comm/enterprise/ida/index.htm.

informal em linha para as comunicações comerciais não solicitadas. Os serviços da Comissão começaram a estudar, juntamente com os Estados-Membros e as autoridades nacionais envolvidas na execução das regras, as medidas concretas necessárias para melhorar o tratamento das queixas transfronteiras. As discussões com as autoridades nacionais continuarão ao longo de 2004.

3.5. Cooperação com os países terceiros

3.5.1. Discussão

As novas regras aplicam-se ao tratamento de dados pessoais em ligação com a oferta de serviços de comunicações electrónicas publicamente disponíveis nas redes de comunicações públicas da União Europeia (e do EEE). Consequentemente, o artigo 13.º da Directiva 2002/58/CE, que estabelece a regra do consentimento prévio, é aplicável a todas as comunicações comerciais não solicitadas recebidas em - ou enviadas de - redes da UE (e do EEE). Tal implica que tais mensagens originadas em países terceiros devem igualmente respeitar as regras da UE, à semelhança das mensagens originadas na UE e enviadas para destinatários de países terceiros.

A aplicação efectiva da regra no que respeita às mensagens originadas em países terceiros será sem dúvida mais complicada do que no que respeita às mensagens provenientes da UE. Apesar disso, tal aplicação é importante, atendendo a que muito do "spam" provém de fora da UE.

Embora seja necessária uma combinação de vários instrumentos, incluindo a prevenção, técnicas de filtragem, auto-regulação, contratos e cooperação internacional, a presente secção centra-se sobretudo na cooperação internacional. O primeiro objectivo da cooperação internacional é promover a adopção de legislação eficaz nos países terceiros. O segundo objectivo é cooperar com os países terceiros para garantir a aplicação efectiva das regras aplicáveis.

Não é grande a experiência em matéria de aplicação das regras de "opt-in" ou "opt-out" para as comunicações originadas fora da UE. Para além do facto de o "spam" ser um fenómeno relativamente novo, entre os obstáculos muitas vezes apontados inclui-se a dificuldade de identificar os remetentes desse "spam" ou o esforço que tal exige, a inexistência de mecanismos de cooperação internacional (apropriados) e a falta de competência de algumas autoridades em questões internacionais.

No que respeita ao "spam" fraudulento e enganoso, a proposta de regulamento da Comissão relativo à cooperação em matéria de protecção do consumidor prevê também a cooperação com os países terceiros em matéria de execução das regras. A Organização para a Cooperação e o Desenvolvimento Económico (OCDE) adoptou em 2003 uma recomendação destinada a proteger os consumidores contra as práticas comerciais fraudulentas e enganosas a nível transfronteiras[32].

[32] Orientações da OCDE para a protecção dos consumidores contra as práticas comerciais fraudulentas e enganosas transfronteiras, OCDE, 2003.

3.5.2. Acções propostas

A nível multilateral, alguns Estados-Membros já participam activamente em instâncias como a OCDE, onde já se começou a trabalhar no "spam". Encoraja-se a participação nesse trabalho, nomeadamente no que respeita à elaboração de soluções a nível internacional.

A Comissão acolherá, em Fevereiro de 2004, um seminário da OCDE sobre "spam", que se espera contribua para uma melhor compreensão do problema e para a elaboração de soluções a nível internacional. As acções concretas a desenvolver posteriormente a nível da OCDE basear-se-ão nos resultados do seminário. Os serviços da Comissão estão a discutir essas acções de seguimento com os Estados-Membros, incluindo os trabalhos da OCDE para promover uma legislação internacional eficaz, a sensibilização, as soluções técnicas, a auto-regulação e a cooperação internacional em matéria de execução das regras.

A nível das Nações Unidas, o projecto de declaração da Cimeira Mundial sobre a Sociedade da Informação (Genebra, 10-12 de Dezembro de 2003) e o plano de acção associado sublinham que o problema do "spam" deve ser tratado nas instâncias adequadas a nível nacional e internacional. A Comissão estudará a melhor maneira de dar seguimento aos resultados da Cimeira Mundial de 2003 na UE, tendo em conta a Cimeira de Túnis, a realizar em 2005.

Os Estados-Membros e as autoridades competentes são igualmente convidados a reforçar ou a estabelecer a cooperação bilateral com os países terceiros. Tal inclui não só a promoção de legislação eficaz, mas também a cooperação em matéria de aplicação das regras, incluindo, na medida do necessário, a cooperação policial e judicial.

Encoraja-se igualmente a cooperação entre as autoridades e o sector privado, nomeadamente entre os FSI e os FSCE (fornecedores de serviços de correio electrónico), para localizar os autores de "spam", sob reserva de protecção jurídica adequada.

Os serviços da Comissão continuarão a participar activamente nos trabalhos desenvolvidos nas instâncias internacionais, incluindo a OCDE e o seminário que a Comissão acolherá em Bruxelas, em Fevereiro de 2004. A Comissão continuará igualmente a efectuar reuniões e discussões bilaterais com os países terceiros, *inter alia* para os incentivar a tomarem medidas eficazes contra o "spam" e, em particular, as suas formas mais ofensivas, e a promoverem a cooperação em matéria de aplicação das regras.

Os serviços da Comissão começaram a estudar, juntamente com os Estados-Membros e as autoridades com poderes de execução, o melhor modo de garantir a cooperação internacional, designadamente garantir o tratamento das queixas relativas a "spam" originado em países terceiros. Este trabalho com as autoridades nacionais prosseguirá durante 2004.

3.6. Monitorização

3.6.1. Discussão

Para avaliar o modo como o sistema "opt-in" funciona na prática e para encontrar soluções adequadas para os problemas específicos, os Estados-Membros precisarão de

dispor de informações objectivas e actualizadas sobre as tendências a nível do "spam", as queixas dos utilizadores e as dificuldades encontradas pelos fornecedores de serviços.

As fontes e o tipo de informações necessárias poderão incluir: as tendências a nível da natureza do "spam", da origem e do volume das mensagens comerciais não solicitadas enviadas por correio electrónico detectadas pelos fornecedores de software de filtragem e fornecedores de serviços e pelas autoridades (regulamentadoras) nacionais e, se for o caso, estatísticas resultantes da utilização de uma caixa de correio para queixas.

A OCDE começou, em 2003, os trabalhos atinentes à quantificação das mensagens electrónicas não solicitadas a nível internacional, tencionando prosseguir esses trabalhos em 2004.

O artigo 18.º da directiva relativa à privacidade e às comunicações electrónicas prevê a apresentação de um relatório em 2006 sobre a aplicação da directiva e o seu impacto nos operadores económicos e nos consumidores, com uma ênfase específica nas comunicações não solicitadas. Para a elaboração desse relatório, a Comissão precisará de obter informações dos Estados-Membros, incluindo estatísticas nesta matéria.

3.6.2. Acções propostas

Os Estados-Membros devem garantir que dispõem das informações e das estatísticas necessárias para centrarem os seus esforços na execução das regras, em cooperação com o sector, se necessário, e tendo em conta os trabalhos em curso na OCDE sobre a medição da quantidade de mensagens electrónicas não solicitadas.

A Comissão utilizará o recentemente criado grupo informal em linha para as comunicações comerciais não solicitadas para facilitar e coordenar as trocas de informações e de melhores práticas sobre as tendências e as estatísticas relativas ao "spam".

4. MEDIDAS TÉCNICAS E DE AUTO-REGULAÇÃO PARA O SECTOR

A presente secção sobre as questões técnicas e da auto-regulação aborda as acções propostas especificamente para os intervenientes no mercado, em domínios como as disposições contratuais, os códigos de conduta, as práticas de marketing aceitáveis, os rótulos e os mecanismos alternativos de resolução de litígios. São ainda abordadas algumas soluções técnicas, como a filtragem e a segurança dos servidores.

4.1. Aplicação eficaz do regime de "opt-in"

4.1.1. Discussão

O combate ao "spam" é matéria da responsabilidade de todas as partes interessadas. A indústria pode ter um papel específico a desempenhar, uma vez que pode transformar o regime de "opt-in" numa prática comercial corrente. A prática corrente inclui não só o estabelecimento de cláusulas e condições para os utilizadores, mas também as relações com os parceiros comerciais.

Em muitos casos, é necessária uma melhor coordenação por intermédio das associações do sector e o envolvimento de organismos de auto-regulação específicos do sector e das

associações de consumidores/utilizadores, incluindo o envolvimento das autoridades responsáveis pela protecção dos dados ou outras autoridades nacionais competentes.

Melhores práticas

A título ilustrativo, nos Países Baixos, desde 2002, a "Electronic Commerce Platform" acolheu uma plataforma chamada 'Basic Principles for Commercial e-Mail', que reúne diferentes ramos do sector (marketing directo e FSI) e a associação de defesa do consumidor neerlandesa. A intenção é desenvolver a implementação prática do princípio de "opt-in". Esta implementação prática será testada com a autoridade responsável pela protecção dos dados[33].

Os contratos podem ajudar a combater o "spam", sob reserva da protecção jurídica dos direitos individuais. Muitos fornecedores de serviços Internet (FSI) e fornecedores de serviços de correio electrónico (FSCE) já incluem, nos contratos com os seus clientes, a obrigação de proibirem a utilização dos seus serviços para o envio de "spam". Esses FSI e FSCE já proíbem o envio de correio electrónico não solicitado, ou correio electrónico multi-destinatários, a partir das suas contas de correio electrónico (*e-mail accounts)* [34].

Os conceitos utilizados nos contratos anteriores entre os FSI e os seus clientes são provavelmente diferentes dos utilizados na nova directiva e na subsequente legislação nacional de transposição.

Em termos de serviço ao cliente, é também necessária uma política mais dinâmica em matéria de filtragem, que passa pelo fornecimento de informações sobre os filtros anti-"spam" e pela oferta aos assinantes, como opção, de serviços ou meios de filtragem.

O mesmo se aplica aos casos em que os FSI ou os operadores móveis estabelecem contratos com terceiros e, em particular, com empresas de venda directa, que não se limitam às relações directas com as empresas que oferecem serviços "de valor acrescentado", bem como aos casos em que os operadores estabelecem acordos de interligação com um dado prestador de serviços, como no caso dos serviços móveis.

O regime de "opt-in" também tem implicações em várias actividades de marketing directo, nomeadamente:

- os métodos de recolha de endereços de correio electrónico e outros elementos de contacto electrónico de acordo com o novo regime (como referido acima, a "colheita" de endereços de correio electrónico é incompatível com a legislação comunitária);

- a adaptação das listas existentes;

-as proibições no que se refere à utilização de dados sem consentimento e à venda de listas não conformes com a regulamentação.

---

33 Ver http://www.ecp.nl/projecten.php#32.

34 Tais cláusulas baseiam-se, por vezes, na necessidade de tomar todas as medidas possíveis para evitar a utilização inapropriada dos seus serviços. Outras remetem para códigos de conduta existentes relativos às mensagens electrónicas multi-destinatários (*bulk*) ou mesmo para princípios de auto-regulação (por exemplo, 'netiquette').

4.1.2. Acções propostas

Deve incentivar-se o envolvimento do sector e a auto-regulação, ou, melhor, a co-regulação, designadamente em domínios em que a legislação e a execução apenas por parte das autoridades públicas podem não ser suficientes. Todas as partes interessadas têm um papel a desempenhar neste domínio, incluindo as associações de consumidores e/ou as associações de utilizadores.

Práticas contratuais dos fornecedores de serviços em relação aos assinantes e parceiros comerciais

Em primeiro lugar, o sector terá, em particular, de avaliar em que medida os seus contratos actuais são compatíveis com as novas regras e, se assim não for, de os adaptar em conformidade.

Tal implica a adaptação das cláusulas e condições dos contratos de assinante, o que se aplica não só aos FSI e FSCE, mas também aos fornecedores de serviços móveis. Como medida complementar, poderá prever-se o fornecimento de informações sobre filtros e software de filtragem, como serviço opcional ao cliente (relativamente à filtragem, ver igualmente a secção 4.3, mais adiante). As cláusulas dos contratos com parceiros comerciais (por exemplo, interligação móvel, serviços de valor acrescentado) deverão igualmente reflectir práticas conformes com o regime de "opt-in" e prever sanções adequadas em caso de violação.

Práticas das empresas de venda directa

Em segundo lugar, pode ser necessário adaptar as práticas das empresas de venda directa ao regime de "opt-in". Estas empresas poderão, nomeadamente, estabelecer um acordo sobre métodos específicos e conformes com a regulamentação para recolherem dados pessoais (por exemplo, sistemas de "opt-in" "duplos" ou "confirmados").

Códigos de conduta

Em terceiro lugar, as associações do sector já anunciaram várias iniciativas, como a adaptação ou a adopção de códigos de conduta e a divulgação das boas práticas de marketing[35]. A Comissão apoiará a elaboração de códigos de conduta em linha à escala europeia no domínio do marketing directo. Os códigos de conduta, outras iniciativas de auto-regulação e os contratos devem ser conformes às regras de "opt-in". Nesta matéria, poderá ser útil o envolvimento da autoridade reguladora competente. Recorde-se que, nesse contexto, o Grupo de Trabalho do Artigo 29.º para a protecção dos dados pode aprovar códigos de conduta (ver artigo 30.º da Directiva "geral" «Protecção dos Dados» (Directiva 95/46/CE).

Como muitas vezes acontece, a aplicação efectiva de soluções assentes na auto-regulação dependerá da estrutura em vigor para controlar o respeito das regras acordadas, incluindo sanções eficazes.

[35] A Federação Europeia de Marketing Directo (FEDMA) anunciou um código de conduta em linha específico para as empresas de marketing directo.

Rótulos

Em quarto lugar, para promover uma maior consciencialização dos utilizadores, poderão utilizar-se ferramentas como os rótulos (também conhecidos por 'trustmarks' (rótulos de confiança) ou 'webseals' (rótulos de confidencialidade)), nomeadamente nos casos em que são terceiros de confiança a controlar e certificar o cumprimento dos códigos de conduta pelos intervenientes no mercado.

A existência de rótulos visíveis pode ajudar os utilizadores a identificar os FSI, os FSCE e outros intervenientes do sector que se conformam às regras comunitárias e/ou a códigos de conduta reconhecidos que aplicam regras comunitárias. Também podem contribuir para tornar os sistemas de filtragem mais eficazes.

Pode igualmente prever-se a rotulagem das bases de dados de utilizadores aderentes ao sistema de "opt-in" e a rotulagem das mensagens de correio electrónico conformes com esse mesmo sistema (por exemplo, utilizar o rótulo 'ADV' (ou PUB) no campo "assunto" de uma mensagem de correio electrónico para indicar que contém publicidade).

Os rótulos podem também permitir aos destinatários identificar claramente essas comunicações comerciais, nos termos da directiva relativa ao comércio electrónico (ver alínea a) do artigo 6.º da Directiva 2000/31/CE; ver também Secção 2 do presente documento).

4.2. Mecanismos alternativos de resolução de litígios (MARL)

4.2.1. Discussão

Para violações da privacidade, como o envio de correio electrónico não solicitado, a instauração de um mecanismo extrajudicial de resolução de litígios poderá permitir uma maior observância das novas regras. Foram lançadas várias iniciativas a nível nacional e comunitário tendentes a criar mecanismos alternativos de resolução de litígios (MARL) em matéria de transacções e comunicações em linha. A Comissão adoptou recomendações sobre os MARL em 1998 e 2001, estabelecendo assim os princípios a aplicar a tais sistemas. Estão em curso várias iniciativas no campo dos sistemas MARL centrados na protecção dos consumidores (por exemplo, EEJ-NET)[36]. O artigo 17.º da directiva relativa ao comércio electrónico também encoraja o desenvolvimento de tais mecanismos.

Nalguns países, existem mecanismos extrajudiciais de resolução de litígios, por vezes criados por legislação, embora variem em muitos aspectos, como a origem (mecanismos sectoriais – marketing directo, marketing por correio electrónico), jurisdição, poderes e sanções (por exemplo, indemnizações), envolvimento de autoridades específicas (por exemplo, APD, organismos responsáveis pelas normas de publicidade), etc.

Para que tais mecanismos sejam suficientemente eficazes, devem estar reunidas certas condições relativas, nomeadamente, à sua organização e promoção e ao modo como garantir o cumprimento das suas decisões. A instituição desses mecanismos exige também a cooperação entre as autoridades e o sector.

---

[36] Mais informações em.: http://europa.eu.int/comm/consumers/redress/out_of_court/index_en.htm.

4.2.2. Acções propostas

Encoraja-se a criação e a utilização de mecanismos eficazes de resposta às queixas e de mecanismos alternativos de resolução de litígios (MARL) baseados na auto-regulação, sempre que possível aproveitando as iniciativas existentes (por exemplo, EEJ-NET). Esses mecanismos podem revelar-se particularmente úteis nos casos em que a cooperação internacional é mais difícil de conseguir.

4.3. Questões técnicas

4.3.1. Discussão

Utilizam-se diferentes soluções para combater o "spam" por meios técnicos. A comunidade Internet (por exemplo, RIPE, IETF) também começa a considerar seriamente o problema do "spam"[37]. O presente documento não foca as iniciativas a mais longo prazo, como as novas normas técnicas para o correio electrónico. Os FSI e os FSCE bloqueiam muitas vezes o correio proveniente de servidores que são utilizados para enviar "spam" (lista negra) até que a fonte do "spam" seja identificada e impedida de utilizar o servidor. Além disso, o software de filtragem pode ser utilizado pelos utilizadores individuais no seu próprio equipamento terminal ou pelos fornecedores de serviços de comunicações electrónicas nos seus servidores.

No entanto, nem todas as práticas e técnicas de filtragem oferecem o mesmo nível de controlo pelo utilizador, nem as mesmas garantias de protecção dos dados e da privacidade, como o respeito pela confidencialidade das comunicações. Além disso, podem também não estar ainda adaptadas ao novo regime de "opt-in" aplicável nos países da UE às comunicações comerciais (consentimento prévio, mensagens que visem a comercialização, correio multi-destinatários em grande volume e em pequeno volume). Por outro lado, uma maior diferenciação entre marketing legítimo (conforme com o regime de "opt-in", por exemplo) e comunicações comerciais não solicitadas pode permitir o desenvolvimento de software de filtragem mais eficaz.

Embora as novas disposições jurídicas relativas ao correio electrónico comercial não solicitado aumentem as salvaguardas para o utilizador e garantam maior protecção para os fornecedores de serviços, que poderão tomar medidas, quando solicitados, contra os autores do "spam", a filtragem pode ocasionalmente bloquear o correio electrónico legítimo ('falso positivo') ou permitir a passagem de "spam" ('falso negativo'). Nalguns casos, corre-se o risco de tanto os remetentes como os destinatários lesados intentarem uma acção judicial contra um FSI/FSCE. Alguns FSI/FSCE, por conseguinte, oferecem a filtragem aos seus utilizadores como serviço opcional e exigem autorização para o activar.

O recurso a técnicas de filtragem para combater o "spam" suscita igualmente outras questões, como a do contraponto entre filtragem e liberdade de expressão e entre filtragem e obrigação dos FSI/FSCE de transmitirem as mensagens de correio electrónico

---

[37] Por exemplo, o grupo de trabalho anti-"spam" da RIPE (Redes IP Europeias) está activo desde 1998 (o documento "Good Practice for combating Unsolicited Bulk Email" pode ser consultado no sítio Web da RIPE (ver: http://www.ripe.net). Mais recentemente, a IRTF (Internet Research Task Force) constituiu um grupo de investigação anti-"spam" (ver: http://www.irtf.org/charters/asrg.html). Este grupo pode desenvolver certas tecnologias que poderão servir de ponto de partida para os esforços de normalização no âmbito da IETF (Internet Engineering Task Force).

aos clientes dos seus clientes. Estas questões não se inserem, porém, no âmbito da presente comunicação.

No que respeita à filtragem nos serviços móveis, as diferenças no contexto dos modelos empresariais entre os serviços móveis e os serviços Internet fixos pode justificar soluções diferentes. Nomeadamente o primeiro modelo inclui normalmente taxas de entrega por mensagem, o que encarece o "spam". No entanto, alguns novos serviços implicam uma facturação baseada na importação (*retrieval*), o que significa que o "spam" aumenta os custos para o destinatário. Além disso, o correio electrónico já pode agora ser entregue em terminais móveis. Poderão então ser fornecidos aos assinantes filtros e meios de visualização para gerirem o "spam" móvel.

Há que ter em conta igualmente os retransmissores abertos. Resumidamente, os retransmissores abertos são servidores SMTP que podem ser utilizados para retransmitir mensagens enviadas por utilizadores distintos dos utilizadores locais do servidor. Até agora, os retransmissores eram, na sua maioria, abertos. No entanto, os retransmissores abertos são facilmente utilizáveis pelos autores de "spam" para o envio de comunicações não solicitadas. A tomada de medidas preventivas simples reduzirá as possibilidades de tais práticas abusivas. O mesmo se pode dizer em relação aos servidores *proxy* abertos, que são servidores que utilizam software que permite a interacção directa com a Internet.

4.3.2. Acções propostas

Os Estados-Membros e as autoridades competentes são convidados a clarificar as condições legais, a nível nacional, em que podem funcionar os diferentes tipos de software de filtragem, incluindo os requisitos em matéria de protecção da privacidade.

Os fornecedores de software de filtragem devem garantir a compatibilidade dos seus sistemas de filtragem com o regime de "opt-in" e outros requisitos da legislação comunitária, incluindo requisitos associados à confidencialidade das comunicações.

Deve ser dada aos utilizadores a oportunidade de gerirem o tratamento do "spam" recebido, de acordo com as necessidades de cada um. Os fornecedores de software de filtragem têm de ter em conta as consequências para os utilizadores dos "falsos positivos", das "falsos negativos", de certas formas de filtragem baseada nos conteúdos e as eventuais questões conexas de responsabilização.

As empresas da área da filtragem devem cooperar com as partes interessadas com vista ao desenvolvimento de técnicas que reconheçam o correio electrónico comercial que corresponde às práticas de marketing aceites pelo direito comunitário, incluindo dispositivos de confidencialidade (*webseals*), rótulos, etc.

Os fornecedores de serviços de correio electrónico (e de serviços móveis, se for o caso) devem oferecer meios ou serviços de filtragem aos seus clientes como opção disponível a pedido, bem como informações sobre os serviços e produtos de filtragem de terceiros que se encontram ao dispor dos utilizadores finais.

Os proprietários de servidores de correio devem certificar-se de que os seus servidores estão protegidos e não se encontram no modo "retransmissão aberta" (excepto em casos justificados). O mesmo se aplica aos servidores *proxy* abertos.

5. ACÇÕES DE SENSIBILIZAÇÃO

A presente secção relativa às questões da sensibilização centra-se nas acções propostas em domínios como a prevenção, a sensibilização do consumidor e a comunicação de problemas.

5.1. Discussão

Os Estados-Membros da UE deviam ter transposto para o direito nacional o novo regime de consentimento prévio ("opt-in") relativo ao correio electrónico não solicitado até 31 de Outubro de 2003. Embora esta nova abordagem tenha sido convenientemente publicitada na imprensa, podem subsistir algumas dúvidas entre os intervenientes no mercado e os cidadãos acerca do verdadeiro significado prático do conceito[38].

Esta nova abordagem baseia-se na atribuição de poderes ao utilizador para autorizar ou não a recepção de comunicações comerciais. Para que tal seja possível, porém, o utilizador tem de conhecer as regras de base aplicáveis às comunicações não solicitadas e saber para onde deve comunicar os problemas.

Melhores práticas

O Comissário para a Informação do Reino Unido (*UK Information Commissioner*), a entidade britânica responsável pela protecção dos dados, publicou, umas semanas antes da entrada em vigor da nova regulamentação que transpõe a directiva, um documento de orientação que explica as novas regras do Reino Unido, dedicando uma parte específica ao marketing por via electrónica. A *Information Commission* anunciou igualmente que os formulários para a apresentação de queixas estariam disponíveis em linha e nas suas instalações a partir do momento em que as regras entrassem em vigor, indicando as informações que será provavelmente necessário fornecer[39].

Os utilizadores devem, além disso, compreender os riscos inerentes à comunicação dos seus dados pessoais através da Internet (por exemplo, deixando-os nos sítios Web ou nos fóruns de discussão Usenet que visitam) e adaptar o seu comportamento em conformidade.

Por último, os utilizadores precisam de saber qual o software de filtragem existente no mercado e de que modo os fornecedores de serviços e os fornecedores de software (FSI, FSCE) os podem ajudar.

Melhores práticas

A *Commission Nationale Informatique et Libertés* ('CNIL'), a entidade francesa responsável pela protecção dos dados, introduziu no seu sítio Web um conjunto completo de informações sobre vários aspectos do "spam", a saber: os resultados da sua experiência com a caixa de correio e os casos remetidos para as autoridades judiciais (ver adiante), orientações básicas sobre o modo de impedir o "spam", informações sobre o modo de participar a recepção de "spam", referências a associações de utilizadores activas neste domínio, etc.

---

38 As informações de base sobre as regras aplicáveis às comunicações não solicitadas previstas na Directiva 2002/58/CE encontram-se disponíveis no seguinte endereço URL: http://europa.eu.int/information_society/topics/ecomm/all_about/todays_framework/privacy_protection/index_en.htm#unsolicited.

39 Ver: http://www.dti.gov.uk/industries/ecommunications/directive_on_privacy_electronic_communications_2002/58/EC.html#guidance

Apesar de se terem realizado, ou estarem previstas, acções de sensibilização relativas ao novo regime de consentimento prévio na maioria dos Estados-Membros, essas acções apresentam grandes diferenças em termos de calendário, natureza das informações fornecidas, público-alvo e partes envolvidas. Alguns Estados-Membros, no entanto, estão a aguardar a entrada em vigor da legislação nacional sobre esta matéria. As consultas públicas sobre a transposição da Directiva 2002/58/CE contribuíram, em certa medida, nos países onde tiveram lugar, para sensibilizar as pessoas.

Estas acções podem ser da responsabilidade de várias autoridades, dependendo dos respectivos poderes em cada Estado-Membro (por exemplo, autoridades responsáveis pela protecção dos dados (APD), ARN, autoridades responsáveis pela protecção dos consumidores (APC), provedores). Não existe (ainda) em todos os Estados-Membros uma coordenação entre as várias autoridades competentes. Tudo indica que, nalguns Estados-Membros, os ministérios estão envolvidos. As associações do sector estão muitas vezes envolvidas. Nalguns casos, as associações de consumidores ou de utilizadores também participam nessas acções.

Alguns intervenientes do sector lançaram igualmente acções de sensibilização a nível nacional, comunitário ou mundial, embora, mais uma vez, essas acções apresentem diferenças consideráveis. Eis algumas delas:

- guias práticos para as empresas de venda directa, ou campanhas dirigidas especificamente ao sector das comunicações;
- orientações gerais para os clientes sobre códigos de conduta, mecanismos de depósito de queixas e filtragem;
- plataformas/grupos de trabalho encarregados de elaborar as boas práticas para as comunicações comerciais.

5.2. Acções propostas

Para dar a conhecer plenamente o novo receituário do correio electrónico comercial, há que desenvolver a curto prazo uma acção sustentável de grande envergadura em todos os Estados-Membros em matéria de prevenção e de aplicação efectiva da lei. Devem fornecer-se informações práticas sobre prevenção, práticas de marketing aceitáveis e soluções legais aos dispor dos utilizadores.

Todas as partes, desde Estados-Membros e autoridades competentes até empresas e associações de consumidores/utilizadores, são chamadas a desempenhar o seu papel nas acções de sensibilização. Os Estados-Membros e as autoridades competentes que ainda o não fazem são convidados a lançar ou a apoiar campanhas de sensibilização no início de 2004.

No que respeita, concretamente, à natureza das informações fornecidas, as acções destinadas às empresas e/ou consumidores devem incluir:

O programa "Para uma Internet mais segura" e o "spam"

A Comissão Europeia publicou um convite à apresentação de propostas no âmbito do programa "Para uma Internet mais segura", em que podiam ser propostos projectos de combate ao "spam" no âmbito de várias acções, nomeadamente no domínio da sensibilização. Os projectos seleccionados após a primeira avaliação prevista por este convite poderão arrancar em Maio de 2004.

A Comissão está neste momento a preparar uma proposta de programa de seguimento, "Para uma Internet mais segura *plus"*, que proporá o financiamento de novas medidas de combate aos conteúdos ilícitos e nocivos e aos conteúdos não desejados, como o "spam".

http://www.europa.eu.int/information_society/programmes/iap/call/index_en.htm

– acções que visem garantir uma compreensão básica mas generalizada das novas regras e dos direitos que lhes assistem por força dessas regras;

– informações práticas sobre as práticas de marketing aceitáveis à luz do regime de consentimento prévio ("opt-in"), incluindo a clarificação do conceito de recolha legítima de dados pessoais;

– informações práticas aos consumidores sobre os métodos para evitar o "spam" (por exemplo, utilização de dados pessoais, etc.);

– informações práticas aos consumidores sobre os produtos e serviços disponíveis para evitar o "spam" (filtragem, segurança);

– informações sobre as medidas práticas a tomar quando confrontados com "spam", incluindo os mecanismos de apresentação de queixas e os mecanismos alternativos de resolução de litígios (MARL), quando disponíveis.

Estas acções devem ter como alvo os seguintes grupos:
a) empresas envolvidas no marketing directo ou que recorrem a essa técnica,
b) consumidores que são assinantes de correio electrónico, incluindo de serviços SMS
c) fornecedores de serviços de correio electrónico, incluindo fornecedores de serviços móveis.

As acções de sensibilização devem efectuar-se através de diferentes canais (e não unicamente através da Web), com o objectivo de atingir efectivamente os vários públicos visados. Nesta matéria, é importante o envolvimento das associações empresariais do sector e de consumidores. Deve garantir-se a coordenação entre as diversas iniciativas eventuais.

As acções atrás enumeradas devem igualmente fazer referência aos códigos de conduta do sector reconhecidos como eficazes, aos mecanismos de apresentação de queixas, aos rótulos (por exemplo, rótulos de confiança) e sistemas de certificação, caso existam.

Os serviços da Comissão já fornecem informações sobre as características básicas do sistema de "opt-in" no sítio Web EUROPA[40]. Essas informações remetem igualmente, através de hiperligações, para aspectos da implementação a nível nacional e para números disponíveis e tendências básicas em matéria de "spam". Os serviços da Comissão utilizarão igualmente os eurogabinetes (Euro Info Centres) para divulgar as informações sobre as novas regras.

CONCLUSÃO

O "spam" é um dos principais desafios com que a Internet se defronta hoje em dia. O combate ao "spam" exige, no entanto, uma acção em várias frentes, envolvendo não só a execução eficaz das regras e a cooperação internacional efectiva, mas também a aplicação de soluções técnicas e de auto-regulação por parte das empresas e a sensibilização dos consumidores. O conjunto de acções identificadas na presente comunicação foi sintetizado no quadro que se segue.

[40] http://europa.eu.int/information_society/topics/ecomm/highlights/current_spotlights/spam/index_en.htm

Embora a Comissão apoie tanto quanto possível esses esforços, as acções a desenvolver tanto a nível nacional como internacional competirão principalmente aos Estados-Membros da UE e autoridades competentes, às empresas do sector e aos consumidores e utilizadores da Internet e dos serviços de comunicações electrónicas.

A implementação integrada e paralela do conjunto de acções identificadas na presente comunicação, que contam com o amplo apoio das partes interessadas, pode contribuir para reduzir substancialmente a quantidade de "spam" que neste momento põe em causa os benefícios do correio electrónico e outras comunicações electrónicas para as nossas sociedades e economias.

A Comissão acompanhará a implementação dessas acções ao longo de 2004, nomeadamente através do grupo informal para as comunicações não solicitadas. Até ao final de 2004, a Comissão decidirá se é necessário propor novas medidas ou acções correctivas.

QUADRO: SÍNTESE DO CONJUNTO DE ACÇÕES INDENTIFICADAS NA COMUNICAÇÃO

O quadro que se segue sintetiza as acções identificadas na comunicação. As acções da Comissão/serviços da Comissão são apresentadas separadamente. Como atrás indicado, as acções interrelacionam-se de certo modo, devendo ser implementadas tanto quanto possível em paralelo e de um modo integrado.

I – Implementação e controlo da aplicação eficazes pelos Estados-Membros e autoridades competentes

Como requisito prévio, os Estados-Membros devem transpor sem demora a directiva relativa à privacidade e às comunicações electrónicas, nomeadamente as disposições respeitantes às comunicações não solicitadas.

Os Estados-Membros e as autoridades competentes devem avaliar a eficácia dos seus mecanismos de execução em termos de reparação judicial e sanções, mecanismos de apresentação de queixas, cooperação intracomunitária e cooperação com países terceiros e monitorização. Os Estados-Membros devem também desenvolver estratégias nacionais para garantir a cooperação entre as autoridades responsáveis pela protecção dos dados, as autoridades responsáveis pela protecção do consumidor e as ARN e para evitar a sobreposição e a duplicação de tarefas entre autoridades.

Os Estados-Membros e as autoridades competentes devem, nomeadamente:

(a) Reparação judicial e sanções eficazes

- prever devidamente a possibilidade de as vítimas exigirem indemnizações e prever sanções concretas, incluindo sanções financeiras e penais, quando adequado;

- nos Estados-Membros em que não está prevista uma reparação administrativa, considerar a criação de tais procedimentos para fazer aplicar as novas regras;

- dotar as autoridades competentes dos necessários poderes de investigação e execução;

(b) Mecanismos de apresentação de queixas

- estabelecer mecanismos adequados para a apresentação de queixas, incluindo caixas de correio específicas, para onde os utilizadores possam enviar as suas queixas;

- coordenar a acção das várias autoridades competentes envolvidas;

(c) Queixas transfronteiras e cooperação em matéria de execução dentro da UE

- utilizar, ou criar, caso seja necessário, um mecanismo de ligação através do qual as autoridades nacionais possam cooperar com vista a fazer aplicar as regras a nível transfronteiras (troca de informações, assistência mútua) dentro da UE. Neste contexto, no que respeita ao "spam" fraudulento e enganoso em particular, pede-se ao Conselho e ao Parlamento que dêem o seu acordo, o mais rapidamente possível, à proposta de regulamento relativo à cooperação em matéria de protecção do consumidor e ponderem em que medida a directiva "Privacidade e Comunicações Electrónicas" deve ser acrescentada ao âmbito do regulamento;

(d) Cooperação com países terceiros

- participar activamente em fóruns multilaterais (como a OCDE) com vista à elaboração de soluções a nível internacional;

- reforçar, ou iniciar, a cooperação bilateral com países terceiros,

- estudar, com a Comissão, as iniciativas que esta pode tomar para facilitar a cooperação internacional;

- cooperar com o sector privado na localização dos autores de "spam", sob reserva das garantias jurídicas apropriadas.

(e) Monitorização

- garantir que dispõem das informações e estatísticas necessárias para poderem centrar os seus esforços no domínio da execução das regras, quando adequado em cooperação com as empresas do sector e tendo em conta os trabalhos de medição em curso na OCDE.

II – Acções de auto-regulação e acções técnicas por parte do sector

Os intervenientes no mercado (FSI, FSCE, operadores móveis, empresas de software, empresas de marketing directo) devem procurar transformar o regime de "opt-in" numa prática quotidiana, em cooperação com as associações de consumidores/utilizadores e as autoridades competentes, quando adequado, e, nomeadamente:

(a) Acções de auto-regulação

- avaliar e, se necessário, adaptar as práticas contratuais dos fornecedores de serviços (FSI, FSCE, operadores móveis) em relação aos assinantes e aos parceiros comerciais, fornecer informações sobre a filtragem e eventualmente fornecer software ou serviços de filtragem como serviço opcional para o cliente;

- adaptar as práticas de marketing directo ao regime de "opt-in" e, eventualmente, acordar em métodos específicos e legais de recolher dados pessoais (por exemplo, sistemas de "opt-in" "duplos" ou "confirmados");

- desenvolver e divulgar códigos de boas práticas eficazes (por exemplo, a iniciativa FEDMA) conformes com o sistema de "opt-in", em cooperação com o Grupo de Trabalho do Artigo 29.º para a protecção dos dados ou as autoridades nacionais competentes, quando adequado;

- considerar a utilização de rótulos para as mensagens de correio electrónico conformes com o sistema de "opt-in" e bases de dados para ajudar os utilizadores (e os filtros) a reconhecê-las, em consonância com a Directiva "Comércio Electrónico";

- utilizar, ou criar, se necessário, por via da auto-regulação, mecanismos de apresentação de queixas e mecanismos alternativos de resolução de litígios (MARL) eficazes, empre que possível com base nas iniciativas existentes (por exemplo, EEJ-NET).

(b) Acções técnicas

- (fornecedores de software de filtragem) garantir a compatibilidade dos seus sistemas de filtragem com o regime de "opt-in" e outros requisitos da legislação comunitária, incluindo os requisitos a nível da confidencialidade das comunicações; os Estados-Membros e as autoridades competentes são convidados a clarificar as condições jurídicas em que os diferentes tipos de software de filtragem podem funcionar no país, incluindo os requisitos em matéria de protecção da privacidade;

- (fornecedores de software de filtragem) ter em conta as consequências para os utilizadores dos "falsos positivos" e dos "falsos negativos", certas formas de filtragem baseadas nos conteúdos e eventuais problemas conexos de responsabilização. Deve ser dada a oportunidade aos utilizadores de determinarem o modo como o correio de entrada é tratado, de acordo com as necessidades de cada um;

- (fornecedores de software de filtragem) cooperar com as partes interessadas com vista ao desenvolvimento de técnicas de reconhecimento do correio electrónico comercial legítimo (ou seja, que corresponde às práticas de marketing aceites à luz do direito comunitário), nomeadamente rótulos.

- (fornecedores de serviços de correio electrónico e, se for o caso, de serviços móveis) oferecer meios ou serviços de filtragem aos seus clientes como opção disponível a pedido, bem como informações sobre os serviços e produtos de filtragem de terceiros ao dispor dos utilizadores finais;

- (proprietários de servidores de correio) certificar-se da segurança dos seus servidores no sentido de não se encontrarem no modo "retransmissor aberto" (excepto em caso justificado). O mesmo se aplica aos servidores *proxy*.

III – Acções de sensibilização por parte dos Estados-Membros, das empresas do sector e das associações de consumidores/utilizadores

Os Estados-Membros e as autoridades competentes que ainda não o fazem são convidados a lançar ou a apoiar campanhas de sensibilização no início de 2004.

Todas as partes, desde Estados-Membros e autoridades competentes até às empresas do sector e associações de consumidores e/ou utilizadores, devem lançar campanhas destinadas a fornecer informações práticas sobre prevenção, práticas de marketing aceitáveis e soluções técnicas e legais ao dispor dos utilizadores, e, nomeadamente:

- centrar as acções: a) nas empresas envolvidas no marketing directo ou que a ele recorrem, b) nos consumidores que são assinantes de serviços de correio electrónico, incluindo serviços SMS, e c) nos fornecedores de serviços de correio electrónico, incluindo fornecedores de serviços móveis;

- fornecer às empresas e/ou consumidores:

- conhecimentos de base, mas largamente difundidos, sobre as novas regras e sobre os seus direitos ao abrigo dessas regras;

- informações práticas sobre as práticas de marketing aceitáveis à luz do regime de "opt-in", incluindo a clarificação do conceito de recolha legítima de dados pessoais;

- informações aos consumidores sobre as maneiras de evitar o "spam" (por exemplo, utilização de dados pessoais, etc.);

- informações aos consumidores sobre os produtos e serviços disponíveis para evitar o "spam" (por exemplo, filtragem, segurança);

- informações sobre as medidas práticas a tomar quando confrontados com "spam", incluindo informações sobre os mecanismos de apresentação de queixas e os mecanismos alternativos de resolução de litígios (MARL), caso existam;

- fazer referência aos códigos de conduta do sector reconhecidos como eficazes, aos mecanismos de apresentação de queixas, aos rótulos (por exemplo, rótulos de confiança. (*trustmarks*) e sistemas de certificação, caso existam;

- realizar estas actividades de sensibilização através de diferentes canais, em linha e fora de linha, com vista a atingir efectivamente os vários públicos visados.

Neste capítulo, o envolvimento das empresas do sector e das associações de consumidores é importante. Deve garantir-se a coordenação entre as várias iniciativas eventualmente lançadas.

IV – Acções da Comissão/serviços da Comissão

A Comissão monitorizará, ao longo de 2004, a implementação das acções acima resumidas, inclusivamente por intermédio do grupo informal para as comunicações não solicitadas, e avaliará, até ao final de 2004, se são necessárias medidas adicionais ou correctivas.

A Comissão continuará a acompanhar atentamente a aplicação da directiva. A Comissão procurará, nomeadamente, certificar-se de que as medidas nacionais de transposição prevêem verdadeiras sanções, incluindo, em certos casos, sanções financeiras ou penais, para a violação dos requisitos da directiva. (Em Novembro de 2003, a Comissão deu início a procedimentos de infracção contra vários Estados-Membros que não notificaram as suas medidas de transposição nacionais.) Os serviços da Comissão prontificam-se a ajudar os Estados-Membros nessa matéria, se necessário.

Os serviços da Comissão criaram, com o apoio dos Estados-Membros e das autoridades responsáveis pela protecção dos dados, um grupo informal em linha para as comunicações comerciais não solicitadas. O grupo facilitará o trabalho relativo à execução eficaz da legislação (por exemplo, no que respeita a queixas, soluções judiciais, sanções, cooperação internacional) e às restantes acções identificadas na presente comunicação.

Os serviços da Comissão pedirão ao Grupo de Trabalho do Artigo 29.º que se pronuncie sobre alguns conceitos utilizados na Directiva "Privacidade e Comunicações Electrónicas" o mais rapidamente possível, contribuindo assim para uma aplicação uniforme das medidas nacionais adoptadas em conformidade com a directiva.

Os serviços da Comissão começaram já a estudar, com os Estados-Membros e as autoridades nacionais envolvidas na execução da legislação, qual o melhor modo de garantir a execução da legislação a nível transfronteiras dentro da UE e em relação a países terceiros. Este trabalho conjunto com as autoridades nacionais prosseguirá ao longo de 2004.

A Comissão apoiará a elaboração de códigos de conduta para toda a Europa relativos ao marketing directo, a disponibilizar em linha, e, se necessário, a sua aprovação pelo Grupo de Trabalho do Artigo 29.º para a protecção dos dados.

Em Fevereiro de 2004, a Comissão acolherá um seminário da OCDE sobre "spam" e discutirá com os Estados-Membros as acções de seguimento a realizar, incluindo os trabalhos em curso na OCDE destinados a promover uma legislação eficaz a nível internacional, a sensibilização, as soluções técnicas, a auto-regulação e a cooperação internacional em matéria de execução da lei.

A Comissão estudará igualmente a melhor maneira de dar seguimento às conclusões da Cimeira Mundial de 2003 sobre a Sociedade da Informação na UE, tendo em conta a Cimeira de Túnis, a realizar em 2005.

A Comissão publicou um convite à apresentação de propostas no âmbito do programa "Para uma Internet mais segura", em que podem ser propostos, ao abrigo de várias acções, projectos para combater o "spam"; a Comissão está neste momento a preparar uma proposta de programa de seguimento, o programa "Para uma Internet mais segura *plus"*, que proporá o financiamento de novas medidas para combater, nomeadamente, o "spam".

Os serviços da Comissão continuarão a fornecer informações sobre as características básicas do regime de "opt-in" no sítio Web EUROPA. Através de hiperligações, far-se-á referência a aspectos da implementação do regime a nível nacional e aos números e tendências básicos relativos ao "spam", caso se encontrem disponíveis. Os serviços da Comissão servir-se-ão igualmente dos eurogabinetes (Euro Info Centres) para divulgar informações sobre as novas regras.