I

(Resoluções, recomendações e pareceres)

PARECERES

AUTORIDADE EUROPEIA PARA A PROTEÇÃO DE DADOS

Parecer da Autoridade Europeia para a Proteção de Dados sobre a neutralidade da Internet, a gestão do tráfego e a proteção da privacidade e dos dados pessoais

(2012/C 34/01)

A AUTORIDADE EUROPEIA PARA A PROTEÇÃO DE DADOS,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia e, nomeadamente, o artigo 16.º;

Tendo em conta a Carta dos Direitos Fundamentais da União Europeia e, nomeadamente, os artigos 7.º e 8.º;

Tendo em conta a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados ([1]);

Tendo em conta o Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados ([2]), nomeadamente o artigo 41.º, n.º 2;

Tendo em conta a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas ([3]),

ADOTOU O SEGUINTE PARECER:

I. **INTRODUÇÃO**

I.1. **Contexto**

1. Em 19 de abril de 2011, a Comissão adotou uma Comunicação sobre abertura e neutralidade da Internet na Europa ([4]).

2. O presente parecer deve ser entendido como a reação da AEPD a esta comunicação e visa contribuir para o debate político atualmente em curso na UE sobre a neutralidade da Internet, nomeadamente sobre os aspectos relacionados com a proteção de dados e a privacidade.

([1]) JO L 281 de 23.11.1995, p. 31, a Diretiva Proteção de Dados.
([2]) JO L 8 de 12.1.2001, p. 1, o Regulamento relativo à proteção de dados.
([3]) JO L 201 de 31.7.2002, p. 37, alterado pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009 (ver nota de rodapé n.º 15), a Diretiva ePrivacidade.
([4]) COM(2011) 222 final.

3. O parecer baseia-se na resposta [5] da AEPD à consulta pública da Comissão sobre a abertura e a neutralidade da Internet na Europa, que precedeu a comunicação da Comissão. A AEPD teve igualmente em conta o recente projeto de conclusões do Conselho sobre a neutralidade da Internet [6].

I.2. **O conceito de neutralidade da Internet**

4. A neutralidade da Internet diz respeito a um debate em curso sobre a questão de os fornecedores de serviços Internet [«FSI [7]»] serem autorizados a limitar, filtrar ou bloquear o acesso à Internet ou afetar o seu desempenho por outro meio. O conceito de neutralidade da Internet baseia-se no pressuposto de que a informação na Internet deve ser transmitida de forma imparcial, independentemente do conteúdo, destino ou origem, e de que os utilizadores devem poder decidir que aplicações, serviços e *hardware* pretendem utilizar. Tal significa que os FSI não podem, por sua livre iniciativa, dar prioridade ou abrandar o acesso a determinados serviços ou aplicações como, por exemplo, *Peer-to-Peer* («P2P»), etc. [8].

5. A filtragem, o bloqueio e a inspeção do tráfego de rede suscita questões importantes, frequentemente excluídas ou marginalizadas, no que respeita à confidencialidade das comunicações e ao respeito pela privacidade das pessoas singulares e pelos seus dados pessoais quando utilizam a Internet. Por exemplo, determinadas técnicas de inspeção envolvem a monitorização de conteúdos de comunicações, sítios Internet visitados, correio eletrónico enviado e recebido, a hora em que ocorreram estas atividades, etc., o que permite a filtragem das comunicações.

6. Através da inspeção dos dados das comunicações, os FSI podem violar a confidencialidade das comunicações, a qual constitui um direito fundamental garantido pelo artigo 8.º da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (a «CEDH») e pelos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia (a «Carta»). A confidencialidade está ainda protegida no direito derivado da UE, nomeadamente o artigo 5.º da Diretiva ePrivacidade.

I.3. **Âmbito e estrutura do parecer**

7. A AEPD considera que um debate político sério sobre a neutralidade da Internet deve abordar a confidencialidade das comunicações, bem como outras implicações em matéria de privacidade e proteção de dados.

8. O presente parecer contribui para o debate em curso na União Europeia. Visa três aspetos:

— Destaca a relevância da privacidade e da proteção de dados nos atuais debates sobre a neutralidade da Internet. Mais especificamente, salienta a necessidade de respeitar as normas em vigor em matéria de confidencialidade das comunicações. Apenas devem ser permitidas as práticas que respeitem essas normas;

— A neutralidade da Internet está associada a possibilidades tecnológicas relativamente recentes e existe pouca experiência quanto à aplicação do quadro jurídico. Por conseguinte, o presente parecer fornece orientações sobre a forma como os FSI devem aplicar e respeitar o quadro jurídico em matéria de proteção de dados caso executem atividades de filtragem, bloqueio e inspeção do tráfego de rede. Essas orientações poderão ser úteis para os FSI e para as autoridades responsáveis pela aplicação do quadro jurídico;

— No âmbito da proteção de dados e da privacidade, o presente parecer identifica domínios que necessitam de especial atenção e podem exigir uma intervenção a nível europeu. Este aspecto é especialmente importante à luz do debate em curso a nível europeu e das medidas políticas que a Comissão poderá lançar neste contexto.

---

[5] A resposta da AEPD salienta a importância de ter em conta as questões em matéria de proteção de dados e privacidade em conjunto com outros direitos e valores existentes. A resposta está disponível em: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-10-06_EC_Consultation_Open_Internet_EN.pdf

[6] Disponível em: http://register.consilium.europa.eu/pdf/en/11/st14/st14209.en11.pdf

[7] Inclui a prestação de serviços de acesso fixo e móvel à Internet.

[8] Embora o princípio não se aplique aos FSI que limitam a velocidade ou o volume de informação que um assinante pode enviar ou receber através de subscrições com limites de largura de banda ou de volume. Por conseguinte, ao abrigo de um princípio de neutralidade, os FSI poderiam ainda oferecer assinaturas de acesso à Internet com limitação de acesso baseada em critérios como a velocidade ou o volume, desde que essa limitação não estabeleça qualquer discriminação a favor ou contra conteúdos específicos.

9. A AEPD está ciente de que a neutralidade da Internet suscita outras questões, pormenorizadas adiante, como as relacionadas com o acesso à informação. Existem questões que apenas são abordadas porque estão relacionadas ou têm impacto sobre a proteção de dados e a privacidade.

10. O parecer está estruturado como segue. A Secção II apresenta uma breve descrição das práticas dos FSI em matéria de filtragem. A Secção III apresenta uma perspetiva do quadro jurídico da União Europeia em matéria de neutralidade da Internet. A Secção IV apresenta uma descrição técnica e uma avaliação das implicações sobre a privacidade, dependendo da técnica utilizada. A Secção V analisa os pormenores práticos relativos à aplicação do atual quadro jurídico europeu em matéria de privacidade e proteção de dados. Com base na análise, a Secção VI contém sugestões para futuras medidas e identifica os domínios em que poderá ser necessário clarificar e melhorar o quadro jurídico. A Secção VII contém as conclusões.

II. **NEUTRALIDADE DA INTERNET E POLÍTICAS DE GESTÃO DO TRÁFEGO**

Reforço da utilização de políticas de gestão do tráfego

11. Tradicionalmente, os FSI executavam atividades de monitorização e condicionamento do tráfego de rede apenas em circunstâncias limitadas. Por exemplo, os FSI aplicavam técnicas de inspeção e restringiam fluxos de informação para preservar a segurança da rede, nomeadamente para combater vírus. Por conseguinte, de uma forma geral, a Internet cresceu mantendo simultaneamente um elevado grau de neutralidade.

12. Nos últimos anos, no entanto, alguns FSI demonstraram interesse em inspecionar o tráfego de rede a fim de diferenciar e aplicar políticas distintas, por exemplo, para bloquear serviços específicos ou dar acesso preferencial a outros. Estas práticas são por vezes mencionadas como «políticas de gestão do tráfego» ([9]).

13. Os motivos que levam os FSI a inspecionar e diferenciar o tráfego são muito diversos. Por exemplo, as políticas de gestão de tráfego podem ajudar os FSI a gerir o tráfego durante períodos de elevado congestionamento, através da atribuição de prioridade a determinado tráfego sensível ao tempo, como o fluxo vídeo, e o abrandamento de outros tipos de tráfego que podem ser menos sensíveis ao tempo, como os serviços P2P ([10]). Além disso, a gestão do tráfego pode constituir um meio para os FSI obterem um potencial fluxo de receitas com origem em fontes diferentes. Por um lado, os FSI podem, por exemplo, cobrar taxas aos fornecedores de conteúdos cujos serviços exigem a utilização de maior largura de banda, dando-lhes prioridade (e, por consequência, velocidade). Tal significaria que o acesso a um determinado serviço, por exemplo, um serviço de fornecimento de vídeos a pedido, seria mais rápido do que o acesso a um serviço idêntico que não tenha contratado uma transmissão de alta velocidade. Também seria possível obter receitas de assinantes interessados em pagar taxas mais elevadas (ou mais baixas) por determinados tipos de assinaturas diferenciadas. Por exemplo, uma assinatura sem acesso a um serviço P2P poderia ser mais barata do que uma assinatura com acesso ilimitado.

14. Além dos motivos do próprio FSI para a utilização de políticas de gestão do tráfego, outras partes poderão igualmente estar interessadas em que os FSI utilizem políticas de gestão do tráfego. Se os FSI efetuarem a gestão das suas redes e executarem atividades de inspeção dos conteúdos que atravessam os seus equipamentos, é provável que aumentem a sua capacidade para detetar alegadas utilizações ilegais, por exemplo, violação de direitos de autor ou utilização de pornografia.

([9]) Ver, por exemplo, o relatório da OFCOM intitulado «Site blocking to reduce online copyright infringement» (Bloqueio de *sites* para combater a violação de direitos de autor em linha), aprovado em 27 de maio de 2011, disponível em: http://www.culture.gov.uk/images/publications/Ofcom_Site-Blocking-_report_with_redactions_vs2.pdf: Alguns FSI já implementam sistemas de inspeção de pacotes nas suas redes para fins de gestão de tráfego e outros; assim, assumimos que pode ser implementado, embora envolva um elevado grau de complexidade e custos para os FSI que ainda não executam esses serviços. Poderá acontecer que, a curto ou médio prazo, a inspeção de pacotes de dados apenas possa ser implementada pelos FSI de grande dimensão, tendo em conta o investimento de capital necessário.

([10]) A qualidade das aplicações em tempo real, como o fluxo vídeo, depende, entre outros fatores, da latência, ou seja, do atraso devido, por exemplo, a congestionamento da rede.

Outros interesses em causa, incluindo a proteção de dados e a privacidade

15. Esta tendência deu origem a um debate sobre a legitimidade deste tipo de práticas e, mais especificamente, sobre se a legislação deve prever outras obrigações específicas em matéria de neutralidade da Internet.

16. O reforço da utilização de políticas de gestão do tráfego por parte dos FSI poderia limitar o acesso à informação. Se este comportamento se tornasse prática comum e não fosse possível (ou tivesse custos muito elevados) os utilizadores terem total acesso à Internet da forma que conhecemos, tal prejudicaria o acesso à informação e a capacidade de os utilizadores enviarem e receberem os conteúdos que pretendem utilizando as aplicações ou os serviços da sua preferência. Um princípio juridicamente vinculativo em matéria de neutralidade da Internet poderia evitar este problema.

17. Essa situação confronta a AEPD com as implicações em matéria de proteção de dados e de privacidade quando os FSI executam a gestão do tráfego. Mais especificamente:

— Quando os FSI processam dados de tráfego com a finalidade única de encaminhar o fluxo de informação do remetente para o destinatário, executam normalmente um tratamento limitado de dados pessoais ([11]). Da mesma forma que os serviços postais processam as informações incluídas no envelope de uma carta, os FSI processam as informações necessárias para encaminhar as comunicações para o destinatário. Este tratamento não infringe os requisitos legais de proteção de dados, privacidade e confidencialidade das comunicações;

— No entanto, quando os FSI inspecionam dados de comunicações a fim de diferenciar cada fluxo de comunicação e aplicar políticas específicas, que podem ser desfavoráveis para as pessoas singulares, as implicações são mais significativas. Dependendo das circunstâncias de cada caso e do tipo de análise realizada, o tratamento pode ser muito invasivo para a privacidade e os dados pessoais das pessoas singulares. Esta situação é mais óbvia nos casos em que as políticas de gestão revelam o conteúdo das comunicações de pessoas singulares na Internet, incluindo mensagens de correio eletrónico enviadas e recebidas, sítios Internet visitados, ficheiros descarregados ou carregados, etc.

III. **PERSPETIVA DO QUADRO JURÍDICO DA UE EM MATÉRIA DE NEUTRALIDADE DA INTERNET E POLÍTICAS FUTURAS**

III.1. **O quadro jurídico em resumo**

18. Até 2009, os instrumentos legislativos da UE não continham disposições que proibissem explicitamente os FSI de executar atividades de filtragem ou bloqueio ou de cobrar custos adicionais aos assinantes pelo acesso aos serviços. Ao mesmo tempo, não continham disposições que reconhecessem explicitamente esta prática. A situação era, em certa medida, incerta.

19. O pacote de reforma das telecomunicações, de 2009, alterou esta situação ao incluir disposições que favorecem a abertura da Internet. Por exemplo, o artigo 8.º, n.º 4, da Diretiva relativa a um quadro regulamentar comum para as redes e serviços de comunicações electrónicas («diretiva-quadro») estabelece que as autoridades reguladoras devem fomentar a capacidade de os utilizadores finais acederem aos conteúdos, aplicações ou serviços à sua escolha ([12]). Esta disposição aplica-se à rede como um todo e não individualmente aos fornecedores. O recente projecto de conclusões do Conselho salientou igualmente a necessidade de manter a abertura da Internet ([13]).

([11]) São excluídas as operações que visam aumentar a segurança da rede e detetar tráfego prejudicial, bem como as operações necessárias para facturação e interligação. São igualmente excluídas as obrigações que decorrem da Diretiva relativa à conservação de dados, Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE (JO L 105 de 13.4.2006, p. 54) («Diretiva relativa à conservação de dados»).

([12]) Diretiva 2002/21/CE do Parlamento Europeu e do Conselho de 7 de março de 2002, relativa a um quadro regulamentar para as redes e serviços de comunicações eletrónicas, alterada pela Diretiva 2009/140/CE e pelo Regulamento (CE) n.º 544/2009 (JO L 337 de 18.12.2009, p. 37).

([13]) Ver o ponto 3(e), onde o Conselho reconhece a necessidade de manter a abertura da Internet e, ao mesmo tempo, assegurar que continua a proporcionar serviços de alta qualidade num quadro que promove e respeita direitos fundamentais, como a liberdade de expressão e a liberdade de atividade comercial, bem como o ponto 8(d), que convida os Estados-Membros a promoverem o caráter aberto e a neutralidade da Internet como objetivo das suas políticas.

20. A Diretiva relativa ao serviço universal ([14]) contém obrigações mais concretas. Os artigos 20.º e 21.º estabelecem requisitos de transparência no que respeita às limitações de acesso e/ou de utilização de serviços e aplicações. A diretiva estabelece igualmente níveis de qualidade mínima de serviço.

21. No que respeita às práticas dos FSI que implicam a inspeção das comunicações das pessoas singulares, o considerando 28 da diretiva que altera a Diretiva relativa ao serviço universal e a Diretiva ePrivacidade ([15]) salienta que «em função da tecnologia utilizada e do tipo de limitação, essas limitações poderão exigir o consentimento do utilizador» nos termos da Diretiva ePrivacidade. Assim, o considerando 28 relembra a necessidade de consentimento, em conformidade com o artigo 5.º, n.º 1, da Diretiva ePrivacidade, no que respeita a quaisquer limitações baseadas na monitorização das comunicações. A Secção IV adiante analisa a aplicação do artigo 5.º, n.º 1, e o quadro jurídico global em matéria de proteção de dados e privacidade.

22. Por último, o artigo 22.º, n.º 3, da Diretiva relativa ao serviço universal confere às autoridades reguladoras nacionais poderes para, se necessário, impor aos FSI requisitos de qualidade mínima de serviço, a fim de evitar a degradação dos serviços e a obstrução ou abrandamento do tráfego nas redes públicas.

23. Tal significa que, a nível da UE, existe uma clara vontade de assegurar uma Internet aberta (ver o artigo 8.º, n.º 4, da diretiva-quadro). No entanto, este objetivo de política, aplicável à Internet como um todo, não está diretamente associado a proibições ou obrigações dos FSI individualmente. Por outras palavras, um FSI pode aplicar políticas de gestão de tráfego que excluam o acesso a determinadas aplicações, desde que os utilizadores sejam informados de forma completa e expressem o seu consentimento de forma livre, específica e inequívoca.

24. Esta situação pode variar em função do Estado-Membro. Em alguns Estados-Membros, os FSI podem, em condições específicas, aplicar políticas de gestão de tráfego, por exemplo, para bloquear aplicações como VoIP (como parte de uma assinatura mais barata da Internet), desde que as pessoas singulares tenham dado o seu consentimento informado, livre, específico e inequívoco. Outros Estados-Membros optaram por reforçar o princípio da neutralidade da Internet. Por exemplo, em julho de 2011, o Parlamento holandês aprovou uma lei que, de uma forma geral, proíbe os fornecedores de obstruírem ou abrandarem aplicações ou serviços na Internet (por exemplo, VoIP), a menos que tal seja necessário para minimizar os efeitos de congestionamento, por motivos de integridade ou de segurança, para combater as comunicações não solicitadas ou em cumprimento de uma ordem judicial ([16]).

III.2. **Comunicação sobre a neutralidade da Internet**

25. Na sua comunicação sobre a neutralidade da Internet ([17]), a Comissão Europeia concluiu que a situação em matéria de neutralidade da Internet deve ser objeto de acompanhamento e de uma análise mais profunda. A sua política tem sido a de aguardar a evolução da situação («esperar para ver») antes de ponderar a adoção de outras medidas regulamentares.

([14]) Diretiva 2002/22/CE alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas e o Regulamento (CE) n.º 2006/2004 relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor. (JO L 337 de 18.12.2009, p.11). Ver igualmente o artigo 1.º, n.º 3, que afirma que a diretiva não exige nem proíbe os FSI de limitarem aos utilizadores finais o acesso e/ou a utilização de serviços e aplicações, sempre que tal seja permitido pela legislação nacional e em conformidade com o direito comunitário, mas prevê, ao invés, a obrigação de prestação de informações relativas a tais condições.

([15]) Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, a Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas e o Regulamento (CE) n.º 2006/2004 relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor.

([16]) O texto original holandês pode ser consultado em: https://zoek.officielebekendmakingen.nl/kst-32549-A.html Os motivos apontados pela imprensa para essa opção de política não referiam aspetos relativos à proteção de dados e à privacidade, mas sim a garantia de que os utilizadores não são impedidos ou têm acesso limitado à informação. Deste modo, esta alteração parece ter sido motivada por questões relacionadas com o acesso à informação.

([17]) Ver nota de pé-de-página 4.

26. A comunicação da Comissão reconheceu que quaisquer outras medidas regulamentares deveriam ser objeto de uma análise profunda dos aspetos relacionados com a proteção de dados e a privacidade. O projeto de conclusões do Conselho sublinha as questões em matéria de proteção de dados e privacidade que estão em causa ([18]).

27. A questão a analisar, do ponto de vista da proteção de dados e da privacidade, é se esta política de aguardar a evolução da situação é suficiente. Embora o quadro jurídico relativo à proteção de dados e à privacidade contemple atualmente algumas proteções, em especial através do princípio da confidencialidade das comunicações, parece ser necessário efetuar um maior controlo do nível de conformidade e emitir orientações sobre vários aspectos que não são particularmente claros. Além disso, devem ser propostas ideias para clarificar e melhorar o quadro jurídico, à luz dos desenvolvimentos tecnológicos. Se a monitorização revelar que o mercado está a evoluir para uma inspeção massiva e em tempo real das comunicações e que existem problemas relacionados com a conformidade com o quadro jurídico, serão necessárias medidas legislativas. A este respeito, são apresentadas sugestões concretas na Secção VI.

IV. **ASPETOS TÉCNICOS E RESPETIVAS IMPLICAÇÕES EM MATÉRIA DE PRIVACIDADE E PROTEÇÃO DE DADOS**

28. Antes de abordar o tema de forma mais profunda, é importante conhecer melhor as técnicas de inspeção que os FSI podem utilizar na gestão do tráfego e a forma como essas técnicas podem afetar o princípio da neutralidade da Internet. As implicações em matéria de privacidade e proteção de dados decorrentes dessas técnicas variam substancialmente, dependendo da(s) técnica(s) utilizadas(s). O conhecimento destes aspetos técnicos é necessário para compreender e aplicar adequadamente o quadro jurídico em matéria de proteção de dados descrito na Secção V. Todavia, deve notar-se que se trata de um domínio complexo e em constante evolução. Por conseguinte, a descrição seguinte não pretende ser exaustiva e totalmente atualizada, mas apenas fornecer as informações técnicas que são indispensáveis para compreender a argumentação jurídica.

IV.1. **Transmissão de informação através da Internet: noções básicas**

29. Quando um utilizador transmite uma comunicação através da Internet, a informação transmitida é dividida em pacotes. Esses pacotes são transmitidos do remetente para o destinatário através da Internet. Cada pacote contém, nomeadamente, informações sobre a origem e o destino. Além disso, os FSI podem incorporar esses pacotes em protocolos e camadas adicionais ([19]), que serão utilizados para gerir os diferentes fluxos de tráfego nas suas redes.

30. Voltando à analogia da carta de correio, a utilização de um protocolo de transmissão em rede é equivalente à inclusão do conteúdo de uma carta de correio num sobrescrito com um endereço de destino que é lido e entregue pelos serviços postais. Os serviços postais podem utilizar protocolos adicionais nos seus trânsitos internos a fim de gerir todos os sobrescritos a entregar, tendo como objetivo que cada sobrescrito seja entregue no seu destinatário, conforme pretendido originalmente pelo remetente. Utilizando esta analogia, cada pacote é constituído por duas partes, o *payload* de IP e o cabeçalho IP. O *payload* de IP contém o conteúdo da comunicação e é equivalente à carta. Contém informação destinada exclusivamente ao destinatário. A segunda parte do pacote, o cabeçalho IP, inclui, entre outras informações, os endereços do destinatário e do remetente e é equivalente ao sobrescrito. O cabeçalho IP permite aos FSI e outros intermediários encaminhar o *payload* desde o endereço de origem até ao endereço de destino.

31. Os FSI e outros intermediários asseguram que os pacotes IP viajam ao longo da rede através de nós que lêem a informação do cabeçalho IP e a verificam em tabelas de encaminhamento e, em seguida, encaminham os pacotes para o nó seguinte no percurso até ao destino. Este processo é executado em toda a rede utilizando uma abordagem «best effort memoryless» (melhor esforço sem memória),

([18]) Ver o ponto 4(e), onde o Conselho sublinha a existência de algumas preocupações, sobretudo por parte dos consumidores e das autoridades de proteção de dados, no que respeita à proteção de dados pessoais.

([19]) Tal como descrito na Secção IV.2, esses protocolos codificam a informação que está a ser transmitida «de extremo a extremo» de uma forma acordada que permite às partes envolvidas na comunicação entenderem-se mutuamente, por exemplo, HTTP, FTP, etc.

uma vez que todos os pacotes que chegam a um nó são tratados de uma forma neutra. Depois de serem encaminhados para o nó seguinte, não é necessário manter as informações no encaminhador (*router*) ([20]).

IV.2. **Técnicas de inspeção**

32. Conforme demonstrado acima, os FSI lêem os cabeçalhos IP com a finalidade de os encaminhar para o seu destino. No entanto, tal como salientado acima, a análise do tráfego (que envolve cabeçalhos IP e *payloads* de IP) pode ser executada para outros fins e com diferentes tipos de tecnologias. Podem, por exemplo, ser utilizadas técnicas de abrandamento de determinadas aplicações usadas pelos utilizadores, como P2P, ou de aumento da velocidade do tráfego para determinados serviços, como os serviços de vídeo a pedido para assinantes de serviços *premium*. Embora, do ponto de vista *técnico*, todas as técnicas de inspeção executem inspeção de pacotes, estas envolvem diferentes níveis de intrusão. Existem duas categorias principais de técnicas de inspeção. Uma é baseada apenas no cabeçalho IP, a outra baseia-se também no *payload* de IP.

Técnicas baseadas na informação do cabeçalho IP. A inspeção do cabeçalho de um pacote IP revela alguns campos que podem permitir aos FSI aplicar várias políticas específicas para gerir o tráfego. Estas técnicas baseadas apenas na inspeção dos cabeçalhos IP processam dados que, em princípio, se destinam ao encaminhamento da informação para uma finalidade diferente (por exemplo, diferenciar tráfego). Ao analisar o endereço do IP de origem, o FSI pode associá-lo a um assinante específico e aplicar políticas específicas como, por exemplo, encaminhar o pacote através de uma ligação mais rápida ou mais lenta. Ao analisar o endereço IP de destino, o FSI pode igualmente aplicar políticas específicas como, por exemplo, bloquear ou filtrar o acesso a sítios Internet específicos.

Técnicas baseadas numa inspeção mais profunda. A inspeção profunda de pacotes permite ao FSI aceder a informação dirigidas apenas ao destinatário da comunicação. Voltando novamente ao exemplo do serviço postal, esta abordagem é equivalente a abrir o sobrescrito e ler a carta contida no seu interior para realizar uma análise do conteúdo da comunicação (encapsulada nos pacotes IP) a fim de aplicar uma política de rede específica. As duas formas existentes de executar a inspeção apresentam, cada uma, diferentes ameaças para a pessoa em causa.

— *Inspeção profunda de pacotes com base na análise dos protocolos e em registos estatísticos*. Além do protocolo IP, que se destina a permitir a transmissão dos dados através da Internet, existem protocolos adicionais que codificam a informação transmitida de uma forma acordada (transporte, sessão, apresentação e aplicação, etc.). O objetivo desses protocolos é o de assegurar que as partes envolvidas na comunicação podem entender-se mutuamente. Por exemplo, existem protocolos que estão associados à navegação na Internet ([21]), outros que se destinam à transferência de ficheiros ([22]), etc. Por conseguinte, as técnicas de inspeção baseadas na inspeção dos protocolos, combinadas com análise estatística, visam encontrar padrões específicos ou impressões digitais que determinam quais os protocolos que estão presentes ([23]). Estas técnicas de inspeção permitem aos FSI entender o tipo de comunicação (correio eletrónico, navegação na Internet, carregamento de ficheiros) e, em alguns casos, identificar a aplicação ou o serviço específico utilizado, como é o caso de algumas comunicações VoIP nas quais os protocolos utilizados são muito específicos para um determinado prestador ou fornecedor de serviço. O conhecimento do tipo de comunicação pode, por si só, permitir aos FSI aplicarem políticas de gestão de tráfego concretas, por exemplo, para bloquear tráfego na Internet. Pode ainda constituir o primeiro passo para permitir ao FSI executar uma análise mais profunda que exija acesso total aos metadados e ao conteúdo da comunicação.

([20]) No entanto, os equipamentos de rede da Internet utilizam protocolos de encaminhamento que registam a atividade, processam estatísticas de tráfego e trocam informações com outros equipamentos de rede a fim de encaminhar os pacotes IP através do caminho mais eficiente. Por exemplo, se uma ligação estiver congestionada ou danificada e um encaminhador receber esta informação, atualizará a sua tabela de encaminhamento com uma alternativa que não utilize essa ligação. Importa ainda referir a recolha e o tratamento que, em alguns casos, podem ser efetuados para efeitos de faturação ou mesmo em conformidade com os requisitos da diretiva relativa à conservação de dados.

([21]) HTTP — Protocolo de transferência de hipertexto (*Hypertext transfer protocol*) — ou HTML — Linguagem de marcação de hipertexto (*Hypertext Markup Language*).

([22]) FTP — Protocolo de transferência de ficheiros (*File transfer protocol*).

([23]) Existem várias formas de identificar os protocolos utilizados. É possível procurar em campos específicos nos protocolos internos, por exemplo, para identificar as portas utilizadas para estabelecer a comunicação. É também possível inferir uma caraterização estatística de um fluxo de comunicação a partir da análise de alguns campos específicos e da correlação dos protocolos utilizados simultaneamente entre os dois endereços IP.

— *Inspeção profunda de pacotes com base na análise do conteúdo da comunicação*. Por último, é igualmente possível inspecionar os metadados ([24]) e o próprio conteúdo da comunicação. Esta técnica consiste na interceção de todos os pacotes IP que fazem parte do fluxo de comunicação original, de modo a que o conteúdo original da comunicação possa ser totalmente reconstruído e analisado. Por exemplo, para detetar conteúdos nocivos ou ilegais como vírus, pornografia infantil, etc., é necessário reconstruir o próprio conteúdo para o poder analisar. Deve notar-se que, por vezes, a comunicação pode ser encriptada explicitamente «de extremo a extremo» pelas partes envolvidas e que esta prática impedirá os FSI de analisar o conteúdo da comunicação.

IV.3. **Implicações em matéria de privacidade e proteção de dados**

33. As técnicas de inspeção baseadas nos cabeçalhos IP e, mais especificamente, as baseadas na inspeção de pacotes envolvem a monitorização e filtragem desses dados e têm sérias implicações em termos de privacidade e proteção de dados. Podem ainda estar em conflito com o direito à confidencialidade das comunicações.

34. A análise das comunicações das pessoas singulares, por si só, tem sérias implicações em termos de privacidade e proteção de dados. Contudo, o problema é mais abrangente, uma vez que, dependendo dos efeitos pretendidos com a monitorização e a interceção, as implicações em termos de privacidade podem aumentar. Na verdade, inspecionar as comunicações apenas para assegurar que o sistema funciona corretamente, por exemplo, não é a mesma coisa que fazê-lo para aplicar políticas que podem ter impacto sobre as pessoas singulares. Se as políticas de tráfego e de seleção apenas pretenderem evitar o congestionamento da rede, não existirão normalmente implicações significativas para a privacidade das pessoas singulares. No entanto, as políticas de gestão de tráfego podem visar o bloqueio da informação de alguns conteúdos ou influenciar a comunicação, por exemplo através de publicidade comportamental. Nesses casos, os efeitos são mais invasivos. A preocupação agrava-se caso se conclua que este tipo de informação seria recolhido não apenas para um pequeno grupo de pessoas mas antes numa base generalizada, para todos os clientes dos FSI ([25]). Se todos os FSI adotarem técnicas de filtragem, tal pode conduzir a uma monitorização generalizada da utilização da Internet. Por outro lado, se atentarmos no tipo de informação processada, os riscos para a privacidade são obviamente elevados, uma vez que muita da informação recolhida pode ser muito sensível e, após a recolha, está disponível para os FSI e todos aqueles que procuram informações a partir destes. Além disso, a informação pode igualmente ser muito valiosa em termos comerciais. Por si só, tal representa um elevado risco de desvio de funções em que as finalidades iniciais podem facilmente evoluir para a exploração comercial ou outra da informação recolhida.

35. A aplicação correta de técnicas de monitorização, inspeção e filtragem deve ser efetuada em conformidade com as garantias aplicáveis em matéria de proteção de dados e privacidade, que estabelecem limites ao que pode ser feito e em que circunstâncias. A seguir, é apresentada uma descrição das garantias aplicáveis no âmbito do atual quadro jurídico europeu em matéria de proteção de dados e privacidade.

V. **APLICAÇÃO DO QUADRO JURÍDICO DA UE EM MATÉRIA DE PRIVACIDADE E PROTEÇÃO DE DADOS**

36. O quadro jurídico europeu de proteção de dados é neutro do ponto de vista tecnológico; como tal, não regulamenta técnicas de inspeção específicas como as descritas acima. A Diretiva ePrivacidade regulamenta a privacidade na prestação de serviços de comunicações electrónicas em redes públicas

([24]) Cada protocolo possui campos específicos no cabeçalho que fornecem informações informais suplementares sobre a comunicação que está a ser transmitida. Por conseguinte, o conteúdo desses campos pode ser designado como os metadados da comunicação. Um exemplo desses campos é o número de porta utilizado: se, por exemplo, for o número 80, é provável que o tipo de comunicação seja navegação na Internet.

([25]) Obviamente, as capacidades de monitorização não são exclusivas dos FSI. Os fornecedores de redes de publicidade são também capazes, através da utilização de testemunhos de conexão de terceiros, de monitorizar utilizadores em sítios Internet. Ver, por exemplo, um artigo académico recente que demonstra que a Google está presente em 97 dos 100 principais sítios Internet, o que significa que a Google pode monitorizar os utilizadores que não tenham realizado a auto-exclusão de testemunhos de conexão de terceiros quando navegam nesses sítios Internet populares. Ver: *Ayenson, Mika, Wambach, Dietrich James, Soltani, Ashkan, Good, Nathan and Hoofnagle, Chris Jay, Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning* (29 de julho de 2011). Disponível no sítio Internet da SSRN: http://ssrn.com/abstract=1898390 A monitorização de utilizadores através de testemunhos de conexão de terceiros foi abordada pelo Grupo de Trabalho do Artigo 29.º para a proteção de dados. Ver o Parecer 2/2010 sobre publicidade comportamental em linha, adotado em 22 de junho de 2010 (WP 171).

(normalmente acesso à Internet e telefonia) ([26]) e a Diretiva Proteção de Dados regulamenta o tratamento de dados em geral. No seu conjunto, este quadro jurídico estabelece obrigações diferentes que são aplicáveis aos FSI que tratam e monitorizam o tráfego e os dados das comunicações.

V.1. **Fundamentos jurídicos para o tratamento de dados de tráfego e de conteúdo**

37. Nos termos da legislação relativa à proteção de dados, o tratamento de dados pessoais como, no caso presente, o tratamento de dados de tráfego e de comunicações, exige uma fundamentação jurídica adequada. Além deste requisito geral, podem ser aplicáveis requisitos específicos em determinados casos.

38. Neste caso, o tipo de dados pessoais que são tratados pelos FSI refere-se aos dados de tráfego e ao conteúdo das comunicações. O conteúdo das comunicações e os dados de tráfego estão ambos protegidos pelo direito à confidencialidade da correspondência, que é garantido pelo artigo 8.º da CEDH e pelos artigos 7.º e 8.º da Carta. Mais especificamente, o artigo 5.º, n.º 1, da Diretiva ePrivacidade, com o título «confidencialidade das comunicações», estabelece que *os Estados-Membros garantirão […] a confidencialidade das comunicações e respetivos dados de tráfego realizadas através de redes públicas e de serviços de comunicações electrónicas publicamente disponíveis*. Ao mesmo tempo, o artigo 5.º, n.º 1, da Diretiva ePrivacidade prevê que o tratamento de dados de tráfego e de conteúdo pelos FSI pode ser permitido, em circunstâncias específicas, com o consentimento dos utilizadores. Para isso, deve estabelecer-se uma *proibição de* «escuta, instalação de dispositivos de escuta, armazenamento ou outras formas de interceção ou vigilância de comunicações e dos respetivos dados de tráfego por pessoas que não os utilizadores, sem o consentimento dos utilizadores em causa, exceto quando legalmente autorizados a fazê-lo, de acordo com o disposto no n.º 1 do artigo 15.º». Este aspeto é desenvolvido adiante.

39. Além do consentimento dos utilizadores em causa, a Diretiva ePrivacidade prevê outros fundamentos que podem legitimar o tratamento de dados de tráfego e de comunicações por parte dos FSI. Os fundamentos jurídicos pertinentes para o tratamento de dados, neste caso, são: i) a prestação do serviço; ii) a garantia da segurança do serviço, e iii) a minimização do congestionamento. No ponto iv) são debatidos outros fundamentos possíveis para legitimar as políticas de gestão baseadas nos dados de tráfego ou de comunicações.

i) Fundamentos jurídicos para a prestação do serviço

40. Conforme demonstrado na Secção IV, os FSI processam a informação existente nos cabeçalhos IP com a finalidade de encaminhar cada pacote IP para o seu destino. O artigo 6.º, n.ºs 1 e 2, da Diretiva ePrivacidade, permite o tratamento de dados de tráfego com a finalidade de envio de uma comunicação. Assim, os FSI podem processar a informação que é necessária para a prestação do serviço.

ii) Fundamentos jurídicos para a garantia da segurança do serviço

41. Nos termos do artigo 4.º da Diretiva ePrivacidade, os FSI têm a obrigação geral de adoptar as medidas adequadas para garantir a segurança dos seus serviços. A prática da filtragem de vírus pode envolver o tratamento de cabeçalhos IP e de *payload* de IP. Tendo em conta que o artigo 4.º da Diretiva ePrivacidade determina que os FSI devem assegurar a segurança da rede, esta disposição legitima as técnicas de inspeção baseadas nos cabeçalhos IP e no conteúdo que visam estritamente atingir esse objetivo. Na prática, tal significa que, dentro dos limites estabelecidos pelo princípio da proporcionalidade (ver Secção V.3), os FSI podem executar atividades de monitorização e filtragem de dados de comunicações para combater vírus e garantir a segurança da rede ([27]).

([26]) O considerando 10 da Diretiva ePrivacidade tem a seguinte redação: «No setor das comunicações eletrónicas, é aplicável a Diretiva 95/46/CE, especialmente no que se refere a todas as questões relacionadas com a proteção dos direitos e liberdades fundamentais não abrangidos especificamente pelas disposições da presente diretiva, incluindo as obrigações que incumbem à entidade que exerce o controlo e os direitos das pessoas singulares». O considerando 17 é igualmente pertinente no que respeita ao consentimento da pessoa em causa: «Para efeitos da presente diretiva, o consentimento por parte do utilizador ou assinante, independentemente de este ser uma pessoa singular ou coletiva, deve ter a mesma acepção que o consentimento da pessoa a quem os dados dizem respeito conforme definido e especificado na Diretiva 95/46/CE».

([27]) Parecer 2/2006 do Grupo de Trabalho «proteção de dados» criado pelo Artigo 29.º sobre a prestação de serviços de filtragem de correio eletrónico, adotado em 21 de fevereiro de 2006 (WP 118). Neste parecer, o Grupo de Trabalho considera que a utilização de objetivos para efeitos do disposto no artigo 4.º pode ser compatível com o artigo 5.º da Diretiva ePrivacidade.

iii) Fundamentos jurídicos para a minimização dos efeitos de congestionamento

42. A *justificação* para este fundamento jurídico encontra-se no considerando 22 da Diretiva ePrivacidade, que explica a proibição relativa ao armazenamento das comunicações prevista no artigo 5.º, n.º 1. Esta disposição não proíbe qualquer armazenamento automático, intermédio e transitório, desde que esse armazenamento se efetue com o propósito exclusivo de realizar a transmissão e desde que as informações não sejam armazenadas por um período de tempo superior ao necessário para a transmissão e para fins de gestão de tráfego e se encontre garantida a confidencialidade das comunicações.

43. Se existir um congestionamento, coloca-se a questão de saber se o FSI pode ponderar aleatoriamente a interrupção ou o abrandamento do tráfego ou, pelo contrário, abrandar as comunicações que não são sensíveis ao tempo, por exemplo, tráfego de correio eletrónico ou P2P, permitindo, por exemplo, a passagem do tráfego de voz com uma qualidade aceitável.

44. Tendo em conta o interesse social global de garantir uma rede de comunicações eficaz, os FSI podem argumentar que dar prioridade ou condicionar o tráfego para solucionar um congestionamento é uma medida legítima que é necessária para prestar um serviço adequado. Isto significa que, nestes casos e para este efeito, existiria um fundamento jurídico geral para o tratamento de dados pessoais e não seria necessário o consentimento específico dos utilizadores.

45. Ao mesmo tempo, a capacidade de interferir desta forma não está isenta de restrições. Caso necessitem de inspecionar as comunicações, os FSI devem, na perspetiva da confidencialidade e aplicando estritamente o princípio da proporcionalidade, utilizar o método menos invasivo disponível para atingir o objetivo (evitando a inspeção profunda de pacotes) e aplicá-lo apenas durante o tempo necessário para resolver o congestionamento.

iv) Fundamentos jurídicos para o tratamento de dados para outros fins

46. Os FSI podem igualmente pretender inspecionar dados de tráfego e de conteúdo para outros fins, por exemplo, para oferecer assinaturas direcionadas (nomeadamente, uma assinatura que limita o acesso a P2P ou uma assinatura que aumenta a velocidade para determinadas aplicações). A inspeção e posterior utilização de dados de tráfego e de comunicação para fins que não sejam a prestação do serviço ou a garantia da sua segurança e o não congestionamento apenas são permitidas em condições restritas, em conformidade com o quadro jurídico.

47. O quadro jurídico é constituído essencialmente pelo artigo 5.º, n.º 1, da Diretiva ePrivacidade, que exige o consentimento dos utilizadores em causa para a escuta, a instalação de dispositivos de escuta, o armazenamento ou outras formas de interceção ou vigilância de comunicações e dos respetivos dados de tráfego. Na prática, tal significa que é necessário o consentimento dos utilizadores envolvidos numa comunicação para legitimar o tratamento dos dados de tráfego e de comunicações nos termos do artigo 5.º, n.º 1.

48. Conforme explicado acima, a aplicação de técnicas de inspeção e filtragem é baseada ou em cabeçalhos IP, que constituem dados de tráfego, ou na inspeção profunda de pacotes, o que implica igualmente *payloads* de IP e constitui dados de comunicação. Por conseguinte, em princípio, a aplicação dessas técnicas para fins que não sejam a prestação do serviço ou a segurança seria proibida, a menos que o tratamento seja permitido por um motivo legítimo, por exemplo, um consentimento (artigo 5.º, n.º 1). Um exemplo de aplicação do artigo 5.º, n.º 1, seria o caso em que um FSI decidisse oferecer aos clientes uma tarifa reduzida de acesso à Internet como contrapartida da receção de publicidade comportamental, utilizando a inspeção profunda de pacotes e, por conseguinte, de dados de comunicação, para esse fim. Nos termos do artigo 5.º, n.º 1, é necessário o consentimento livre, específico e informado.

49. Além disso, o artigo 6.º da Diretiva ePrivacidade, com o título «dados de tráfego», estabelece determinadas regras aplicáveis especificamente aos dados de tráfego. Prevê nomeadamente a possibilidade de os

FSI tratarem dados de tráfego com base no consentimento dos utilizadores para receberem serviços de valor acrescentado ([28]). Esta disposição específica o requisito de consentimento previsto no artigo 5.º, n.º 1, quando estão em causa dados de tráfego.

50. Na prática, nem sempre será fácil determinar, por exemplo, os casos em que é necessário consentimento e os casos em que a segurança da rede pode legitimar o tratamento, em especial se as técnicas de inspeção tiverem fins duplos (por exemplo, evitar o congestionamento e prestar serviços de valor acrescentado). Deve salientar-se que o consentimento não pode ser considerado uma forma simples e sistémica de assegurar a conformidade com os princípios de proteção de dados.

51. A experiência sobre a aplicação do quadro jurídico e, em especial, sobre os vários aspetos salientados acima, é escassa. Este domínio necessita de orientações suplementares, tal como especificado na Secção VI. Além disso, existem outros aspetos pertinentes relacionados com a obtenção do consentimento que exigem especial consideração. Esses aspetos são descritos a seguir.

V.2. **Questões relacionadas com a prestação de consentimento informado como fundamento jurídico**

52. O consentimento exigido nos termos dos artigos 5.º e 6.º da Diretiva ePrivacidade tem a mesma aceção que o consentimento da pessoa em causa tal como definido e especificado na Diretiva 95/46/CE ([29]). Nos termos do artigo 2.º, alínea h), da Diretiva Proteção de Dados, entende-se por consentimento da pessoa em causa «qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objeto de tratamento». Recentemente, a função do consentimento e os requisitos para a sua validade foram abordados pelo Grupo de Trabalho do Artigo 29.º, no seu Parecer 15/2011 sobre o consentimento ([30]).

53. Os FSI que necessitam de consentimento para realizar atividades de inspeção e filtragem de dados de tráfego e de conteúdo devem, por conseguinte, assegurar que esse consentimento é livre e especificado e deve constituir uma indicação totalmente informada do desejo da pessoa singular, através da qual esta manifesta o seu acordo para que os dados pessoais que lhe dizem respeito sejam objeto de tratamento. O considerando 17 da Diretiva ePrivacidade reafirma que «(…) O consentimento do utilizador pode ser dado por qualquer forma adequada que permita obter uma indicação comunicada de livre vontade, específica e informada sobre os seus desejos, incluindo por via informática ao visitar um sítio na Internet». Seguem-se alguns exemplos práticos do significado de consentimento livre, específico e informado neste contexto.

Consentimento: indicação livre, específica e informada de desejos

54. *Livre consentimento*. Os utilizadores não devem ser alvo de restrições que associem o consentimento à assinatura da Internet que pretendem subscrever.

55. O consentimento das pessoas singulares não seria prestado livremente se tivessem de consentir a monitorização dos seus dados de comunicações para obterem acesso a um serviço de comunicações. Tal seria ainda mais verdadeiro se *todos* os fornecedores de um dado mercado realizassem atividades de gestão de tráfego para fins que não sejam a segurança da rede. A única opção que restaria seria não assinar qualquer serviço da Internet. Tendo em conta que a Internet se tornou uma ferramenta essencial tanto para fins profissionais como de lazer, não assinar nenhum serviço da Internet não constitui uma

([28]) O considerando 18 da diretiva contém uma lista de exemplos de serviços de valor acrescentado. Não é claro que os serviços aos quais são aplicáveis políticas de gestão de tráfego possam ser considerados parte integrante da lista. As políticas de gestão de tráfego que visam dar prioridade a determinados conteúdos podem ser entendidas como prestando uma qualidade do serviço. Por exemplo, a gestão de tráfego que implica apenas o tratamento de cabeçalhos IP e tem como objetivo oferecer serviços de jogos a preços atrativos, nos quais o tráfego do utilizador relativo a jogos tem prioridade na rede, pode ser entendida como um serviço de valor acrescentado. Por outro lado, não é claro que a gestão de tráfego destinada a condicionar determinados tipos de tráfego, por exemplo, o abrandamento do tráfego P2P, possa ser considerada como tal.

([29]) Ver o considerando 17 e artigo 2.º, alínea f), da Diretiva ePrivacidade.

([30]) Adotado em 13 de julho de 2011 (WP 187).

alternativa válida. O resultado seria que as pessoas singulares não teriam qualquer poder real de escolha, ou seja, não poderiam prestar livremente o seu consentimento ([31]).

56. A AEPD considera que é evidente a necessidade de a Comissão e as autoridades nacionais monitorizarem o mercado, especialmente para determinar se este cenário — os fornecedores associarem os serviços de telecomunicações à monitorização das comunicações — se torna frequente. Os fornecedores devem oferecer serviços alternativos, incluindo uma assinatura da Internet não sujeita a gestão de tráfego, sem impor custos elevados às pessoas singulares.

57. *Consentimento específico.* A necessidade de um consentimento específico exige, neste caso, que os FSI obtenham de forma clara e inequívoca o consentimento para monitorizar dados de tráfego e de comunicações. Nos termos do Grupo de Trabalho do Artigo 29.º, «… para ser específico, o consentimento deve ser inteligível: deve fazer referência, de forma clara e precisa, ao âmbito e consequências do tratamento de dados. Não pode aplicar-se a um conjunto aberto de atividades de tratamento. Significa isto, por outras palavras, que o consentimento se aplica a um contexto limitado». O consentimento específico dificilmente será obtido se o consentimento para a inspeção de dados de tráfego e de comunicações for «incorporado» no consentimento global para subscrever o serviço. Em alternativa, a especificidade deve ser objeto de meios destinados a obter o consentimento como, por exemplo, um formulário de consentimento específico ou uma caixa de texto separada claramente dedicados ao objetivo de monitorização (em vez de inserir a informação nas condições gerais do contrato e solicitar a assinatura do contrato tal como está).

58. *Consentimento informado*. Para que seja válido, o consentimento tem de ser informado. A necessidade de prestar informações prévias adequadas decorre não só da Diretiva ePrivacidade e da Diretiva Proteção de Dados, mas também dos artigos 20.º e 21.º da Diretiva relativa ao serviço universal, alterada pela Diretiva 2009/136/CE ([32]). A necessidade de informação e consentimento foi expressamente confirmada no considerando 28 da Diretiva 2009/136/CE: «Os utilizadores deverão, em qualquer caso, ser informados de forma completa sobre quaisquer limitações impostas à utilização dos serviços de comunicações eletrónicas pelo prestador de serviço e/ou rede. Essa informação deverá, por opção do prestador, especificar o tipo de conteúdo, aplicação ou serviço em questão, ou aplicações ou serviços individuais, ou ambos». Especifica também que: «Em função da tecnologia utilizada e do tipo de limitação, essas limitações poderão exigir o consentimento do utilizador nos termos da Diretiva 2002/58/CE».

59. Tendo em conta a complexidade destas técnicas de monitorização, a prestação de informações prévias pertinentes é uma das principais dificuldades para obter um consentimento válido. Os consumidores devem ser informados de forma a serem capazes de identificar a informação que está a ser tratada, como está a ser utilizada e o impacto sobre a experiência do utilizador, bem como o nível de invasão da privacidade associado às técnicas.

60. Tal significa não só que a própria informação deve ser clara e compreensível para os utilizadores comuns como também que a informação deve ser prestada diretamente às pessoas singulares de uma forma clara para que não possam ignorá-la.

61. *Indicação de desejos*. No âmbito do quadro jurídico aplicável, o consentimento exige igualmente uma ação afirmativa por parte do utilizador para manifestar o seu acordo. O consentimento implícito não cumpre esta norma. Esta afirmação confirma a necessidade de utilizar meios dedicados para obter o consentimento que permite aos FSI inspecionar dados de tráfego e de comunicações no contexto das políticas de gestão de tráfego aplicáveis. No seu recente parecer sobre o consentimento, o Grupo de Trabalho do Artigo 29.º salientou a necessidade de detalhe na obtenção do consentimento no que respeita aos diferentes elementos que constituem o tratamento de dados.

([31]) Um caso idêntico são os registos de identificação dos passageiros (PNR, *Passenger Name Records*), no qual foi discutido se o consentimento dos passageiros para a transferência dos dados de reserva para as autoridades dos EUA era válido. O Grupo de Trabalho considerou que o consentimento dos passageiros não pode ser prestado de forma livre, uma vez que as companhias aéreas estão obrigadas a enviar os dados antes de o avião descolar, pelo que os passageiros não têm, assim, nenhum poder real de escolha sobre se pretendem ou não viajar; Parecer 6/2002 do Grupo de proteção de dados pessoais do Artigo 29.º sobre a transmissão para os Estados Unidos de informações sobre o manifesto de passageiros e outros dados provenientes das companhias aéreas.

([32]) Diretiva 2009/136/CE, de 25 de novembro de 2009, que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações electrónicas (Ver nota de pé-de-página 15.).

62. Pode argumentar-se que, se as partes envolvidas numa comunicação não pretenderem que os FSI intercetem essa comunicação a fim de aplicar políticas de gestão de tráfego, podem sempre encriptar a comunicação. Esta abordagem pode ser considerada útil em termos práticos, mas exige algum esforço e conhecimentos técnicos e não pode ser equiparada a um consentimento livre, específico e informado. De igual modo, a utilização de técnicas de encriptação não preserva totalmente a confidencialidade da comunicação, uma vez que o FSI terá, pelo menos, acesso à informação do cabeçalho IP a fim de encaminhar a comunicação e estará igualmente em condições de aplicar uma análise estatística.

63. Nos termos do artigo 51.º, n.º 1, da Diretiva ePrivacidade, deve ser obtido o consentimento dos utilizadores em causa. Em muitos casos, o utilizador será simultaneamente o assinante, o que permite o consentimento no momento da assinatura do serviço de telecomunicações. Noutros casos, nomeadamente aqueles em que podem estar envolvidas pelo menos duas pessoas, o consentimento dos utilizadores em causa deve ser obtido separadamente. Esta situação pode colocar questões de ordem prática, conforme indicado a seguir.

Consentimento de todos os utilizadores interessados

64. O artigo 5.º, n.º 1, prevê o consentimento do utilizador para legitimar o tratamento de dados. Deve ser obtido o consentimento de *todos os utilizadores* envolvidos numa comunicação. A *justificação* subjacente é que a comunicação diz normalmente respeito a, pelo menos, duas pessoas (o remetente e o destinatário). Por exemplo, se um FSI examinar *payloads* de IP que fazem referência a uma mensagem de correio eletrónico, está a inspecionar informações relacionadas quer com o remetente quer com o destinatário da mensagem.

65. Ao monitorizar e intercetar tráfego e comunicações (por exemplo, algum tráfego da Internet), a obtenção do consentimento do utilizador, ou seja, do assinante, pode ser suficiente para os FSI. Tal deve-se ao facto de a outra parte da comunicação, neste caso, um sítio Internet visitado, poder não ser considerada um «utilizador interessado» ([33]). No entanto, a situação pode ser mais complexa quando essa monitorização envolve a inspeção do conteúdo de mensagens de correio eletrónico e, consequentemente, das informações pessoais do remetente e do destinatário da mensagem, que poderão não ter ambos uma relação contratual com o mesmo FSI. Com efeito, nestes casos, o FSI estaria a tratar dados pessoais (nome, endereço de correio eletrónico e dados de conteúdos potencialmente sensíveis) de não clientes. De um ponto de vista prático, a obtenção do consentimento dessas pessoas singulares pode ser mais difícil, uma vez que deve ser efectuada numa base casuística e não no momento da assinatura do serviço de telecomunicações. Também não seria realista pressupor que o consentimento do assinante foi igualmente prestado em nome de outros utilizadores, como é frequentemente o caso de agregados privados.

66. Neste contexto, a AEPD considera que os FSI devem respeitar os requisitos legais existentes e implementar políticas que não envolvam a monitorização e inspeção da informação. Este aspeto é ainda mais importante no que respeita aos serviços de comunicações que envolvem terceiros que não podem prestar o seu consentimento à monitorização, em especial no que respeita ao correio eletrónico enviado e recebido (não se aplica se a finalidade for baseada em considerações de segurança).

67. Ao mesmo tempo, deve notar-se que a legislação nacional que dá execução ao artigo 5.º, n.º 1, da Diretiva ePrivacidade, pode não ser sempre satisfatória a este respeito, e que, em geral, parece ser necessária uma melhor orientação quanto aos requisitos da Diretiva ePrivacidade neste contexto. Por conseguinte, a AEPD exorta a Comissão a ser mais ativa nesta matéria e a adotar uma iniciativa que possa beneficiar das conclusões das autoridades de supervisão reunidas no Grupo de Trabalho do Artigo 29.º e de outras partes interessadas. Se necessário, a Comissão poderá recorrer ao Tribunal de Justiça para que a aceção e as consequências do artigo 5.º, n.º 1, sejam totalmente clarificadas.

([33]) Não obstante os casos em que o tráfego na Internet envolve a transferência de informações pessoais como, por exemplo, imagens de pessoas singulares identificáveis colocadas num sítio Internet. O tratamento dessas informações necessita de base jurídica, mas não seria abrangido pelo artigo 5.º, n.º 1, uma vez que essas pessoas não seriam «utilizadores interessados».

V.3. **Proporcionalidade — princípio da minimização dos dados**

68. O artigo 6.º, alínea c), da Diretiva Proteção de Dados estabelece o princípio da proporcionalidade ([34]), aplicável aos FSI, uma vez que são controladores de dados, na aceção desta diretiva, quando realizam atividades de monitorização e filtragem.

69. De acordo com aquele princípio, os dados pessoais podem ser objeto de tratamento apenas se forem «adequados, pertinentes e não excessivos em relação às finalidades prosseguidas com a recolha e/ou o tratamento». A aplicação deste princípio implica a necessidade de avaliar se os meios utilizados para o tratamento dos dados e os tipos de dados pessoais utilizados são adequados e têm possibilidades razoáveis de atingir os seus objetivos. Caso a conclusão aponte para a necessidade de recolha de mais dados, então o princípio não é cumprido.

70. A conformidade com o princípio da proporcionalidade de determinados tipos de técnicas de inspeção deve ser avaliada numa base casuística. Não é possível chegar a conclusões *in abstracto*. No entanto, é possível apontar vários aspetos concretos que devem ser analisados ao avaliar a conformidade com o princípio da proporcionalidade.

71. *O volume de informação objeto de tratamento*. A vigilância das comunicações dos clientes dos FSI nos níveis mais profundos possíveis será, na maior parte dos casos, excessiva e ilegal. O facto de que essa vigilância pode ser feita por meios que não são aparentes para as pessoas singulares e que estas poderão ter dificuldade em compreender o que está a acontecer aumenta o impacto na sua privacidade. Os FSI devem avaliar quais os meios menos invasivos que podem estar disponíveis para atingir o resultado pretendido. Por exemplo, a monitorização dos cabeçalhos IP pode obter o resultado pretendido em vez da inspeção profunda de pacotes? Mesmo utilizando a inspeção profunda de pacotes, a identificação de apenas determinados protocolos pode proporcionar as informações necessárias. A aplicação de garantias em matéria de proteção de dados, nomeadamente a «pseudo-anonimização», também pode ser pertinente. O resultado da avaliação deve confirmar que o tratamento dos dados é proporcional.

72. *Os efeitos do tratamento (diretamente associados aos fins)*. A proporcionalidade pode não existir nos casos em que os FSI utilizam políticas de gestão de tráfego que excluem o acesso a determinados serviços sem permitir, em troca, uma distribuição justa dos benefícios aos utilizadores.

73. É importante recordar que o princípio da proporcionalidade continua a ser aplicável mesmo que tenham sido cumpridos outros requisitos legais, nomeadamente se um FSI tiver, por exemplo, obtido o consentimento de pessoas singulares para realizar atividades de monitorização de conteúdos. Tal significa que o tratamento de dados realizado através da monitorização de conteúdos pode ainda ser ilegal se violar o princípio fundamental da proporcionalidade subjacente.

V.4. **Medidas organizativas e de segurança**

74. O artigo 4.º da Diretiva ePrivacidade exige explicitamente que os FSI adoptem medidas técnicas e organizativas adequadas para garantir: i) que aos dados pessoais apenas possa ter acesso pessoal autorizado, para fins autorizados a nível legal; ii) a proteção dos dados pessoais contra o tratamento acidental ou ilegal, e iii) a aplicação de uma política de segurança relativa ao tratamento de dados pessoais. Autoriza ainda as autoridades nacionais competentes a realizar auditorias sobre essas medidas.

75. Além disso, nos termos do artigo 4.º, n.os 2 e 3, da Diretiva ePrivacidade, os FSI estão igualmente obrigados a notificar as autoridades nacionais competentes, no caso de violação de dados, e as pessoas singulares afetadas, caso a divulgação dos dados possa ter consequências negativas para essas pessoas.

76. O tratamento de informações pessoais contidas em comunicações com a finalidade de aplicar políticas de gestão de tráfego pode proporcionar aos FSI acesso a dados ainda mais sensíveis do que os dados de tráfego.

([34]) Conforme salientado acima, a Diretiva Proteção de Dados aplica-se a todas os aspetos relativos à proteção dos direitos e liberdades fundamentais que não sejam abrangidos especificamente pela Diretiva ePrivacidade.

77. Por conseguinte, as políticas de segurança desenvolvidas pelos FSI devem incorporar garantias específicas para assegurar que as medidas adotadas são adequadas a esses riscos. Ao mesmo tempo, as autoridades nacionais competentes que realizam a auditoria dessas medidas devem ser especialmente exigentes. Por último, deve assegurar-se que são executados procedimentos de notificação eficazes a fim de informar as pessoas em causa cujas informações foram comprometidas e podem, assim, ter sido afetadas negativamente.

VI. **SUGESTÕES DE MEDIDAS DE POLÍTICA E LEGISLATIVAS**

78. As técnicas de inspeção baseadas no tráfego de dados e a inspeção de *payloads* de IP, ou seja, do conteúdo das comunicações, podem revelar a atividade dos utilizadores na Internet: sítios Internet visitados e atividades realizadas nesses sítios, utilização de aplicações P2P, ficheiros descarregados, correio eletrónico enviado e recebido, de quem, sobre que assunto e em que termos, etc. Os FSI podem pretender utilizar estas informações para dar prioridade a algumas comunicações sobre outras como, por exemplo, vídeo a pedido. Podem pretender utilizá-las para identificar vírus ou criar perfis com o intuito de fornecer publicidade comportamental. Essas ações interferem com o direito à confidencialidade das comunicações.

79. Dependendo das técnicas utilizadas e das especificidades do caso, as implicações em matéria de privacidade aumentarão. Quanto mais profunda for a interceção e a análise das informações recolhidas, maior será o conflito com o princípio da confidencialidade das comunicações. As finalidades da monitorização realizada e as garantias de proteção dos dados que têm sido aplicadas são igualmente elementos essenciais para determinar o grau de invasão da privacidade e dos dados pessoais das pessoas singulares. O bloqueio e a monitorização para efeitos de combate de programas malévolos (*malware*), com limitações rigorosas no que respeita à retenção e utilização dos dados inspecionados, não podem ser comparados com situações em que as informações são registadas para criar perfis individuais com vista a fornecer publicidade comportamental.

80. Em princípio, a AEPD considera que o atual quadro jurídico europeu em matéria de privacidade e proteção de dados, se for interpretado, aplicado e executado corretamente, será adequado para garantir que o direito à confidencialidade é respeitado e, em geral, que a privacidade e a proteção dos dados das pessoas singulares não são comprometidas ([35]). Os FSI não devem utilizar esses mecanismos, a menos que tenham aplicado corretamente o quadro jurídico. Mais especificamente, os elementos pertinentes do quadro jurídico que os FSI devem considerar e respeitar são:

— Os FSI podem aplicar políticas de gestão de tráfego destinadas a garantir a segurança do serviço e da prestação do serviço, nomeadamente diminuir o congestionamento, nos termos dos artigos 4.º e 6.º da Diretiva ePrivacidade;

— Os FSI necessitam de outro fundamento jurídico específico, e possivelmente do consentimento dos utilizadores, para aplicar políticas de gestão de tráfego que impliquem o tratamento de dados de tráfego e/ou de comunicações para outros fins que não os indicados acima. Por exemplo, o consentimento informado dos utilizadores é necessário para monitorizar e filtrar as comunicações de pessoas singulares com a finalidade de limitar (ou permitir) o acesso a determinados serviços e aplicações, como P2P ou VoIP;

— O consentimento deve ser livre, explícito e informado. Deve ser indicado através de uma ação afirmativa. Estes requisitos incidem sobretudo na necessidade de aumentar os esforços com vista a assegurar que as pessoas singulares são informadas adequadamente, de uma forma direta, compreensível e específica que lhes permita avaliar os efeitos das práticas e, por último, tomar uma decisão informada. Tendo em conta a complexidade destas técnicas, a prestação de informações prévias pertinentes aos utilizadores é uma das principais dificuldades para obter um consentimento válido. Além disso, não devem existir consequências prejudiciais (nomeadamente custos financeiros) para os utilizadores que não consintam qualquer monitorização;

([35]) Tal não impede que seja necessário alterar a legislação com base noutras considerações, nomeadamente no contexto da revisão geral do quadro jurídico europeu em matéria de proteção de dados, com vista a torná-lo mais eficaz à luz das novas tecnologias e da globalização.

— O princípio da proporcionalidade desempenha um papel fundamental quando os FSI aplicam políticas de gestão de tráfego, independentemente do fundamento jurídico do tratamento e da finalidade: prestar o serviço, evitar congestionamentos ou oferecer assinaturas direcionadas com ou sem acesso a determinados serviços e aplicações. Este princípio limita a capacidade dos FSI para realizar atividades de monitorização do conteúdo das comunicações de pessoas singulares que impliquem o tratamento de demasiadas informações ou resultem em benefícios apenas para os FSI. As actividades que os FSI podem executar do ponto de vista logístico dependerão do nível de invasão das técnicas, dos resultados exigidos (dos quais podem obter benefícios) e das garantias específicas aplicadas em matéria de privacidade e proteção de dados. Antes de implementarem técnicas de inspeção, os FSI devem avaliar se essas técnicas respeitam o princípio da proporcionalidade.

81. Embora o quadro jurídico contenha atualmente condições e garantias pertinentes, é necessário prestar especial atenção ao cumprimento efetivo dos requisitos legais por parte dos FSI, se estes fornecem as informações necessárias aos consumidores para que estes possam fazer escolhas com o conhecimento adequado e se observam o princípio da proporcionalidade. A nível nacional, as autoridades competentes para aplicação do acima exposto incluem, por um lado, as autoridades nacionais de telecomunicações e, por outro, as autoridades nacionais de proteção de dados. A nível da UE, os organismos pertinentes incluem o ORECE (Organismo de Reguladores Europeus das Comunicações Eletrónicas). A AEPD pode também desempenhar um papel neste contexto.

82. Além do acompanhamento do atual nível de conformidade, e dado que a possibilidade de realização de um elevado número de inspeções de comunicações em tempo real é relativamente recente, alguns aspetos relacionados com a aplicação do quadro jurídico que foram debatidos no presente parecer exigem uma análise mais profunda e uma clarificação posterior. São necessárias orientações especialmente pertinentes em vários domínios, nomeadamente:

— Determinar as práticas de inspeção que são legítimas para assegurar o fluxo contínuo do tráfego e que não exigem o consentimento dos utilizadores como, por exemplo, o combate às comunicações não solicitadas. Além do nível de invasão da monitorização aplicada, são pertinentes aspetos como, por exemplo, o nível de perturbação do fluxo contínuo de tráfego que de outro modo ocorreria;

— Determinar as técnicas de inspeção que podem ser utilizadas para efeitos de segurança e que poderão não exigir o consentimento dos utilizadores;

— Determinar em que situações a monitorização necessita do consentimento das pessoas singulares, nomeadamente o consentimento de todos os utilizadores em causa, bem como os parâmetros técnicos admissíveis para assegurar que a técnica de inspeção não implica um tratamento de dados que não seja proporcional tendo em conta os fins previstos;

— Além disso, nos três casos acima descritos, poderão ser necessárias orientações no que respeita à aplicação das garantias de proteção de dados necessárias (limitação da finalidade, segurança, etc.).

83. Tendo em conta que as competências neste domínio são nacionais e europeias, a AEPD considera essencial a partilha de opiniões e experiências com vista a encontrar abordagens harmonizadas. Para esse efeito, a AEPD sugere a criação de uma plataforma ou de um grupo de peritos que deve reunir representantes das autoridades reguladoras nacionais, o Grupo de Trabalho do Artigo 29.º, a AEPD e o ORECE. O primeiro objetivo desta plataforma seria o de desenvolver orientações, pelo menos sobre os aspetos acima identificados, a fim de assegurar abordagens sólidas e harmonizadas e condições equitativas. A AEPD exorta a Comissão a organizar esta iniciativa.

84. Por último, tanto as autoridades nacionais como as suas homólogas europeias, incluindo o ORECE e a Comissão Europeia, devem prestar especial atenção aos desenvolvimentos de mercado neste domínio. Do ponto de vista da proteção de dados e da privacidade, um cenário no qual os FSI aplicassem regularmente políticas de gestão de tráfego com a oferta de assinaturas baseadas na filtragem do acesso a conteúdos e aplicações seria extremamente problemático. Se esse cenário alguma vez acontecesse, seria necessário elaborar legislação para resolver esta situação.

VII. **CONCLUSÕES**

85. A crescente dependência dos FSI de técnicas de monitorização e inspeção interfere com a neutralidade da Internet e a confidencialidade das comunicações. Esta situação suscita sérias questões no que respeita à proteção da privacidade e dos dados pessoais dos utilizadores.

86. Embora a Comunicação da Comissão sobre abertura e neutralidade da Internet na Europa aborde resumidamente estas questões, a AEPD considera que é necessário adotar medidas adicionais para desenvolver uma política satisfatória quanto ao rumo a seguir. No presente parecer, a AEPD contribuiu para o debate político em curso sobre a neutralidade da Internet, em especial sobre os aspetos relacionados com a proteção de dados e a privacidade.

87. A AEPD considera que é necessário que as autoridades nacionais e o ORECE acompanhem a situação do mercado. Este acompanhamento deve resultar numa perspetiva clara que permita determinar se o mercado está a evoluir para uma inspeção massiva e em tempo real das comunicações e identificar as questões relacionadas com o cumprimento do quadro jurídico.

88. O acompanhamento do mercado deve ser antecedido de uma análise pormenorizada dos efeitos das novas práticas sobre a proteção de dados e a privacidade na Internet. O presente parecer salienta alguns domínios que beneficiariam de uma clarificação. Embora as agências e os organismos europeus como o ORECE, o Grupo de Trabalho do Artigo 29.º e a AEPD possam estar em boa posição para clarificar as condições de aplicação do quadro jurídico, a AEPD considera que a Comissão tem o dever de coordenar e orientar o debate. Por conseguinte, exorta a Comissão a adotar uma iniciativa que reúna todas as partes interessadas numa plataforma ou num grupo de trabalho com este objetivo. Entre as questões que necessitam de uma análise mais profunda, salientam-se os seguintes aspetos:

— Determinar as práticas de inspeção que são legítimas para assegurar o fluxo contínuo do tráfego e quais as que podem ser executadas para fins de segurança;

— Determinar em que situações a monitorização necessita do consentimento das pessoas singulares, nomeadamente o consentimento de todos os utilizadores em causa, e os parâmetros técnicos admissíveis para assegurar que a técnica de inspeção não implica um tratamento de dados que não seja proporcional tendo em conta os fins previstos;

— Nos casos acima descritos, poderão ser necessárias orientações no que respeita à aplicação das garantias de proteção de dados necessárias (limitação da finalidade, segurança, etc.).

89. Dependendo destas conclusões, poderão ser necessárias medidas legislativas adicionais. Nesse caso, a Comissão deve apresentar medidas que visem reforçar o quadro jurídico e garantir a segurança jurídica. As novas medidas devem clarificar as consequências práticas do princípio da neutralidade da Internet, uma vez que esta clarificação já foi efetuada em alguns Estados-Membros, e assegurar que os utilizadores podem exercer um poder real de escolha, nomeadamente forçando os FSI a oferecer ligações não monitorizadas.

Feito em Bruxelas, em 7 de outubro de 2011.

Peter HUSTINX

Supervisor Europeu para a Proteção de Dados