00451/06/PT
WP 118

Parecer do Grupo de trabalho "protecção de dados" criado pelo artigo 29.º sobre a prestação de serviços de filtragem de correio electrónico

Adoptado em 21 de Fevereiro de 2006

GRUPO DE TRABALHO SOBRE A PROTECÇÃO DAS PESSOAS NO QUE DIZ RESPEITO AO TRATAMENTO DE DADOS PESSOAIS,

criado pela Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995[1],

Tendo em conta o artigo 29.° e o n.º 1, alínea c) e o n.º 3 do artigo 30.º da referida directiva,

Tendo em conta o seu regulamento interno, nomeadamente os artigos 12.º e 14.º,

ADOPTOU O PRESENTE PARECER:

I. INTRODUÇÃO

O Grupo de trabalho "protecção de dados", criado pelo artigo 29.º da Directiva 95/46/CE (a seguir designado "Grupo de trabalho do artigo 29.º") está consciente do desenvolvimento dos diferentes serviços de comunicação em linha, incluindo os serviços gratuitos de correio electrónico na Internet e serviços afins. O desenvolvimento dos serviços de comunicações electrónicas fez aumentar as preocupações relativas à protecção da privacidade das comunicações, em especial devido às práticas existentes em matéria de verificação do conteúdo de mensagens com a finalidade de eliminar mensagens não solicitadas (*spam*) e vírus, bem como para detectar certos conteúdos predeterminados.

O Grupo de trabalho do artigo 29.º está consciente de que a maioria dos fornecedores de serviços Internet e de serviços de correio electrónico ("ISP – internet service providers" e "ESP - email service providers") utiliza ferramentas de filtragem para proteger redes e máquinas bem como, nalguns casos, para inspeccionar as comunicações com finalidades comerciais. Contudo, este Grupo de trabalho considera que, em certos casos, a utilização de tais ferramentas de filtragem pode não estar em conformidade com a legislação de protecção dos dados em vigor, que a seguir se descreve. Isso deve-se, nomeadamente, ao facto de a aplicação da legislação a estes novos tipos de serviços nem sempre ser clara.

O objectivo principal deste parecer é fornecer orientações relativamente às questões de confidencialidade do correio electrónico e, mais especificamente, à filtragem das comunicações em linha. Em especial, surgiu uma questão relativa à análise das comunicações que geralmente os ISP e ESP realizam, com vários objectivos, que constitui uma intercepção das comunicações, e sobre as condições em que tal intercepção pode ser justificada.

Para tanto, este documento analisa, entre outras, as disposições relativas à confidencialidade das comunicações electrónicas, tal como definidas no n.º 1 do artigo 5.° da Directiva 2002/58 relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas, bem como noutras disposições relevantes que são parte do acervo comunitário e das legislações nacionais que o aplicam.

II. QUADRO JURÍDICO DA PROTECÇÃO DOS DADOS E DA PRIVACIDADE DAS COMUNICAÇÕES DE CORREIO ELECTRÓNICO

A) Convenção Europeia para a Protecção dos Direitos do Homem e das Liberdades Fundamentais

A confidencialidade das comunicações está garantida nos termos dos instrumentos internacionais relativos aos direitos humanos, nomeadamente da Convenção Europeia para a Protecção dos Direitos do Homem e das Liberdades Fundamentais (CEDH) e das constituições dos Estados-Membros. É igualmente garantida pelas duas directivas comunitárias descritas em seguida.

---

[1] JO L 281 de 23.11.1995, p. 31,disponível em: http://europa.eu.int/comm/internal_market/privacy/law_fr.htm

O artigo 8.° da CEDH assegura a todos o respeito da sua vida privada e da sua correspondência, estabelecendo as condições em que podem ser aceites restrições a estes direitos. O Tribunal Europeu dos Direitos do Homem (a seguir designado "Tribunal") aplicou em várias ocasiões o artigo 8.° às comunicações de correio clássico.

Considerou-se que a intercepção, abertura, leitura, atraso da recepção, ou criação de entraves ao envio de correspondência contrariam o artigo 8.° da CEDH[2]. Da jurisprudência da Comissão e do Tribunal Europeu dos Direitos do Homem pode concluir-se que, mediante a conjugação das noções de "vida privada" e de "correspondência", as comunicações de correio electrónico estão seguramente abrangidas pelo artigo 8.° da CEDH[3]. Os utilizadores de correio electrónico podem razoavelmente esperar que as suas comunicações não sejam inspeccionadas por terceiros, quer públicos quer privados.

O dever de respeito da "correspondência" inclui não só a sua confidencialidade mas também o direito de a enviar e receber[4]. Assim, pode concluir-se que uma proibição genérica do envio ou recepção de correio electrónico viola o artigo 8.° da CEDH.

Qualquer pessoa abrangida pela jurisdição de um dos Estados signatários da CEDH tem direito ao respeito da sua vida privada e da sua correspondência, o que inclui todas as partes envolvidas numa comunicação. No processo A/França (1993), o Tribunal decidiu que a gravação de uma conversa telefónica com o consentimento apenas de uma das partes contrariava o direito ao respeito pela correspondência da outra parte envolvida na comunicação.

Segundo a CEDH, os Estados contratantes podem legalmente interceptar a correspondência, incluindo as comunicações electrónicas, ou adoptar outras medidas, se tal for necessário para alcançar determinados objectivos previstos na Convenção, interpretados segundo a jurisprudência do Tribunal Europeu dos Direitos do Homem. Pode definir-se "intercepção" como o acesso por terceiros ao conteúdo e/ou aos dados de tráfego relacionados com as comunicações privadas entre dois correspondentes ou mais, incluindo os dados de tráfego referentes à utilização dos serviços de comunicação electrónicos, que constitua uma violação do direito das pessoas à privacidade e à confidencialidade da correspondência. Tal ingerência é inaceitável, a menos que, nos termos do n.º 2 do artigo 8.° da CEDH e da interpretação que o Tribunal faz desta disposição, preencha três critérios fundamentais:

"…um fundamento legal, a necessidade de tal medida numa sociedade democrática e a sua conformidade com um dos objectivos legítimos constantes da Convenção…".

---

[2] No processo "Niemitz" (de 1992), o Tribunal decidiu que as cartas já entregues ao destinatário estavam abrangidas pelo artigo 8.° da CEDH. Nessa decisão o Tribunal afirmou igualmente que esta protecção abrange não só as comunicações privadas, como também a correspondência comercial. Nos processos "Klass" (de 1978), "Malone" (de 1984) e "Huvig" (de 1990), o Tribunal afirmou que as comunicações telefónicas são igualmente abrangidas pelo artigo 8.°. No que se refere a outros meios de comunicação, tem relevância o processo "Mersch" da Comissão (1985): a Comissão considerou que a intercepção de qualquer forma de comunicação constitui uma violação do artigo 8.°.

[3] Esta conclusão é apoiada pelo facto de na maioria dos Estados-Membros a inspecção de mensagens de correio electrónico estar proibida e de, tanto a nível internacional como nacional, terem sido criados poderes específicos para interceptar correio electrónico.

[4] Processo Golder (1975), considerando 43: "Impedir alguém de trocar correspondência constitui, desde logo, a forma mais grave de "ingerência" (n.º 2 do artigo 8.°) com o exercício do direito ao "respeito da sua correspondência"; é inconcebível que tal não esteja abrangido pelo artigo 8.º, quando este abrange inquestionavelmente a sua mera supervisão". A retenção de correio recebido também constitui uma ingerência (processo "Schöneberger & Durmaz" de 1988).

A nível das relações privadas, contudo, o mecanismo mais relevante para a aplicação dos direitos previstos na Convenção é a doutrina das obrigações positivas das Partes Contratantes. Para lá da obrigação de não ingerência, as Partes Contratantes também têm de adoptar medidas positivas para assegurar o gozo efectivo destes direitos, não só relativamente aos poderes públicos como na esfera das relações entre os privados. Isso inclui a obrigação de estabelecer um quadro jurídico adequado para o exercício destes direitos.

O n.º 2 do artigo 6.° do Tratado da União Europeia indica claramente que a União respeitará os direitos fundamentais tal como os garante a CEDH, e tal como resultam das tradições constitucionais comuns aos Estados-Membros, enquanto princípios gerais do direito comunitário. Nos termos do n.º 3 do artigo 52.° da Carta dos Direitos Fundamentais da UE, o significado e o âmbito dos direitos constantes da Carta serão os mesmos do que os previstos na CEDH. Esta disposição não impede o direito comunitário de prever uma protecção acrescida.

B) Disposições específicas aplicáveis à confidencialidade das comunicações de correio electrónico

Conforme referimos, a confidencialidade das comunicações é garantida por mais duas directivas comunitárias. Ao avaliar a questão da confidencialidade das comunicações, as disposições destas directivas devem ser interpretadas em conjugação com a CEDH, bem como com a jurisprudência do Tribunal Europeu dos Direitos do Homem anteriormente descrita.

A Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Directiva "protecção de dados"), cria um regime jurídico horizontal para assegurar o respeito dos direitos individuais à protecção de dados. No que se refere ao tratamento dos dados pessoais, a Directiva "protecção de dados" faz referência ao direito à privacidade, tal como reconhecida no artigo 8.° da CEDH[5]. O direito de receber e enviar informação é igualmente reconhecido como estando incluído na liberdade de informação garantida pelo artigo 10.° da CEDH[6]. Além disso, segundo o considerando 47, será a pessoa de quem emana a mensagem, e não quem propõe o serviço de transmissão, que em regra será considerada responsável pelo tratamento dos dados pessoais contidos na mensagem; contudo, as pessoas que propõem esses serviços serão em regra consideradas responsáveis pelo tratamento dos dados pessoais suplementares necessários ao funcionamento do serviço.

A Directiva 2002/58/CE do Parlamento Europeu e do Conselho, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva "privacidade das comunicações electrónicas"), aplica-se ao tratamento de dados pessoais no contexto da prestação de serviços de comunicações electrónicas publicamente disponíveis nas redes públicas de comunicações da Comunidade. As disposições desta directiva especificam e complementam as da Directiva "protecção de dados". A confidencialidade das comunicações é protegida, em especial, pelo artigo 5.° da Directiva "privacidade das comunicações electrónicas", que estabelece:

---

5 Considerando 10: "Considerando que o objectivo das legislações nacionais relativas ao tratamento de dados pessoais é assegurar o respeito dos direitos e liberdades fundamentais, nomeadamente do direito à vida privada, reconhecido não só no artigo 8.º da Convenção Europeia para a Protecção dos Direitos do Homem e das Liberdades Fundamentais como nos princípios gerais do direito comunitário".

6 Considerando 37: Considerando que o tratamento de dados pessoais para fins jornalísticos ou de expressão artística ou literária, nomeadamente no domínio do audiovisual, deve beneficiar de derrogações ou de restrições a determinadas disposições da presente directiva, desde que tal seja necessário para conciliar os direitos fundamentais da pessoa com a liberdade de expressão, nomeadamente a liberdade de receber ou comunicar informações, tal como é garantida, nomeadamente, pelo artigo 10º da Convenção Europeia para a Protecção dos Direitos do Homem e das Liberdades Fundamentais".

"Os Estados-Membros garantirão, através da sua legislação nacional, a confidencialidade das comunicações e respectivos dados de tráfego realizadas através de redes públicas de comunicações e de serviços de comunicações electrónicas publicamente disponíveis. Proibirão, nomeadamente, a escuta, a instalação de dispositivos de escuta, o armazenamento ou outras formas de intercepção ou vigilância de comunicações e dos respectivos dados de tráfego por pessoas que não os utilizadores, sem o consentimento dos utilizadores em causa, excepto quando legalmente autorizados a fazê-lo…".

Além disso, o artigo 4.° da Directiva "privacidade das comunicações electrónicas" determina que "*o prestador de um serviço de comunicações electrónicas publicamente disponível adoptará as medidas técnicas e organizativas adequadas para garantir a segurança dos seus serviços, se necessário conjuntamente com o fornecedor da rede pública de comunicações no que respeita à segurança da rede*".

Igualmente relevante é a Directiva "comércio electrónico", em especial as disposições relativas à responsabilidade dos fornecedores de serviços Internet e de correio electrónico, segundo as quais os Estados-Membros não podem atribuir obrigações genéricas de controlo aos ISP e ESP. Essas obrigações constituiriam uma infracção à liberdade de informação bem como à confidencialidade da correspondência (artigo 15.° da Directiva "comércio electrónico"[7]).

III. FILTRAGEM DO CONTEÚDO DAS MENSAGENS DE CORREIO ELECTRÓNICO

Neste contexto jurídico, coloca-se a questão de saber se a filtragem das comunicações frequentemente realizada pelos ISP ou ESP para atingirem diversos objectivos é compatível com a legislação comunitária.

A maioria dos ISP e ESP examinam minuciosamente as mensagens de correio electrónico de forma rotineira para fins como a filtragem de *spam*, a detecção de vírus ou a correcção ortográfica. As mensagens também são reencaminhadas, classificadas como urgentes, respondidas automaticamente, convertidas em mensagens de texto para telemóveis (SMS), guardadas automaticamente e armazenadas em pastas ou são ainda objecto de conversão das suas hiperligações em texto.

Em seguida é analisado o enquadramento jurídico da filtragem efectuada pelas seguintes razões: a) detecção de vírus, b) filtragem de *spam* e c) detecção de quaisquer conteúdos predeterminados.

A) Filtragem de mensagens de correio electrónico com a finalidade de detectar vírus

A filtragem de vírus consiste no procedimento de verificação dos ficheiros para saber se contêm vírus conhecidos. Nalguns casos, a detecção dos vírus é acompanhada da sua limpeza, que é o procedimento de remoção do vírus detectado, de forma a que o ficheiro possa ser utilizado em segurança. Em linhas gerais, essa verificação tem lugar quando a mensagem chega aos servidores do ESP. A maioria dos prestadores de serviços de correio electrónico inclui a filtragem de vírus como elemento do seu serviço, para se protegerem a si próprios e aos utilizadores dos vírus prejudiciais. Na maioria dos casos, os utilizadores não podem desligar a filtragem automática que vem incluída por defeito como parte do serviço.

Ao avaliar os fundamentos legais que legitimam esta prática, o Grupo de trabalho do artigo 29.º considerou que a criação e utilização pelos ESP de sistemas de filtragem com o objectivo de detectar vírus se pode justificar pela obrigação de adoptar as medidas técnicas e organizativas adequadas para garantir a segurança dos seus serviços, tal como previsto no supracitado artigo 4.° da Directiva "privacidade das comunicações electrónicas".

---

[7] Directiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de Junho de 2000, relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico, no mercado interno.

Com efeito, dado que a entrega de mensagens com vírus pode interromper os serviços de correio electrónico dos prestadores (para além de danificar outros documentos e programas no equipamento do utilizador final) e prejudicar assim a transmissão de outras mensagens de correio electrónico, o Grupo de trabalho do artigo 29.º considera que a filtragem é uma medida de segurança que visa a protecção do sistema que controla os dados (ESP), o que, como anteriormente se disse, é uma obrigação vinculativa para os prestadores dos serviços electrónicos de comunicações decorrente do artigo 4.° da Directiva "privacidade das comunicações electrónicas".

O Grupo de trabalho do artigo 29.º considera que a utilização de filtros para efeitos do artigo 4.° pode ser compatível com o artigo 5.° da Directiva "privacidade das comunicações electrónicas".

O Grupo de trabalho do artigo 29.º deseja sublinhar, em especial, que as medidas referidas anteriormente estão em conformidade com os princípios gerais de direito comunitário.

Além disso, o Grupo de trabalho do artigo 29.º considera que a aplicação de sistemas de filtragem pelos ESP pode igualmente considerar-se como uma garantia da segurança do desempenho do contrato de prestação de serviços com os seus clientes, que esperam poder receber e enviar mensagens de correio electrónico com um certo grau de segurança. Deste modo, o processamento de dados efectuado pelos ESP que aplicam sistemas de filtragem pode igualmente ser considerado legítimo nos termos da alínea b) do artigo 7.° da Directiva "protecção de dados" que prevê o tratamento dos dados "*necessário para a execução de um contrato no qual a pessoa em causa é parte*".

Dado que, como se disse, nos termos do artigo 4.° da Directiva "privacidade das comunicações electrónicas" a filtragem de vírus pode ser justificada para proteger a segurança dos serviços e/ou, nos termos da alínea b) do artigo 7.° da Directiva "protecção de dados", para assegurar o próprio desempenho do contrato, sem prejuízo da confidencialidade das comunicações, o Grupo de trabalho do artigo 29.º recorda a necessidade de os fornecedores de serviços de correio electrónico assegurarem o cumprimento das seguintes condições:

a) o conteúdo das mensagens e dos anexos tem de ser mantido secreto só deve ser divulgado ao(s) destinatário(s);

b) se for encontrado um vírus, o programa instalado deve oferecer garantias suficientes em relação à confidencialidade;

c) se a filtragem dos vírus for executada sob a forma de análise do conteúdo, deve ser efectuada automaticamente e apenas com esta finalidade, ou seja, os conteúdos não devem ser analisados com qualquer outro objectivo.

Devem ser igualmente fornecidas informações sobre a filtragem (ver em seguida a secção específica.

B) Filtragem de mensagens de correio electrónico com a finalidade de detectar *spam*[8]

Os ISP e ESP utilizam várias técnicas para evitar que as mensagens de correio electrónico indesejáveis, isto é, o *spam* (não necessariamente só com publicidade), cheguem aos seus destinatários.

Uma delas consiste na utilização das chamadas "lista negras", em que os endereços IP de certos servidores e as séries de endereços IP dinâmicos atribuídos a certos ISP são repertoriados[9]. As "lista negras" não são objecto de análise aprofundada neste parecer.

A filtragem do *spam* tornou-se, de facto, uma prática necessária. Se os serviços de correio electrónico não utilizassem a filtragem do correio electrónico para eliminar o *spam*, haveria cada vez mais entradas de *spam* e os sistemas tornar-se-iam provavelmente muito lentos e ineficientes, impossibilitando praticamente o recurso aos serviços de correio electrónico pelos utilizadores. Obviamente, isso causaria o descontentamento dos consumidores e, provavelmente, implicaria limitações à possibilidade de fornecer um serviço de correio electrónico fidedigno e seguro.

Apesar de o *spam* não ser, por si só, uma ameaça para a segurança dos serviços dos ESP, mas antes para o desempenho global da rede e do serviço de correio electrónico em particular, este pode provocar a incapacidade de os ESP fornecerem o próprio serviço de correio electrónico. O Grupo de trabalho do artigo 29.º considera que o facto de o artigo 4.º da Directiva "privacidade das comunicações electrónicas" exigir que os fornecedores de serviços de correio electrónico adoptem medidas técnicas e organizativas adequadas para garantir a segurança dos seus serviços é relevante, não só para efeitos da segurança dos próprios ESP e dos serviços de rede, como também para o desempenho global dos serviços de correio electrónico e de rede. A segurança dos ESP é um problema, na medida em que afecte os seus serviços. Por este motivo, o Grupo de trabalho do artigo 29.º considera que o artigo 4.° poderia igualmente aplicar-se a esta situação. Por outras palavras, as ameaças ao desempenho geral dos serviços de correio electrónico e dos serviços de rede podem justificar que os ISP e ESP continuem a efectuar a filtragem com a finalidade de combater o *spam*. Se tivermos em conta os efeitos do *spam*, mesmo nos casos em que por dia o seu remetente distribui diariamente pouca informação através de mensagens, mas em que essa informação é enviada a um grande número de destinatários, reforça-se o argumento a favor da aplicação do artigo 4.° da Directiva "privacidade das comunicações electrónicas" porque, mesmo nestes casos, o envio de um número limitado de mensagens poderia obstruir o tráfego da Internet e lesar seriamente a fiabilidade, segurança e eficiência de serviços de correio electrónico em geral. Além disso, pelos mesmos motivos, o Grupo de trabalho do artigo 29.º considera igualmente que essa filtragem poderia ser legitimada com base na alínea b) do artigo 7.° da Directiva "protecção de dados", tendo em conta a necessidade de filtrar o spam para que o fornecedor de correio electrónico possa executar correctamente o contrato de prestação de serviços de que o destinatário é parte.

---

8 O documento da OCDE designado "Regulamentos anti-*spam*", elaborado pelo Grupo de trabalho "*spam*" em Março de 2005 (DSTI/CP/ICCP/SPAM(2005)1), define o conceito de *spam* da seguinte forma: "*O termo"spam" é frequentemente utilizado nos meios de comunicação internacionais e em declarações políticas dos diferentes países, mas não há uma definição comum geralmente aceite. Embora em geral se refira aos mesmos fenómenos, os diferentes países definem-no segundo o seu ambiente local. Para desenvolver uma política anti-spam é essencial que a sua natureza seja claramente compreendida e definida e que se separe o spam das práticas legítimas".*

9 Ao usar esta técnica, o fornecedor de correio electrónico não efectua uma filtragem, limita-se a obstruir (ou seja, recusa-se a aceitar) as mensagens provenientes dos servidores constantes da "lista negra" ou de séries de endereços IP, sem examinar o seu conteúdo. Apesar de esta prática ser, em princípio, menos intrusiva do que a filtragem dos conteúdos, podem levantar-se dúvidas a nível da liberdade de expressão, bem como do direito à liberdade de enviar e receber correspondência reconhecido pelo artigo 8.º da CEDH, de acordo com a interpretação do Tribunal.

Por outro lado, o Grupo de trabalho do artigo 29.º está preocupado com o facto de, por vezes, a filtragem dar "falsos positivos", ou seja, há mensagens "desejadas" e legítimas que não são entregues porque são consideradas *spam*. O Grupo de trabalho do artigo 29.º considera que a acção de filtrar e reter o correio recebido supostamente indesejável pode implicar não só uma ameaça à liberdade de expressão, mas também uma violação do artigo 10.° da CEDH e constituir uma ingerência nas comunicações privadas[10].

Nestes termos, sem prejuízo da aplicação do artigo 4.° da Directiva "privacidade das comunicações electrónicas" e a fim de proteger o princípio da liberdade de comunicações reconhecida pelo artigo 10.° da CEDH, bem como a confidencialidade das comunicações estabelecida no artigo 5.° da Directiva "privacidade das comunicações electrónicas" e reconhecida pelo artigo 8.° da CEDH, o Grupo de trabalho do artigo 29.º recomenda vivamente aos fornecedores de serviços de correio electrónico que tenham em conta as seguintes recomendações, que visam principalmente permitir aos destinatários de mensagens controlar as comunicações que, em princípio, lhes são endereçadas:

a) O Grupo de trabalho do artigo 29.º incentiva a prática que consiste em dar aos subscritores a possibilidade de optar por não submeter as suas mensagens à filtragem para efeitos de detecção de *spam*, de verificar se as mensagens consideradas *spam* o eram mesmo e de decidir os "tipos" de *spam* que devem ser suprimidos. Além disso, o Grupo de trabalho do artigo 29.º é igualmente favorável ao facto de alguns ESP oferecerem aos subscritores uma forma simples de optar de novo pela filtragem das suas mensagens com a finalidade de eliminar o *spam*;

b) O Grupo de trabalho do artigo 29.º incentiva igualmente o desenvolvimento de ferramentas de filtragem que os utilizadores finais podem instalar ou configurar no seu equipamento terminal, em servidores de terceiros ou no servidor de correio electrónico dos fornecedores e que lhes permitem controlar o que querem receber ou não, a fim de diminuir igualmente os custos inerentes à recepção de correio electrónico não solicitado, tal como previsto no quadragésimo quarto considerando da Directiva 2002/58. O Grupo de trabalho do artigo 29.º apoia igualmente a investigação com vista à criação de outras ferramentas para combater o *spam* que sejam menos intrusivas.

Além disso, o Grupo de trabalho do artigo 29.º lembra aos prestadores de serviços de correio electrónico que filtram mensagens para efeitos da detecção de *spam* o seu dever, decorrente do artigo 10.° da Directiva "protecção de dados", de informar os subscritores da sua política de *spam* de forma clara e inequívoca, tal como descrito na Secção IV do presente parecer. O fornecedor de serviços de correio electrónico deve igualmente assegurar a confidencialidade dos mensagens filtradas, que não devem ser utilizadas para qualquer outro objectivo.

C) Filtragem de mensagens com o objectivo de detectar quaisquer conteúdos predeterminados

O Grupo de trabalho do artigo 29.º nota que alguns fornecedores de serviços de correio electrónico se reservam o direito de examinar e até de remover qualquer conteúdo predeterminado[11], por exemplo, no caso de tal conteúdo poder alegadamente incluir material

[10] Tal como reconhecido pelo Tribunal no processo Schöneberger & Durmaz, de 1988.

[11] Ver as "condições contratuais" do serviço Yahoo: é aceite que a Yahoo! poderá, ou não, visualizar os conteúdos, mas que a Yahoo! ou os seus agentes ou representantes terão o direito (mas não a obrigação), segundo o seu critério, de visualizar, recusar ou remover qualquer conteúdo acessível através do serviço. Sem prejuízo do que precede, a Yahoo! ou os seus representantes têm o direito de remover qualquer conteúdo que desrespeite as "condições gerais" do serviço, ou que por outro motivo seja condenável. É aceite o dever de avaliar e suportar todos os riscos associados à utilização de qualquer conteúdo, incluindo a confiança na exactidão, integralidade ou utilidade de tais conteúdos. É aceite que não se pode confiar em

ilegal ou indesejado pelo destinatário que utiliza esse serviço específico. A técnica utilizada neste tipo de filtragem é muito semelhante à utilizada na detecção de vírus e *spam*.

Ao contrário da detecção de vírus, a filtragem de mensagens para detectar conteúdos predeterminados, mesmo que esses conteúdos sejam alegadamente ilegais, não pode ser considerada uma medida técnica e organizativa para proteger a segurança dos serviços de correio electrónico, tal como previsto no artigo 4.° da Directiva "privacidade das comunicações electrónicas". O material contido nessas mensagens não representa qualquer ameaça de prejuízo para o prestador de serviços de correio electrónico nem de paragem das comunicações. Por conseguinte, a filtragem para efeitos de detecção deste material não é legitimada pela necessidade de o fornecedor proteger a segurança do serviço. O Grupo de trabalho do artigo 29.º está igualmente preocupado com o facto de esse tipo de filtragem permitir aos prestadores de serviços de correio electrónico exercerem censura sobre as comunicações por correio electrónico privado, por exemplo bloqueando mensagens cujo conteúdo pode ser perfeitamente legal, o que levanta sérias dúvidas a nível da liberdade de expressão e de informação. O Grupo de trabalho do artigo 29.º sublinha que os prestadores de serviços não têm qualquer obrigação genérica de controlar os conteúdos predeterminados ou alegadamente prejudiciais mas, como em seguida se explica, este tipo de serviço poderia ser oferecido por um prestador enquanto serviço de valor acrescentado.

Assim, o Grupo de trabalho do artigo 29.º considera que, nos termos do n.º 1 do artigo 5.° da Directiva "privacidade das comunicações electrónicas", os fornecedores de correio electrónico estão proibidos de filtrar, armazenar ou efectuar qualquer outro tipo de intercepção das comunicações e dos dados de tráfego conexos com o objectivo de detectar qualquer conteúdo predeterminado sem o consentimento dos utilizadores dos serviços, sem para tanto estarem legalmente autorizados nos termos do artigo 15.° da referida directiva, tal como aplicada pela legislação dos Estados-Membros.

IV. OBRIGAÇÃO DE INFORMAR

Para além do artigo 5.° da Directiva "privacidade das comunicações electrónicas", o tratamento dos dados pessoais com a finalidade de conhecer o conteúdo e/ou os dados de tráfego referentes a comunicações privadas deve igualmente obedecer a vários requisitos previstos na Directiva "protecção de dados".

A Directiva "protecção de dados" prevê, nomeadamente, a obrigação de informar as pessoas sobre o processamento dos seus dados pessoais. Em especial, o artigo 10.° "*Informação em caso de recolha de dados junto da pessoa em causa*" impõe aos responsáveis pelo tratamento dos dados a obrigação de fornecer à pessoa cujos dados pessoais são recolhidos certas informações, incluindo a identidade do responsável pelo tratamento desses dados e os objectivos para que serão processados. Além disso, o n.º 1, alínea a), do artigo 6.° da Directiva "protecção de dados" prevê que os dados devem ser processados leal e licitamente, o que reforça a obrigação de os responsáveis pelo tratamento dos dados serem completamente transparentes em relação às condições de tratamento dos dados pessoais.

---

qualquer conteúdo criado pela Yahoo! ou apresentado à Yahoo!, incluindo, sem limitações, a infomação constante dos "Message Boards" Yahoo! ou nas outras partes do serviço. É aceite e consentido que a Yahoo! pode aceder, guardar e revelar a informação e conteúdos da sua conta, se a tal for obrigada por lei ou pela convicção, de boa fé, de que tal acesso, guarda ou revelação é razoavelmente necessário para: a) respeitar um processo judicial; b) aplicar as condições contratuais do serviço; c) responder a alegações de que qualquer conteúdo viola os direitos de terceiros; d) responder aos pedidos de apoio ao cliente; ou e) proteger os direitos, propriedade ou a segurança pessoal da Yahoo!, dos seus utilizadores e do público.

Quanto à filtragem com finalidade de detectar vírus e *spam*, o Grupo de trabalho do artigo 29.º considera adequada a prática dos ESP que consiste em informar os subscritores no âmbito das condições contratuais do serviço.

Além disso, os ESP devem igualmente respeitar o artigo 4.° da Directiva "privacidade das comunicações electrónicas", que exige que os prestadores de serviços de comunicações electrónicas publicamente disponíveis informem os subscritores dos riscos específicos de falhas na segurança da rede. Quando as soluções possíveis para os problemas de segurança se encontrarem fora do âmbito de acção dos prestadores de serviços, estes devem informar os utilizadores e subscritores das medidas que podem tomar para proteger a segurança das suas comunicações.

V. OUTROS SERVIÇOS CONEXOS DO CORREIO ELECTRÓNICO

O Grupo de trabalho do artigo 29.º nota o desenvolvimento de um novo tipo de produtos de software e de serviços, como por exemplo o chamado serviço *"Did they read it?"*, que visa detectar a abertura de correio electrónico.

Este tipo de serviço permite aos subscritores saber se uma mensagem por si enviada a) foi lida pelo destinatário(s), b) quando foi lida, c) quantas vezes foi lida (ou pelo menos aberta), d) se foi reencaminhada e e) para que servidor de correio electrónico, incluindo a sua localização. Finalmente, permite igualmente saber o programa de navegação na Web e o sistema operativo utilizado pelo destinatário do correio electrónico.

O processamento de dados é executado secretamente, ou seja, não é fornecida qualquer informação sobre o processamento dos dados aos destinatários das mensagens cujos dados são recolhidos. Além disso, os destinatários das mensagens não têm a possibilidade de aceitar ou recusar a referida recolha de informação. Em suma, ao contrário dos sistemas de reconhecimento de mensagens clássicos, com estes novos produtos o destinatário não tem a possibilidade de aceitar ou recusar o envio da informação para o utilizador do programa.

O Grupo de trabalho do artigo 29.º manifesta a sua firme oposição a esta forma de processamento, porque os dados pessoais sobre o comportamento dos destinatários são registados e transmitidos sem o seu consentimento inequívoco. Este processamento, executado secretamente, é contrário aos princípios de protecção dos dados que exigem a lealdade e transparência na recolha dos dados pessoais prevista pelo artigo 10.° da Directiva "protecção de dados".

Para se poder proceder ao processamento dos dados do destinatário de uma mensagem de correio electrónico no sentido de saber se a mensagem foi lida e quando e se foi reenviada, é necessário o seu consentimento inequívoco. Não existe qualquer outra justificação legal para este processamento. Por conseguinte, o processamento de dados efectuado secretamente é contrário aos princípios de protecção dos dados que, nos termos do artigo 7° da Directiva "protecção de dados", exigem claramente um consentimento.

VI. CONCLUSÃO

Dada a incerteza relativa à compatibilidade da filtragem de mensagens de correio electrónico e o facto de as partes interessadas terem pedido orientações, o Grupo de trabalho considerou útil publicar o presente parecer.

O Grupo de trabalho do artigo 29.º incentiva os prestadores de serviços de correio electrónico a terem em conta as orientações e recomendações contidas no presente parecer na forma como prestam os seus serviços. Além disso, como elemento da sua política de promoção das tecnologias que incorporam os requisitos de protecção de dados e de privacidade na concepção das infra-estruturas e dos sistemas de informação, incluindo o equipamento terminal, o Grupo de trabalho do artigo 29.º gostaria de incentivar os criadores de programas de correio electrónico a conceber e desenvolver sistemas que assegurem a privacidade de forma a reduzir ao mínimo o processamento dos dados pessoais, limitando-o ao que seja absolutamente necessário e proporcional para alcançar os objectivos desse processamento.

Feito em Bruxelas, em 21 de Fevereiro de 2006

Pelo Grupo de trabalho

O Presidente
Peter Schaar