Segundo parecer da Autoridade Europeia para a Protecção de Dados sobre a revisão da Directiva 2002/58/CE relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas)

(2009/C 128/04)

A AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS,

Tendo em conta o Tratado que institui a Comunidade Europeia, nomeadamente o artigo 286.º,

Tendo em conta a Carta dos Direitos Fundamentais da União Europeia, nomeadamente o artigo 8.º,

Tendo em conta a Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados,

Tendo em conta a Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas,

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

APROVOU O SEGUINTE PARECER:

I. INTRODUÇÃO

Antecedentes

1. Em 13 de Novembro de 2007, a Comissão Europeia adoptou uma proposta (a seguir designada por «proposta» ou «proposta da Comissão») que altera, dentre outras, a Directiva relativa à privacidade no sector das comunicações electrónicas (Directiva «Privacidade e Comunicações Electrónicas») [1]. Em 10 de Abril de 2008, a AEPD emitiu um parecer sobre a proposta da Comissão no qual formulou recomendações destinadas a melhorá-la a fim de garantir que as modificações sugeridas proporcionem a maior protecção possível da privacidade e dos dados pessoais das pessoas singulares («primeiro parecer da AEPD») [2].

2. A AEPD recebeu positivamente a proposta da Comissão de se criar um sistema de notificação obrigatória das violações da segurança que exija que as empresas notifiquem as pessoas sempre que os seus dados pessoais tenham sido colocados em risco. Além disso, elogiou a nova disposição que permite que as pessoas colectivas (por exemplo, associações de consumidores e prestadores de serviços Internet) intentem acções contra os autores de *spam*, em complemento dos instrumentos já existentes de luta contra o *spam*,

3. Durante os debates parlamentares que antecederam a primeira leitura do Parlamento Europeu, a AEPD apresentou um novo contributo ao emitir observações sobre determinadas questões suscitadas nos relatórios elaborados pelas comissões do Parlamento Europeu competentes para rever as Directivas «Serviço Universal» [3] e «Privacidade e Comunicações Electrónicas» («observações») [4]. As observações abordaram essencialmente assuntos relacionados com o tratamento dos dados de tráfego e a protecção dos direitos de propriedade intelectual.

4. Em 24 de Setembro de 2008, o Parlamento Europeu («PE») aprovou uma resolução legislativa sobre a Directiva «Privacidade e Comunicações Electrónicas» («primeira leitura») [5]. A AEPD acolheu favoravelmente várias alterações do PE aprovadas na sequência do parecer e das obser vações da AEPD supramencionados. Entre as importantes modificações introduzidas, contava-se a inclusão dos prestadores de serviços da sociedade da informação (isto é,

[1] A revisão da Directiva «Privacidade e Comunicações Electrónicas» insere-se no âmbito de um processo de revisão mais vasto que tem por objectivo a criação de uma autoridade da UE em matéria de telecomunicações e a revisão das Directivas 2002/21/CE, 2002/19/CE, 2002/20/CE, 2002/22/CE e 2002/58/CE e do Regulamento (CE) n.º 2006/2004 (a seguir designada, no seu conjunto, por «revisão do pacote Telecom»).

[2] Parecer de 10 de Abril de 2008 sobre a proposta de directiva que altera, dentre outras, a Directiva 2002/58/CE relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva Privacidade e Comunicações Electrónicas), JO C 181 de 18.7.2008, p. 1.

[3] Directiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações electrónicas (Directiva «Serviço Universal»), JO L 108, de 24.4.2002, p. 51.

[4] «*EDPS Comments on selected issues that arise from the IMCO report on the review of Directive 2002/22/EC (Universal Service) & Directive 2002/58/EC (ePrivacy)*» [Observações da AEPD sobre determinadas questões suscitadas no relatório da Comissão do Mercado Interno e da Protecção dos Consumidores sobre a revisão das Directivas 2002/22/CE («Serviço Universal») e 2002/58/CE («Privacidade e Comunicações Electrónicas»)], 2 de Setembro de 2008. Disponível no sítio: www.edps.europa.eu

[5] Resolução legislativa do Parlamento Europeu, de 24 de Setembro de 2008, sobre uma proposta de directiva do Parlamento Europeu e do Conselho que altera a Directiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações electrónicas, a Directiva 2002/58/CE relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas e o Regulamento (CE) n.º 2006/2004 relativo à cooperação no domínio da defesa do consumidor [COM(2007) 698 — C6-0420/2007 — 2007/0248(COD)].

empresas que operam na internet) no âmbito de aplicação da obrigação de notificar violações da segurança. A AEPD congratulou-se igualmente com a alteração que permite que as pessoas singulares e colectivas intentem acções por infracção a qualquer disposição da Directiva «Privacidade e Comunicações Electrónicas» (e não apenas por violação das disposições relativas ao *spam*, como inicialmente previa a proposta da Comissão). A primeira leitura do Parlamento foi seguida da adopção, pela Comissão, de uma proposta alterada relativa à Directiva «Privacidade e Comunicações Electrónicas» (a seguir designada por «proposta alterada») ([6]).

5. Em 27 de Novembro de 2008, o Conselho chegou a um acordo político sobre a revisão das regras relativas ao pacote Telecom, incluindo a Directiva «Privacidade e Comunicações Electrónicas», acordo esse que dará lugar à posição comum do Conselho («posição comum») ([7]). A posição comum, que poderá integrar a proposta de alterações do PE, será notificada ao PE nos termos do n.º 2 do artigo 251.º do Tratado que institui a Comunidade Europeia.

Observações gerais sobre a posição comum

6. O Conselho modificou elementos essenciais do texto da proposta e não aceitou muitas das alterações aprovadas pelo PE. Sendo embora certo que a posição comum contém elementos positivos, a AEPD está, na generalidade, preocupada com o seu conteúdo, em especial porque a posição comum não incorpora algumas das alterações positivas apresentadas pelo PE, na proposta alterada ou nos pareceres da AEPD e nos pareceres das autoridades europeias de protecção de dados emitidos no âmbito do Grupo do Artigo 29.º ([8]).

7. Pelo contrário, em não poucos casos, as disposições da proposta alterada e as alterações do PE, que ofereciam salvaguardas aos cidadãos, foram suprimidas ou substancialmente enfraquecidas. Em consequência, o nível de protecção concedido às pessoas singulares na posição comum ficou consideravelmente enfraquecido. É por este motivo que a AEPD emite agora um segundo parecer, na esperança de que, à medida que a Directiva «Privacidade e Comunicações Electrónicas» for percorrendo todas as etapas do processo legislativo, serão aprovadas novas alterações que restabeleçam as salvaguardas em matéria de protecção de dados.

8. Esse segundo parecer centra-se nalgumas preocupações essenciais, mas não retoma todos os aspectos abordados no primeiro parecer da AEPD ou nas observações, que não obstante continuam todos válidos. Em especial, o presente parecer debruça-se sobre os seguintes pontos:

— Disposições em matéria de notificação das violações da segurança;

— O escopo da aplicação da Directiva «Privacidade e Comunicações Electrónicas» às redes privadas e às redes privadas acessíveis ao público;

— Tratamento de dados de tráfego para fins de segurança;

— Capacidades de as pessoas colectivas intentarem acções por infracção à Directiva «Privacidade e Comunicações Electrónicas».

9. No âmbito da análise dos pontos acima enunciados, o presente parecer examina a posição comum do Conselho e compara-a à primeira leitura do PE e à proposta alterada da Comissão. O presente parecer inclui recomendações destinadas a racionalizar as disposições da Directiva «Privacidade e Comunicações Electrónicas» e a garantir que a directiva continue a proteger adequadamente a privacidade e os dados pessoais das pessoas singulares.

II. DISPOSIÇÕES EM MATÉRIA DE NOTIFICAÇÃO DAS VIOLAÇÕES DA SEGURANÇA

10. A AEPD apoia a adoção de um sistema de notificação das violações da segurança nos termos do qual as autoridades e as pessoas singulares sejam notificadas sempre que os seus dados pessoais tenham sido colocados em risco ([9]). A notificação das violações da segurança pode ajudar as pessoas singulares a tomar as medidas necessárias para atenuar os potenciais danos decorrentes de tal situação. Além disso, a obrigação de notificação das violações da segurança incentivará as empresas a melhorar a segurança dos dados e a prestar mais contas no que respeita aos dados pessoais pelos quais são responsáveis.

11. A proposta alterada da Comissão, a primeira leitura do Parlamento Europeu e a posição comum do Conselho constituem três abordagens diferentes da notificação de violações da segurança actualmente em análise. Cada uma destas três abordagens apresenta aspectos positivos. Todavia, a AEPD considera que todas elas podem ser melhoradas e preconiza que sejam tidas em conta as recomendações a seguir formuladas na ponderação das últimas etapas para a adopção de um sistema de notificação das violações da segurança.

([6]) Proposta alterada de directiva do Parlamento Europeu e do Conselho que altera a Directiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações electrónicas, a Directiva 2002/58/CE relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas e o Regulamento (CE) n.º 2006/2004 relativo à cooperação no domínio da defesa do consumidor, Bruxelas, 6.11.2008 COM(2008) 723 final.

([7]) Disponível no sítio web do Conselho.

([8]) Parecer 2/2008 sobre a Directiva 2002/58/CE relativa à privacidade no sector das comunicações electrónicas (Directiva Privacidade Electrónica), disponível no sítio web do Grupo do Artigo 29.º.

([9]) No presente parecer usa-se a expressão «colocados em risco» sempre que tenha ocorrido uma violação de dados pessoais resultante, de modo acidental ou ilegal, da destruição, da perda, da alteração ou da divulgação ou acesso não autorizados a dados pessoais transmitidos, armazenados ou de outro modo tratados.

12. Na análise dos três sistemas de notificação das violações da segurança, há cinco pontos críticos a levar em consideração: *i)* a definição de violação da segurança; *ii*) as entidades abrangidas pela obrigação de notificação («entidades abrangidas»); *iii*) o critério que determina a obrigação de notificar; *iv*) a determinação da entidade responsável por decidir se uma violação da segurança preenche ou não esse critério; *v)* os destinatários da notificação.

Análise geral das abordagens da Comissão, do Conselho e do PE

13. O Parlamento Europeu, a Comissão e o Conselho adoptaram todos abordagens diferentes para a notificação das violações da segurança. A primeira leitura do PE modificou o sistema de notificação das violações da segurança apresentado na proposta inicial da Comissão ([10]). No âmbito da abordagem do PE, a obrigação de notificar aplica-se não só aos prestadores de serviços de comunicações electrónicas publicamente disponíveis (PPECS), como também aos prestadores de serviços da sociedade da informação (ISSP). Além disso, ao abrigo desta abordagem todas as violações de dados pessoais têm de ser notificadas à autoridade reguladora nacional ou às autoridades competentes (conjuntamente designadas por «autoridades»). Se as autoridades considerarem que a violação é *grave*, exigem aos PPECS e aos ISSP que notifiquem sem demora a pessoa afectada. Em caso de violações que representem um perigo iminente e directo, os PPECS e os ISSP notificam as pessoas em causa antes de notificarem as autoridades, sem aguardar uma decisão regulamentar. O texto prevê uma isenção da obrigação de notificação dos consumidores para as entidades que possam demonstrar às autoridades que «*foram aplicadas*» «*medidas tecnológicas de protecção adequadas*» que tornam os dados indecifráveis a qualquer pessoa que não esteja autorizada a aceder a eles.

14. A abordagem do Conselho também prevê que tanto os assinantes como as autoridades devem ser notificados, mas só nos casos em que a *entidade abrangida* considere que a violação representa um *grave risco* para a privacidade do assinante (por exemplo furto ou usurpação de identidade, danos físicos, humilhação significativa ou prejuízo para a reputação).

15. A proposta alterada da Comissão mantém a obrigação, proposta pelo PE, de notificar às autoridades todas as violações. Todavia, contrariamente à abordagem do PE, a proposta alterada prevê uma isenção da obrigação de notificação das pessoas em causa se o PPECS demonstrar à autoridade competente: *i)* que não existe «*probabilidade*» *razoável* de efeitos lesivos (por exemplo, prejuízos económicos, danos sociais ou furto de identidade) em consequência da violação ou *ii*) que foram aplicadas «*medidas tecnológicas de protecção adequadas*» aos dados a que diz respeito a violação. Assim, a abordagem da Comissão inclui uma análise baseada no efeito lesivo no contexto das notificações às pessoas em causa.

16. Importa registar que, no âmbito das abordagens do PE ([11]) e da Comissão, cabe em última instância *às autoridades* decidir se a violação é ou não grave ou se existe uma probabilidade razoável de que venha a ter efeitos lesivos. Em sentido contrário, na abordagem do Conselho a decisão é deixada às *entidades em causa*.

17. As abordagens do Conselho e da Comissão aplicam-se ambas apenas aos PPECS e não aos ISSP, contrariamente à abordagem do PE.

Definição de violação da segurança

18. A AEPD congratula-se por verificar que as três propostas legislativas contêm a mesma definição de violação da segurança, a saber: «*uma violação da segurança que provoca, de modo acidental ou ilegal, a destruição, a perda, a alteração, a divulgação ou acesso não autorizados a dados pessoais transmitidos, armazenados ou de outro modo tratados […]*» ([12]).

19. Como adiante descrito mais detalhadamente, esta definição é de saudar, uma vez que é suficientemente ampla para abarcar a maioria das situações relevantes susceptíveis de justificar a notificação de violações da segurança.

20. Em primeiro lugar, a definição inclui as situações em que houve um *acesso não autorizado* a dados pessoais por terceiros, como o ataque de um servidor que contenha dados pessoais e a extracção dessas informações.

21. Em segundo lugar, a definição permite igualmente incluir as situações em que houve perda ou divulgação de dados pessoais, mesmo que o acesso não autorizado tenha ainda de ser demonstrado, o que inclui situações em que os dados pessoais possam ter sido perdidos (por exemplo, CD-ROM, chaves USB ou outros dispositivos portáteis) ou tornados publicamente disponíveis por utilizadores regulares (ficheiros de dados de empregados tornados inadvertida e temporariamente acessíveis ao público pela internet). Atendendo a que em muitos casos não haverá provas que demonstrem que os dados em causa podem ou não, em determinado momento, ter sido objecto de acesso ou utilização por terceiros não autorizados, afigura-se adequado incluir estas situações no âmbito de aplicação da definição. Por conseguinte, a AEPD recomenda que se mantenha esta definição. A AEPD recomenda também que a definição de violação da segurança seja incluída no artigo 2.º da Directiva «Privacidade e Comunicações Electrónicas», o que é mais coerente com a estrutura global da directiva e permite assegurar maior clareza.

([10]) Em particular, abordam esta questão as alterações do PE n.os 187, 124 a 127 e 27, 21 e 32.

([11]) Excepto nos casos de perigo iminente e directo, em que as entidades abrangidas devem primeiro notificar os consumidores.

([12]) Alínea i) do artigo 2.º da posição comum e da proposta alterada e n.º 3 do artigo 3.º da primeira leitura do PE.

Entidades a serem abrangidas pela obrigação de notificação

22. No âmbito da abordagem do PE, a obrigação de notificar aplica-se tanto aos PPECS como aos ISSP. No entanto, ao abrigo dos sistemas previstos pelo Conselho e pela Comissão, só os PPECS, como as empresas de telecomunicações e os fornecedores de acesso à Internet, serão obrigados a notificar as pessoas objecto de violações da segurança que coloquem em risco os seus dados pessoais. Outros sectores de actividade, por exemplo, os bancos em linha, os retalhistas em linha, os prestadores de serviços de saúde em linha e outros não são vinculados por esta obrigação. Pelas razões acima expostas, a AEPD considera que, numa perspectiva de política pública, é imperativo assegurar que os serviços da sociedade da informação, que incluem as empresas em linha, os bancos em linha, os prestadores de serviços de saúde em linha, etc., sejam também abrangidos pela obrigação de notificar.

23. Em primeiro lugar, a AEPD regista que, se é certo que as empresas de telecomunicações são alvo de violações da segurança que justificam uma obrigação de notificar, o mesmo acontece para outros tipos de empresas/fornecedores. Os retalhistas, bancos e farmácias em linha são tão susceptíveis, senão mais, de sofrer violações da segurança como as empresas de telecomunicações. Por conseguinte, as considerações relativas aos riscos não apoiam a limitação aos PPECS do âmbito de aplicação da obrigação de notificação das violações. A necessidade de uma abordagem mais ampla é ilustrada pela experiência adquirida noutros países. Por exemplo, nos Estados Unidos, quase todos os Estados (mais de 40 até ao momento) promulgaram leis em matéria de notificação de violações da segurança com um âmbito de aplicação mais vasto, que engloba não apenas os PPECS mas também qualquer entidade que detenha os dados pessoais em causa.

24. Em segundo lugar, se a violação dos tipos de dados pessoais tratados de forma regular pelos PPECS pode claramente ter consequências para a privacidade das pessoas, o mesmo se verifica, e talvez até em maior medida, para os tipos de dados pessoais tratados pelos ISSP. Os bancos e outras instituições financeiras podem certamente estar na posse de informações altamente confidenciais (por exemplo, dados das contas bancárias) cuja divulgação pode permitir uma utilização para fins de furto de identidade. Da mesma forma, a divulgação de informações de grande sensibilidade relacionadas com a saúde por serviços de saúde em linha pode ser especialmente lesiva para as pessoas em causa. Assim, os tipos de dados pessoais que podem ser colocados em risco exigem também que a obrigação de notificação das violações da segurança seja aplicada de forma mais ampla e abranja, pelo menos, os ISSP.

25. Foram invocados alguns argumentos jurídicos contra a extensão do âmbito de aplicação deste artigo, ou seja, das entidades abrangidas pela obrigação de notificar. Em especial, o facto de o âmbito de aplicação global da Directiva «Privacidade e Comunicações Electrónicas» apenas dizer respeito aos PPECS foi apresentado como um obstáculo a que a obrigação de notificar se aplique também aos ISSP.

26. Neste contexto, a AEPD gostaria de recordar que: *i)* Não há qualquer tipo de obstáculo jurídico à inclusão de outros actores, para além dos PPECS, no âmbito de aplicação de determinadas disposições da directiva. O legislador comunitário dispõe de plenos poderes discricionários nesta matéria. *ii)* Existem outros precedentes, na Directiva «Privacidade e Comunicações Electrónicas» em vigor, de aplicação a outras entidades que não os PPECS.

27. Por exemplo, o artigo 13.º aplica-se não só aos PPECS mas também a qualquer empresa que envie comunicações não solicitadas, exigindo para tal um consentimento prévio. Por seu lado, o n.º 3 do artigo 5.º da Directiva «Privacidade e Comunicações Electrónicas», que proíbe, nomeadamente, a armazenagem de informações tais como *cookies* no equipamento terminal dos utilizadores, vincula não só os PPECS como também qualquer pessoa que procure armazenar informações ou obter acesso à informação armazenada no equipamento terminal das pessoas em causa. Além disso, no âmbito do processo legislativo em curso, a Comissão até propôs alargar a aplicação do n.º 3 do artigo 5.º aos casos em que as tecnologias deste tipo (*cookies*/*software* espião) são transmitidas não só através de sistemas de comunicações electrónicas mas também por qualquer outro método (distribuição por telecarregamento a partir da internet ou utilização de um suporte externo de armazenamento de dados, nomeadamente CD-ROM, memórias *flash* USB, outros dispositivos de memória *flash*, etc.). Todos estes elementos são de saudar e deverão ser mantidos, constituindo ainda precedentes pertinentes para a presente discussão sobre o âmbito de aplicação.

28. Além disso, no âmbito do processo legislativo em curso, a Comissão e o PE — e pode considerar-se que também o Conselho —, propuseram um novo n.º 6-A para o artigo 6.º, analisado mais adiante, que se aplica a outras entidades que não os PPECS.

29. Por último, tendo em conta os elementos globalmente positivos derivados da obrigação de notificar violações da segurança, é muito provável que os cidadãos esperem beneficiar-se dessas vantagens quando os seus dados pessoais tenham sido colocados em risco não só por PPECS mas também por ISSP. As expectativas dos cidadãos não poderão ser satisfeitas se, por exemplo, não forem notificados quando um banco em linha tiver perdido informações sobre as suas contas bancárias.

30. Em resumo, a AEPD está convicta de que os benefícios da notificação das violações da segurança só se farão plenamente sentir se o âmbito de aplicação das entidades abrangidas incluir tanto os PPECS como os ISSP.

Critério que determina a notificação

31. No que se refere ao critério que determina a notificação, como a seguir explicado mais pormenorizadamente, a AEPD considera que o critério previsto na proposta alterada (existência de uma «*probabilidade razoável de lesar*») é o mais adequado dos três critérios propostos. Contudo, é importante assegurar que o termo «lesar» tenha uma acepção suficientemente ampla para cobrir todas as situações pertinentes de efeitos negativos na privacidade ou noutros interesses legítimos das pessoas singulares. De outra forma, seria preferível criar um novo critério segundo o qual a notificação seja obrigatória «*se for razoável a probabilidade de a violação ter efeitos negativos nas pessoas*».

32. Tal como referido na secção anterior, as condições em que as pessoas devem ser notificadas (designadas por «factor de determinação» ou «critério») variam nas abordagens do PE, da Comissão e do Conselho. Obviamente, o volume de notificações que as pessoas receberem dependerá, em larga medida, do «factor de determinação» ou «critério» previsto para a notificação.

33. No âmbito dos sistemas propostos pelo Conselho e pela Comissão, a notificação deve ter lugar se a violação representar «*um grave risco para a privacidade do assinante*» (Conselho) e se for razoável «*a probabilidade de os interesses dos consumidores serem lesados em consequência da violação*» (Comissão). Ao abrigo do sistema proposto pelo PE, o factor que determina a notificação das pessoas é a «*gravidade da violação*» (ou seja, a notificação das pessoas é exigida quando a violação é considerada «*grave*»). A notificação não é necessária abaixo deste limiar ([13]).

34. A AEPD entende que, se os dados pessoais tiverem sido colocados em risco, poderá defender-se que as pessoas a quem esses dados pertencem têm o direito de ser do facto informadas, em todas as circunstâncias. Todavia, é perfeitamente legítimo analisar se esta é uma solução adequada tendo em conta outros interesses e considerações.

35. Tem sido sugerido que a obrigação de notificar sempre que os dados pessoais tenham sido colocados em risco ou, por outras palavras, sem qualquer limite, pode conduzir a uma sobrenotificação e a uma certa «fatiga» perante tal excesso de notificações, o que poderá gerar um efeito de «dessensibilização». Como adiante descrito mais detalhadamente, a AEPD é sensível a este argumento; no entanto, deseja ao mesmo tempo salientar o seu receio de que a sobrenotificação possa constituir um sinal de falha generalizada das práticas seguidas em matéria de segurança da informação.

36. Como anteriormente referido, a AEPD está ciente das potenciais consequências negativas da sobrenotificação e gostaria de ajudar a garantir que o quadro jurídico adoptado para a notificação das violações da segurança não tenha esse resultado. Se as pessoas passarem a receber frequentes notificações de violação, mesmo nas situações que não geram efeitos negativos ou lesivos nem qualquer apreensão, poderemos acabar por comprometer um dos principais objectivos da notificação, uma vez que as pessoas poderão, paradoxalmente, ignorar as notificações nos casos em que teriam efectivamente necessidade de tomar medidas para se protegerem. Assim, importa estabelecer o equilíbrio certo e assegurar uma notificação pertinente, dado que, se as pessoas não reagirem às notificações recebidas, a eficácia dos sistemas de notificação ficará altamente reduzida.

37. A fim de adoptar um critério adequado que não leve a sobrenotificações, haverá que ter em conta, para além do factor que determina a notificação, outros factores, especialmente a definição de violação da segurança e as informações abrangidas pela obrigação de notificar. A este respeito, a AEPD observa que, no âmbito das três abordagens propostas, o volume de notificações pode vir a ser elevado, tendo em conta a ampla definição de violação da segurança acima analisada. Este receio de sobrenotificação é ainda realçado pelo facto de a definição de violação da segurança abranger todos os tipos de dados pessoais. Embora a AEPD considere que esta (não limitação dos tipos de dados pessoais sujeitos a notificação) é a abordagem correcta, ao contrário de outras abordagens, como as da legislação dos EUA, em que os critérios se centram na sensibilidade das informações, a questão da sobrenotificação não deixa de ser um factor a ter em conta.

38. À luz do acima exposto, e atendendo às diferentes variáveis tomadas em conjunto, a AEPD considera adequado incluir um limiar ou critério abaixo do qual a notificação não seja obrigatória.

39. Os critérios propostos, ou seja, que a violação representa um «*grave risco para a privacidade*» ou tem «*razoável probabilidade de lesar*» parecem ambos abranger, por exemplo, os danos sociais ou os prejuízos para a reputação e as perdas económicas. Por exemplo, esses critérios permitem contemplar as situações de risco de furto de identidade através da divulgação de elementos de identificação não públicos tais como números de passaporte, bem como a exposição das informações relativas à vida privada das pessoas. A AEPD congratula-se com esta abordagem. A AEPD está convicta de que os benefícios da notificação das violações da segurança não serão plenamente atingidos se o sistema de notificação apenas abranger as violações conducentes a prejuízos económicos.

([13]) Ver nota 11 relativa à excepção a esta regra.

40. Dos dois critérios propostos, a AEPD prefere o da Comissão («*razoável probabilidade de lesar*»), uma vez que este permite proporcionar um nível de protecção das pessoas mais adequado. É bastante mais provável que as violações preencham os critérios de notificação se estes se referirem à sua *razoável probabilidade de lesar* a privacidade das pessoas do que se se referirem ao seu *grave risco* de causar tal efeito. Assim, abranger apenas as violações que apresentam um grave risco para a privacidade das pessoas limitará consideravelmente o número de violações a notificar. Além disso, dará um excessivo poder discricionário aos PPECS e aos ISSP para decidir se a notificação é ou não requerida, na medida em que lhes será muito mais fácil justificar conclusões no sentido de que não há qualquer *risco grave* de efeitos lesivos do que no sentido de que não existe *probabilidade razoável de lesar*. Muito embora haja certamente que evitar a sobrenotificação, em última análise deve privilegiar-se a protecção da privacidade das pessoas, que deverão ser protegidas pelo menos quando a violação tenha razoável probabilidade de as lesar. Por outro lado, a expressão *probabilidade razoável* será mais eficaz na prática, tanto para as entidades abrangidas como para as autoridades competentes, uma vez que exige uma avaliação objectiva da situação e do respectivo contexto.

41. Além disso, as violações de dados pessoais podem ter efeitos lesivos susceptíveis de variar e que podem ser difíceis de quantificar. Com efeito, a divulgação de dados do mesmo tipo pode, consoante as circunstâncias de cada caso, lesar significativamente certas pessoas e ter efeitos menos lesivos para outras. Assim, não serão adequados critérios que exijam que os efeitos lesivos sejam substanciais, significativos ou graves. Por exemplo, a abordagem do Conselho, que requer que a violação afecte *gravemente* a privacidade das pessoas, proporciona uma protecção inadequada, na medida em que esse critério exige que o efeito na privacidade seja «grave». Essa opção dá também lugar a avaliações subjectivas.

42. Embora, como acima descrito, a existência de uma *razoável probabilidade de lesar* pareça constituir um critério adequado para a notificação das violações da segurança, a AEPD continua preocupada pelo facto de esta opção poder não cobrir todas as situações que justificam a notificação das pessoas, isto é, todas as situações em que existe uma probabilidade razoável de ocorrência de efeitos negativos na privacidade ou noutros direitos legítimos das pessoas. Por esta razão, poder-se-á analisar a possibilidade de escolher um critério segundo o qual a notificação será obrigatória «*se for razoável a probabilidade de a violação ter efeitos negativos nas pessoas*».

43. Este novo critério oferece a vantagem suplementar da coerência com a legislação da UE em matéria de protecção de dados. Com efeito, a Directiva «Protecção de Dados» refere-se frequentemente aos efeitos negativos nos direitos e nas liberdades das pessoas em causa. Por exemplo, o artigo 18.º e o considerando 49, que dizem respeito à obrigação de notificação das operações de tratamento de dados às autoridades de protecção de dados, autorizam os Estados-Membros a conceder isenções desta obrigação nos casos em que «*o tratamento não seja susceptível de prejudicar os direitos e liberdades das pessoas em causa*». O n.º 6 do artigo 16.º da posição comum apresenta uma redacção semelhante, a fim de permitir que as pessoas colectivas intentem acções contra os autores de *spam*.

44. Além disso, atendendo ao acima exposto, será de esperar que as entidades abrangidas, em especial as autoridades competentes para fazer cumprir a legislação em matéria de protecção de dados, estejam mais familiarizadas com o critério supramencionado, o que deverá facilitar a sua avaliação quanto a saber se determinada violação preenche o critério necessário.

Entidade encarregada de decidir se as violações da segurança preenchem ou não o critério

45. No âmbito da abordagem do PE (excepto em casos de perigo iminente) e da proposta alterada da Comissão, caberá às autoridades dos Estados-Membros decidir se as violações da segurança preenchem ou não o critério que determina a obrigação de notificação das pessoas em causa.

46. A AEPD considera que a participação de uma autoridade na decisão relativa ao preenchimento do critério é importante, na medida em que constitui, até certo ponto, uma garantia de correcta aplicação da lei. Este sistema pode impedir as empresas de avaliarem inadequadamente as violações como não tendo efeitos lesivos/graves e de assim evitarem notificações que, na realidade, são necessárias.

47. Por outro lado, a AEPD receia que um regime que exija que a avaliação seja realizada por autoridades possa ser pouco viável e difícil de aplicar ou possa, na prática, revelar-se contraproducente. Tal regime poderá assim até reduzir as salvaguardas em matéria de protecção de dados das pessoas.

48. Com efeito, no âmbito dessa abordagem, as autoridades de protecção de dados são susceptíveis de ser «inundadas» de notificações de violações da segurança e podem ter de enfrentar sérias dificuldades para proceder às necessárias avaliações. Importa recordar que, para avaliar se determinada violação preenche ou não o critério, as autoridades terão de dispor de suficientes informações internas, frequentemente de carácter técnico complexo, que terão de tratar com grande rapidez. Tendo em conta a dificuldade da avaliação e o facto de algumas autoridades disporem de recursos limitados, a AEPD receia que seja muito difícil às autoridades respeitar esta obrigação e que para tal sejam desviados recursos destinados a outras prioridades importantes. Além disso, um sistema deste tipo pode sujeitar as autoridades a uma pressão excessiva; com efeito, se decidirem que a violação não é grave e no entanto as pessoas em causa sofrerem danos, as autoridades poderão eventualmente ser responsabilizadas.

49. A dificuldade acima referida é ainda sublinhada se se tiver em conta que o tempo é um factor essencial na minimização dos riscos decorrentes das violações da segurança. A não ser que as autoridades possam proceder às avaliações em prazos muito curtos, o tempo suplementar necessário para que realizem as avaliações pode aumentar os danos sofridos pelas pessoas em causa. Por conseguinte, este passo adicional, destinado a proporcionar maior protecção às pessoas, pode paradoxalmente resultar numa diminuição da protecção oferecida em relação aos sistemas baseados na notificação directa.

50. Pelos motivos acima expostos, a AEPD considera que será preferível criar um sistema em que caiba às entidades em causa avaliar se as violações preenchem ou não o critério, tal como previsto na abordagem do Conselho.

51. Todavia, a fim de evitar qualquer risco de eventual abuso, por exemplo de as entidades recusarem proceder à notificação em circunstâncias em que esta é claramente exigível, é da maior importância incluir algumas das salvaguardas em matéria de protecção de dados adiante descritas.

52. Em primeiro lugar, a obrigação de as entidades abrangidas decidirem se devem ou não enviar notificações deve, evidentemente, ser acompanhada da obrigação de notificação às autoridades de todas as violações que preenchem o critério exigido. Nesses casos, as entidades abrangidas deverão ser obrigadas a informar as autoridades da violação e dos motivos subjacentes à sua decisão quanto à notificação, bem como do conteúdo de qualquer notificação enviada.

53. Em segundo lugar, deve ser atribuído às autoridades um real papel de supervisão. No desempenho deste papel, as autoridades devem ter a possibilidade, mas não a obrigação, de investigar as circunstâncias da violação e de exigir as medidas correctivas que possam ser adequadas ([14]). Neste contexto, deverão poder não só exigir a notificação das pessoas (quando ainda não tenha sido realizada), como também impor a obrigação de tomar medidas para evitar novas violações. As autoridades deverão dispor de efectivos poderes e recursos nesta matéria, bem como da margem de manobra necessária para decidir se devem ou não reagir a determinada violação da segurança. Em outras palavras, as autoridades poderão assim ser selectivas e lançar investigações, por exemplo, em caso de violações da segurança de grande dimensão e verdadeiramente lesivas, verificando e fazendo cumprir os requisitos da legislação.

54. Para conseguir o acima exposto, para além dos poderes reconhecidos ao abrigo da Directiva «Privacidade e Comunicações Electrónicas», nomeadamente do n.º 3 do artigo 15.º-A, e da Directiva «Protecção de Dados», a AEPD recomenda que se insira o seguinte texto: «*Se o assinante ou pessoa em causa ainda não tiver sido notificado, a autoridade nacional competente, tendo analisado a natureza da violação, pode exigir ao PPECS ou ao ISSP que proceda a essa notificação*».

55. A AEPD recomenda ainda que o PE e Conselho confirmem a proposta do PE (emenda 122, n.º 1-A do artigo 4.º) de que as entidades têm obrigação de avaliar e identificar os riscos associados aos seus sistemas, bem como aos dados pessoais que tencionam tratar. De acordo com essa obrigação, as entidades deverão definir medidas de segurança adaptadas e precisas, que serão aplicadas aos respectivos casos e que deverão ficar à disposição das autoridades. Em caso de violação da segurança, esta obrigação ajudará as entidades abrangidas — e, eventualmente, também as autoridades, no seu papel de supervisão — a determinar se o facto de as informações em causa terem sido colocadas em risco pode ou não ter efeitos negativos ou lesivos para as pessoas.

56. Em terceiro lugar, a obrigação de as entidades abrangidas decidirem se devem ou não notificar as pessoas deve ser acompanhada da obrigação de manter uma plataforma de auditoria interna pormenorizada e exaustiva que descreva todas as violações ocorridas e respectivas notificações, bem como todas as medidas tomadas para evitar futuras violações. Esta plataforma de auditoria interna deve ser colocada à disposição das autoridades para efeitos de análise e eventual investigação, o que lhes permitirá desempenhar o seu papel de supervisão. Para tal, poder-se-á adoptar uma formulação nos seguintes moldes: «*Os PPECS e os ISSP conservarão e manterão actualizados registos exaustivos que descrevam pormenorizadamente todas as violações de segurança ocorridas, as informações técnicas pertinentes conexas e as medidas correctivas tomadas. Esses registos conterão igualmente uma referência a todas as notificações emitidas aos assinantes ou pessoas em causa e às autoridades nacionais competentes, incluindo a respectiva data e conteúdo. Os registos serão apresentados à autoridade nacional competente a pedido desta*».

57. Evidentemente, para garantir uma implementação coerente deste critério, bem como de outros aspectos pertinentes do quadro relativo às violações da segurança, tais como o formato e os procedimentos de notificação, será conveniente que a Comissão adopte medidas de execução técnica, após consulta da AEPD, do Grupo do Artigo 29.º e das partes interessadas relevantes.

([14]) O n.º 3 do artigo 15.º-A reconhece estes poderes de supervisão ao dispor que «*os Estados-Membros assegurarão que as autoridades nacionais competentes e, se for caso disso, outros organismos nacionais, disponham de todos os poderes e recursos de investigação necessários, nomeadamente a possibilidade de obterem quaisquer informações relevantes de que necessitem para acompanhar e fazer cumprir as disposições nacionais aprovadas nos termos da presente directiva.*».

Destinatários da notificação

58. No que respeita aos destinatários das notificações, a AEPD prefere a terminologia do PE e da Comissão à do Conselho. Com efeito, o PE substituiu o termo «assinantes» por «utilizadores». A Comissão utiliza as expressões «assinante» e «outra pessoa afectada». Tanto a formulação do PE como a da Comissão permitem incluir como destinatários das notificações não só os actuais assinantes como os antigos assinantes e partes terceiras, tais como utilizadores que estabelecem relações com algumas entidades abrangidas sem serem assinantes das mesmas. A AEPD aprecia esta abordagem e convida o PE e o Conselho a mantê-la.

59. Todavia, a AEPD regista um certo número de incoerências em matéria de terminologia na primeira leitura do PE, que deverão ser corrigidas. Por exemplo, o termo «assinantes» foi substituído na maioria dos casos, mas não em todos, por «utilizadores», e noutros casos por «consumidores». O texto deverá ser harmonizado.

III. ÂMBITO DE APLICAÇÃO DA DIRECTIVA «PRIVACIDADE E COMUNICAÇÕES ELECTRÓNICAS»: REDES PÚBLICAS E PRIVADAS

60. O n.º 1 do artigo 3.º da Directiva «Privacidade e Comunicações Electrónicas» em vigor define as principais entidades a que a directiva diz respeito, isto é, aquelas que tratam dados «*no contexto da*» prestação de serviços públicos de comunicações electrónicas nas redes públicas (atrás designados por «PPECS») ([15]). Como exemplos de actividades de PPECS, podem citar-se o fornecimento de acesso à Internet, a transmissão de informações através das redes electrónicas, as ligações de telemóveis e de telefones fixos, etc.

61. O PE aprovou uma emenda (n.º 121) que modifica o artigo 3.º da proposta inicial da Comissão, alargando o âmbito de aplicação da Directiva «Privacidade e Comunicações Electrónicas» por forma a incluir o «*tratamento de dados pessoais no contexto do fornecimento de serviços de comunicações electrónicas publicamente disponíveis em redes de comunicações públicas e privadas e em redes privadas acessíveis ao público na Comunidade, […]*» (n.º 1 do artigo 3.º da Directiva «Privacidade e Comunicações Electrónicas»). Infelizmente, o Conselho e a Comissão não estiveram em condições de aceitar esta emenda, pelo que não incluíram esta abordagem na posição comum nem na proposta alterada.

Aplicação da Directiva «Privacidade e Comunicações Electrónicas» às redes privadas acessíveis ao público

62. Pelas razões a seguir expostas, e para ajudar a promover um consenso, a AEPD exorta a que se mantenha o espírito da emenda 121. A AEPD sugere ainda que se inclua uma alteração que permita clarificar melhor os tipos de serviços abrangidos pelo âmbito de aplicação alargado.

63. As redes privadas são frequentemente utilizadas para fornecer serviços de comunicações electrónicas, tais como o acesso à internet, a um número indefinido de pessoas, que pode ser potencialmente elevado. É o que acontece, por exemplo, no caso do acesso à internet nos cibercafés, bem como nos pontos de acesso sem fios disponíveis nos hotéis, restaurantes, aeroportos, comboios e outros estabelecimentos abertos ao público em que este tipo de serviço é muitas vezes oferecido como complemento de outros serviços (bebidas, alojamento, etc.).

64. Em todos os exemplos acima referidos, o serviço de comunicações em causa, nomeadamente o acesso à internet, é disponibilizado ao público, não através de uma rede pública, mas antes de uma rede que se pode considerar privada, isto é, uma rede operada por entidades privadas. Além disso, embora nos casos supramencionados o serviço de comunicações seja fornecido ao público, o facto de a rede utilizada ser privada e não pública faz com que *se possa defender* que as disposições da Directiva «Privacidade e Comunicações Electrónicas», ou pelo menos algumas delas, não se aplicam à prestação desse serviço ([16]). Consequentemente, os direitos fundamentais das pessoas singulares garantidos pela Directiva «Privacidade e Comunicações Electrónicas» não são protegidos nesses casos e é criada uma situação jurídica desigual entre os utilizadores que acedem aos serviços de acesso internet através de telecomunicações públicas e aqueles que o fazem através de telecomunicações privadas, apesar de o risco para a privacidade e os dados pessoais das pessoas, em todos os casos acima referidos, ser idêntico ao que existe quando o serviço é fornecido através de redes públicas. Em resumo, não parece haver *razões* que justifiquem a diferença de tratamento, ao abrigo da directiva, entre os serviços de comunicações fornecidos através de redes privadas e os fornecidos através de redes públicas.

65. Assim, a AEPD é favorável a uma alteração, como a emenda 121 do PE, que preveja que a Directiva «Privacidade e Comunicações Electrónicas» se aplica também ao tratamento de dados pessoais no contexto do fornecimento de serviços de comunicações electrónicas publicamente disponíveis em redes de comunicações *privadas*.

66. Todavia, a AEPD reconhece que esta formulação poderá acarretar consequências imprevisíveis e eventualmente indesejadas. Com efeito, a mera referência às redes privadas

([15]) «A presente directiva é aplicável ao tratamento de dados pessoais no contexto da prestação de serviços de comunicações electrónicas publicamente disponíveis nas redes públicas de comunicações».

([16]) Poderá também argumentar-se, em sentido contrário, que o facto de o serviço de comunicações ser fornecido ao público, mesmo tratando-se de uma rede privada, implica que a prestação desse serviço é abrangida pelo quadro jurídico existente, apesar de a rede ser privada. De facto, por exemplo na França os empregadores que fornecem um acesso Internet aos seus empregados têm sido equiparados aos fornecedores de acesso internet que oferecem esse acesso a título comercial. Esta interpretação não é amplamente aceite.

poderá ser interpretada como abrangendo situações que claramente não se destinam a ser abrangidas pela directiva. Por exemplo, poder-se-á afirmar que uma interpretação literal ou estrita desta formulação pode implicar que os proprietários de casas equipadas com sistemas sem fios ([17]), que permitem a ligação de qualquer pessoa dentro do seu raio de acção (geralmente a própria casa) são abrangidos pelo âmbito de aplicação da directiva, mesmo não sendo esta a intenção da emenda 121. A fim de evitar esta interpretação, a AEPD sugere que a emenda 121 seja reformulada, nomeadamente no que se refere ao âmbito de aplicação da Directiva «Privacidade e Comunicações Electrónicas», passando a ter a seguinte redacção: «*tratamento de dados pessoais no contexto do fornecimento de serviços de comunicações electrónicas publicamente disponíveis em redes de comunicações públicas ou em redes de comunicações privadas acessíveis ao público na Comunidade, …*».

67. Esta nova formulação ajudará a clarificar que só as redes privadas acessíveis ao público serão abrangidas pela Directiva «Privacidade e Comunicações Electrónicas». Ao prever que as disposições da Directiva «Privacidade e Comunicações Electrónicas» se apliquem *apenas* às *redes privadas acessíveis ao público* (e não a todas as redes privadas), limitar-se-á o âmbito de aplicação da directiva por forma a que abranja apenas os serviços de comunicações fornecidos através de redes privadas que são intencionalmente tornados *acessíveis* ao público. Esta formulação ajudará a sublinhar ainda mais que a *acessibilidade* da rede privada *ao público em geral* é o principal factor para a determinação das entidades abrangidas pela directiva (para além do fornecimento de um serviço de comunicações publicamente disponível). Por outras palavras, independentemente da sua natureza pública ou privada, se a rede for intencionalmente tornada acessível ao público para o fornecimento de um serviço público de comunicações, como o acesso Internet, e mesmo que esse serviço seja complementar de outro serviço (por exemplo, alojamento num hotel), o serviço/rede em causa ficará abrangido pela Directiva «Privacidade e Comunicações Electrónicas».

68. A AEPD observa que a abordagem acima defendida, que prevê que as disposições da Directiva «Privacidade e Comunicações Electrónicas» se apliquem às *redes privadas acessíveis ao público*, é coerente com as abordagens adoptadas em vários Estados-Membros em que as autoridades já consideraram que este tipo de serviços, bem como os serviços fornecidos em redes meramente privadas, são abrangidos pelo âmbito de aplicação das disposições nacionais de execução da directiva ([18]).

69. Para reforçar a segurança jurídica no que se refere às entidades abrangidas pelo novo âmbito de aplicação, poderá ser útil introduzir na Directiva «Privacidade e Comunicações Electrónicas» uma alteração que defina as «redes privadas acessíveis ao público»; essa alteração poderá ter a seguinte redacção: «*rede privada acessível ao público é uma rede operada por entidades privadas a que o público em geral tem normalmente acesso sem quaisquer restrições, a título oneroso ou gratuito, ou no contexto de outros serviços ou ofertas, sujeito à aceitação dos termos e condições aplicáveis*».

70. Na prática, a abordagem acima referida significa que serão abrangidas as redes privadas nos hotéis e outros estabelecimentos que fornecem um acesso internet ao público em geral através de uma rede privada. Inversamente, não será abrangido o fornecimento de serviços de comunicações em redes exclusivamente privadas em que o serviço se restrinja a um grupo limitado de pessoas identificáveis. Por conseguinte, não serão abrangidas, por exemplo, as redes privadas virtuais nem as casas de consumidores equipadas com sistemas sem fios. Também não serão abrangidos os serviços fornecidos através de redes exclusivamente empresariais.

Redes privadas abrangidas pelo âmbito de aplicação da Directiva «Privacidade e Comunicações Electrónicas»

71. A exclusão das redes privadas enquanto tais, como acima sugerido, deverá ser considerada uma medida temporária sujeita a posterior debate. Com efeito, esta opção poderá ter de ser reconsiderada, atendendo, por um lado, às implicações, em termos de privacidade, da exclusão das redes exclusivamente privadas enquanto tais e, por outro, ao facto de essa exclusão afectar um grande número de pessoas que habitualmente acedem à Internet através de redes empresariais. Por este motivo, e a fim de fomentar o debate sobre esta questão, a AEPD recomenda a inclusão, na Directiva «Privacidade e Comunicações Electrónicas», de um considerando que preveja que a Comissão realizará uma consulta pública sobre a aplicação da directiva a todas as redes privadas, com o contributo da AEPD, das autoridades de protecção de dados e de outras partes interessadas pertinentes. Esse considerando poderá ainda especificar que, na sequência dessa consulta pública, a Comissão deverá elaborar uma proposta adequada para alargar ou limitar os tipos de entidades a abranger pela directiva.

72. Além do acima exposto, os artigos da Directiva «Privacidade e Comunicações Electrónicas» deverão ser alterados em conformidade, de forma que todas as disposições operacionais se refiram explicitamente não só às redes públicas como também às redes privadas acessíveis ao público.

IV. **TRATAMENTO DE DADOS DE TRÁFEGO PARA FINS DE SEGURANÇA**

73. Durante o processo legislativo relacionado com a revisão da Directiva «Privacidade e Comunicações Electrónicas», as empresas que prestam serviços de segurança insistiram em que era necessário introduzir na directiva uma disposição que legitimasse a recolha de dados de tráfego para garantir uma efectiva segurança em linha.

([17]) Tipicamente redes locais sem fios.
([18]) Ver nota 16.

74. Em consequência, o PE introduziu a emenda 181, que criou um novo n.º 6-A do artigo 6.º que autoriza expressamente o tratamento de dados de tráfego para fins de segurança: «*Sem prejuízo do respeito de outras disposições para além das que figuram no artigo 7.º da Directiva 95/46/CE e no artigo 5.º da presente directiva, os dados relativos ao tráfego podem ser tratados no interesse legítimo do controlador dos dados para fins de aplicação de medidas técnicas destinadas a garantir a segurança das redes e da informação, nos termos da alínea c) do artigo 4.º do Regulamento (CE) n.º 460/2004 do Parlamento Europeu e do Conselho, de 10 de Março de 2004, que cria a Agência Europeia para a Segurança das Redes e da Informação, de um serviço público de comunicações electrónicas, de uma rede pública ou privada de comunicações electrónicas, de um serviço da sociedade da informação ou do respectivo equipamento terminal e de comunicação electrónica, salvo se os direitos fundamentais e as liberdades da pessoa em questão prevalecerem sobre o referido interesse. Esse tratamento deve restringir-se ao estritamente necessário para efeitos de actividades em matéria de segurança.*».

75. Na sua proposta alterada, a Comissão aceitou esta emenda quanto ao seu princípio, mas suprimiu uma cláusula essencial destinada a assegurar que as restantes disposições da directiva devem ser respeitadas, a saber a seguinte: «*sem prejuízo […] da presente directiva*». O Conselho aprovou uma versão reformulada, que enfraquece mais um pouco as importantes protecções e equilíbrios de interesses proporcionados pela emenda 181, tendo adoptado a seguinte redacção: «*Os dados de tráfego podem ser tratados, na medida do estritamente necessário, para garantir […] a segurança das redes e da informação, na acepção da alínea c) do artigo 4.º do Regulamento (CE) n.º 460/2004 do Parlamento Europeu e do Conselho, de 10 de Março de 2004, que cria a Agência Europeia para a Segurança das Redes e da Informação*».

76. Conforme adiante explicado mais detalhadamente, o n.º 6-A do artigo 6.º é desnecessário e apresenta riscos de utilização abusiva, em especial se for adoptado sob uma forma que não inclua importantes salvaguardas, cláusulas relativas ao respeito das outras disposições da directiva e equilíbrios de interesses. Por conseguinte, a AEPD recomenda que se rejeite esta disposição ou, pelo menos, se assegure que qualquer disposição sobre esta questão inclua os tipos de salvaguardas previstos na emenda 181 tal como adoptada pelo PE.

Fundamentos jurídicos para o tratamento de dados de tráfego aplicáveis aos serviços de comunicações electrónicas e outros responsáveis pelo tratamento de dados no âmbito da legislação relativa à protecção de dados em vigor

77. As possibilidades de tratamento legal de dados de tráfego por fornecedores de serviços de comunicações electrónicas publicamente disponíveis são reguladas pelo artigo 6.º da Directiva «Privacidade e Comunicações Electrónicas», que restringe o tratamento de dados de tráfego a um número limitado de fins tais como a facturação, a interligação e a comercialização. O tratamento destes dados só pode ser realizado em determinadas condições, como o consentimento das pessoas em causa na hipótese de comercialização. Além disso, outros responsáveis pelo tratamento de dados, tais como os prestadores de serviços da sociedade da informação, podem tratar dados de tráfego ao abrigo do artigo 7.º da Directiva «Protecção de Dados», que dispõe que os responsáveis pelo tratamento de dados podem tratar dados pessoais se cumprirem pelo menos uma das bases jurídicas (também designadas por fundamentos jurídicos) enumeradas.

78. Como exemplo de uma dessas bases jurídicas, pode mencionar-se a alínea a) do artigo 7.º da Directiva «Protecção de Dados», que exige o consentimento da pessoa em causa. Por exemplo, se um retalhista em linha desejar tratar dados de tráfego para efeitos de publicidade ou *marketing*, tem de obter o consentimento da pessoa em causa. Outra base jurídica prevista no artigo 7.º pode permitir, em certos casos, o tratamento de dados de tráfego para fins de segurança por, nomeadamente, empresas de segurança que oferecem serviços de segurança. Esta possibilidade baseia-se na alínea f) do artigo 7.º que dispõe que os responsáveis pelo tratamento de dados podem tratar dados pessoais se «*for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa …*». A Directiva «Protecção de Dados» não especifica as situações em que o tratamento de dados pessoais satisfaz este requisito. Em vez disso, a decisão é tomada pelos responsáveis pelo tratamento de dados, caso a caso, frequentemente com a concordância das autoridades nacionais de protecção de dados e outras autoridades.

79. Há que analisar a articulação entre o artigo 7.º da Directiva «Protecção de Dados» e a proposta de n.º 6-A do artigo 6.º da Directiva «Privacidade e Comunicações Electrónicas». A proposta de n.º 6-A do artigo 6.º especifica as circunstâncias em que são cumpridos os requisitos da alínea f) do artigo 7.º acima descrita. Com efeito, ao autorizar o tratamento de dados de tráfego para ajudar a garantir a segurança das redes e da informação, o n.º 6-A do artigo 6.º permite esse tratamento para prosseguir interesses legítimos do responsável pelo tratamento de dados.

80. Como adiante explicado mais pormenorizadamente, a AEPD considera que a proposta do n.º 6-A do artigo 6.º não é nem necessária nem útil. Com efeito, de um ponto de vista jurídico, em princípio, é desnecessário estabelecer se determinado tipo de actividade de tratamento de dados — aqui o tratamento de dados de tráfego para fins de segurança — cumpre os requisitos da alínea f) do artigo 7.º da Directiva «Protecção de Dados» ou não; neste caso, poderá ser exigível o consentimento da pessoa em causa, por força da alínea a) do artigo 7.º. Como acima referido, esta avaliação é normalmente levada

a cabo pelos responsáveis pelo tratamento de dados, isto é, pelas empresas, a nível de execução, em concertação com as autoridades de protecção de dados e, se necessário, pelos tribunais. Em termos gerais, a AEPD considera que, em casos específicos, o tratamento legítimo de dados de tráfego para fins de segurança, efectuado sem prejudicar os direitos e liberdades fundamentais das pessoas em causa, é susceptível de cumprir os requisitos da alínea f) do artigo 7.º da Directiva «Protecção de Dados», e pode por isso ser realizado. Além disso, não há qualquer outro precedente nas Directivas «Protecção de Dados» e «Privacidade e Comunicações Electrónicas» no sentido de prever isenções ou disposições especiais para certos tipos de actividades de tratamento de dados que satisfazem os requisitos da alínea f) do artigo 7.º, nem tem sido demonstrada a necessidade de tal excepção. Pelo contrário, como acima observado, afigura-se que, em muitas circunstâncias, este tipo de actividade está claramente contemplado no texto actual. Por conseguinte, é em princípio desnecessária uma disposição jurídica que confirme esta avaliação.

Versões do PE, do Conselho e da Comissão do n.º 6-A do artigo 6.º

81. Como acima explicado, importa salientar que, embora desnecessária, a emenda 181, tal como aprovada pelo PE, foi redigida, até certo ponto, tendo em conta princípios de protecção da privacidade e dos dados consagrados na legislação relativa à protecção de dados. A emenda 181 do PE poderá atender ainda mais aos interesses da protecção de dados e da privacidade, por exemplo, através da inserção da expressão «em casos específicos» para garantir a aplicação selectiva deste artigo, ou através da inclusão de um período de conservação específico.

82. A emenda 181 contém alguns elementos positivos. Confirma que o tratamento deverá respeitar qualquer outro princípio em matéria de protecção de dados aplicável ao tratamento de dados pessoais («*sem prejuízo do respeito de outras disposições […] da Directiva 95/46/CE e […] da presente directiva*»). Além disso, embora permita o tratamento de dados de tráfego para fins de segurança, a emenda 181 estabelece um equilíbrio entre os interesses da entidade que trata os dados de tráfego e os das pessoas cujos dados são tratados, de modo a que o tratamento dos dados só possa ser realizado se os direitos e liberdades fundamentais da pessoa em causa não prevalecerem sobre os interesses da entidade que trata os dados («*salvo se os direitos fundamentais e as liberdades da pessoa em questão prevalecerem sobre o referido interesse*»). Este requisito é essencial na medida em que pode permitir o tratamento de dados de tráfego em casos específicos; todavia, não permite que uma entidade trate dados de tráfego em bloco.

83. A versão da emenda reformulada pelo Conselho contém elementos positivos, nomeadamente o facto de manter a expressão «*estritamente necessário*», que realça o carácter limitado do âmbito de aplicação deste artigo. Todavia, a versão do Conselho suprime as salvaguardas em matéria de protecção de dados e de privacidade acima referidas. Embora, em princípio, se apliquem as disposições gerais relativas à protecção de dados, quer sejam ou não feitas referências específicas em cada caso, a versão do Conselho do n.º 6 do artigo 6.º-A pode ser interpretada como conferindo plenos poderes discricionários para o tratamento de dados de tráfego sem qualquer das salvaguardas em matéria de protecção de dados e privacidade aplicáveis sempre que são tratados dados de tráfego. Por conseguinte, poderá defender-se que os dados de tráfego podem ser recolhidos, armazenados e posteriormente utilizados sem que seja necessário respeitar os princípios e as obrigações específicas em matéria de protecção de dados de outro modo aplicáveis aos responsáveis, tais como o princípio da qualidade ou a obrigação de o tratamento ser efectuado de forma lícita e leal e de os dados serem mantidos confidenciais e conservados de forma segura. Além disso, como o artigo não inclui qualquer referência aos princípios de protecção de dados que impõem limites temporais para o armazenamento das informações ou prazos específicos, a versão do Conselho pode ser interpretada no sentido de permitir a recolha e o tratamento de dados de tráfego para fins de segurança por um período indefinido.

84. O Conselho enfraqueceu, ainda, a protecção da privacidade nalgumas partes do texto, ao utilizar uma formulação potencialmente mais abrangente. Por exemplo, a referência ao «*interesse legítimo do controlador dos dados*» foi suprimida, o que levanta dúvidas quanto ao tipo de entidades que poderão prevalecer-se desta excepção. É da maior importância evitar abrir a possibilidade a que qualquer utilizador ou entidade jurídica beneficie desta alteração.

85. As recentes experiências do PE e do Conselho demonstram que é difícil definir por lei o âmbito e as condições em que o tratamento de dados para fins de segurança pode ser legalmente realizado. É improvável que algum artigo, já existente ou novo, permita suprimir os riscos evidentes de aplicação excessivamente ampla da excepção acima referida, por motivos não exclusivamente relacionados com a segurança ou por entidades que não deveriam poder beneficiar dessa excepção. Isto não significa que tal tratamento não deve nunca ter lugar. No entanto, a questão de saber se e em que medida pode ser efectuado poderá ser mais bem avaliada a nível de execução. As entidades que pretendam realizar tal tratamento deverão discutir o respectivo âmbito e condições de aplicação com as autoridades de protecção de dados e, eventualmente, com o Grupo do Artigo 29.º. Em alternativa, a Directiva «Privacidade e Comunicações Electrónicas» poderá incluir um artigo que permita o tratamento de dados de tráfego para fins de segurança sob reserva de autorização expressa das autoridades de protecção de dados.

86. Tendo em conta, por um lado, os riscos que o n.º 6-A do artigo 6.º coloca para o direito fundamental das pessoas singulares à protecção dos dados e à privacidade e, por outro, o facto de, tal como explicado no presente parecer, essa disposição ser desnecessária de um ponto de vista jurídico, a AEPD chegou à conclusão de que a melhor solução consistirá em suprimir inteiramente essa disposição.

87. Se, contra a recomendação da AEPD, for aprovado algum texto nos moldes da actual versão do n.º 6-A do artigo 6.º, tal texto deverá em qualquer caso incorporar as salvaguardas em matéria de protecção de dados acima analisadas. Deverá ainda ser adequadamente integrado na estrutura existente do artigo 6.º, de preferência enquanto novo n.º 2-A.

V. **CAPACIDADE DE AS PESSOAS COLECTIVAS INTENTAREM ACÇÕES POR INFRACÇÃO À DIRECTIVA «PRIVACIDADE E COMUNICAÇÕES ELECTRÓNICAS»**

88. O PE aprovou a emenda 133, que permite que os fornecedores de acesso à internet e outras entidades jurídicas como as associações de consumidores intentem acções junto dos tribunais contra os infractores de qualquer disposição da Directiva «Privacidade e Comunicações Electrónicas» ([19]). Infelizmente, nem a Comissão nem o Conselho aceitaram esta emenda. A AEPD considera esta emenda muito positiva e recomenda que seja mantida.

89. Para entender a importância desta emenda, é necessário ter em mente que, em matéria de privacidade e de protecção de dados, o prejuízo causado à pessoa em causa, considerada individualmente, não é em geral só por si suficiente para que esta intente uma acção judicial. As pessoas geralmente não recorrem aos tribunais por sua própria iniciativa por terem recebido *spams* ou por o seu nome ter sido indevidamente incluído numa lista. Esta emenda permitirá às associações de consumidores e aos sindicatos que representam os interesses dos consumidores, a nível colectivo, intentar acções judiciais em seu nome. O facto de dispor de uma mais ampla diversidade de mecanismos para fazer cumprir a lei é susceptível de estimular um maior respeito da mesma, sendo por isso no interesse da aplicação eficaz das disposições da Directiva «Privacidade e Comunicações Electrónicas».

90. Existem precedentes jurídicos nos quadros jurídicos de alguns Estados-Membros, que já prevêem a possibilidade de recurso colectivo a fim de permitir que os consumidores ou grupos de interesses exijam reparação pela parte responsável pelos prejuízos causados.

91. Além disso, em alguns Estados-Membros ([20]) o direito da concorrência autoriza os consumidores e os grupos de interesses (para além do *concorrente afectado*) a intentarem uma acção judicial contra a entidade infractora. A lógica subjacente a esta abordagem é a de que as empresas que infringem o direito da concorrência são susceptíveis de beneficiar do facto de os consumidores que sofrem apenas prejuízos marginais terem geralmente relutância em intentar acções judiciais. Esta lógica pode ser aplicada, *mutatis mutandis*, no domínio da protecção de dados e da privacidade.

92. Mais importante ainda, como acima referido, permitir que as entidades jurídicas como as associações de consumidores e os PPECS intentem acções judiciais fortalece a posição dos consumidores e promove o cumprimento, em termos globais, da legislação relativa à protecção de dados. Se as empresas infractoras correrem maior risco de ser processadas, é provável que passem a investir mais no respeito da legislação relativa à protecção de dados, o que a longo prazo aumentará o nível de protecção da privacidade e dos consumidores. Por todos estes motivos, a AEPD convida o PE e o Conselho a aprovar uma disposição que autorize as entidades jurídicas a intentar acções judiciais contra os infractores de qualquer disposição da Directiva «Privacidade e Comunicações Electrónicas».

([19]) N.º 6 do artigo 13.º da primeira leitura do PE.

([20]) Ver, por exemplo, o parágrafo 8 da UWG — Lei alemã sobre a concorrência desleal.

VI. **CONCLUSÃO**

93. A posição comum do Conselho, a primeira leitura do Parlamento Europeu e a proposta alterada da Comissão contêm, em graus diversos, elementos positivos que poderão servir para reforçar a protecção da privacidade e dos dados pessoais das pessoas singulares.

94. Todavia, a AEPD considera que é possível introduzir melhorias, em especial no que respeita à posição comum do Conselho que, infelizmente, não manteve algumas das alterações do PE destinadas a ajudar a assegurar uma adequada protecção da privacidade e dos dados pessoais das pessoas singulares. A AEPD insta o PE e o Conselho a restabelecerem as salvaguardas em matéria de privacidade incorporadas na primeira leitura do PE.

95. A AEPD considera, ainda, que é oportuno racionalizar algumas das disposições da directiva. Esta racionalização é especialmente necessária no caso das disposições relativas à violação da segurança, uma vez que a AEPD entende que os benefícios da notificação das violações só se farão plenamente sentir se o respectivo quadro jurídico for fixado desde o início. Por último, a AEPD considera igualmente oportuno melhorar e clarificar a formulação de algumas disposições da directiva.

96. Tendo em conta o acima exposto, a AEPD insta o PE e o Conselho a redobrarem os esforços para melhorar e clarificar algumas disposições da Directiva «Privacidade e Comunicações Electrónicas», restabelecendo simultaneamente as alterações adoptadas pelo PE em primeira leitura destinadas a proporcionar um nível adequado de protecção da privacidade e dos dados. Para este fim, os pontos 97, 98, 99 e 100 *infra* fazem uma síntese das questões em jogo e apresentam algumas recomendações e propostas de redacção. A AEPD apela a todas as partes envolvidas para que as tenham em conta ao longo do processo conducente à aprovação final da Directiva «Privacidade e Comunicações Electrónicas».

Violação da segurança

97. O Parlamento Europeu, a Comissão e o Conselho adoptaram todos abordagens diferentes para a notificação das violações da segurança. As diferenças entre os três modelos dizem respeito, respectivamente, às entidades abrangidas pela obrigação, ao factor ou critério que determina a notificação, às pessoas com direito a serem notificadas, etc. O PE e o Conselho deverão fazer tudo o que estiver ao seu alcance para elaborar um quadro jurídico sólido em matéria de violação da segurança. Para tal, o PE e o Conselho deverão:

— *Manter* a definição de violação da segurança contida nos textos do PE, do Conselho e da Comissão, uma vez que é suficientemente ampla para abarcar a maioria das situações relevantes susceptíveis de justificar a notificação de violações da segurança;

— No que se refere às entidades a abranger pelo requisito de notificação proposto, *incluir* os prestadores de serviços da sociedade da informação. Os retalhistas, bancos e farmácias em linha são tão susceptíveis, senão mais, de sofrer violações de segurança quanto as empresas de telecomunicações. Os cidadãos esperam ser notificados não só quando os fornecedores de acesso à Internet sejam objecto de violações da segurança mas também, muito especialmente, quando sejam os seus bancos e farmácias em linha a ser afectados;

— No que toca ao factor que determina a notificação, o critério enunciado na proposta alterada (existência de uma «*probabilidade» razoável «de lesar*») é adequado e garante um bom funcionamento do sistema. Contudo, importa assegurar que o termo «lesar» tenha uma acepção suficientemente ampla para cobrir todas as situações pertinentes de efeitos negativos na privacidade ou noutros interesses legítimos das pessoas singulares. De outra forma, será preferível criar um novo critério segundo o qual a notificação será obrigatória «*se for razoável a probabilidade de a violação ter efeitos negativos nas pessoas*». A abordagem do Conselho, que requer que a violação afecte *gravemente* a privacidade das pessoas, proporciona uma protecção inadequada, na medida em que esse critério exige que o efeito na privacidade seja «grave». Essa opção dá também lugar a avaliações subjectivas;

— Embora a participação de uma autoridade para determinar se a entidade abrangida deve ou não notificar as pessoas tenha certamente efeitos positivos, poderá ser pouco viável e difícil de aplicar, podendo ainda desviar recursos destinados a outras prioridades importantes. Se as autoridades não puderem reagir com extrema rapidez, a AEPD receia que um sistema deste tipo possa até diminuir a protecção das pessoas singulares e sujeitar as autoridades a uma pressão excessiva. Assim, globalmente, a AEPD preconiza *criar* um sistema em que caiba às entidades em causa avaliar se devem ou não proceder à notificação;

— Para permitir às autoridades supervisionar as avaliações realizadas pelas entidades abrangidas quanto à questão da notificação, *implementar* as seguintes salvaguardas:

  — *garantir* que as entidades abrangidas sejam obrigadas a notificar as autoridades de todas as violações que preenchem o critério exigido,

  — *atribuir* às autoridades um papel de supervisão que lhes permita ser selectivas, a fim de garantir a sua eficácia. Para tal, inserir o seguinte texto: «*Se o assinante ou pessoa em causa ainda não tiver sido notificado, a autoridade nacional competente, tendo analisado a natureza da violação, pode exigir ao PPECS ou ao ISSP que proceda a essa notificação*»,

  — *aprovar* uma nova disposição que exija que as entidades mantenham uma plataforma de auditoria interna pormenorizada e exaustiva. Para tal, poder-se-á adoptar a seguinte formulação: «*Os PPECS e os ISSP deverão conservar e manter actualizados registos exaustivos que descrevam pormenorizadamente todas as violações da segurança ocorridas, as informações técnicas pertinentes conexas e as medidas correctivas tomadas. Esses registos deverão conter igualmente uma referência a todas as notificações emitidas aos assinantes ou pessoas em causa e às autoridades nacionais competentes, incluindo a respectiva data e conteúdo. Os registos deverão ser apresentados à autoridade nacional competente a pedido desta.*»;

— Para garantir uma implementação coerente do quadro jurídico relativo às violações da segurança, *dar* à Comissão a possibilidade de adoptar medidas de execução técnicas, após consulta prévia da AEPD, do Grupo do Artigo 29.º e de outras partes interessadas relevantes;

— No que respeita às pessoas a notificar, *utilizar* a terminologia da Comissão ou do PE (*pessoas em causa* ou *utilizadores afectados*), uma vez que abrange todas as pessoas cujos dados pessoais tenham sido colocados em risco.

Redes privadas acessíveis ao público

98. Os serviços de comunicações são frequentemente disponibilizados ao público não através de redes públicas, mas sim de redes operadas por entidades privadas (por exemplo, pontos de acesso sem fios disponíveis em hotéis ou aeroportos), que se podem considerar não abrangidas pela directiva. O PE aprovou a emenda 121 (artigo 3.º), que alarga o âmbito de aplicação da directiva por forma a incluir as redes de comunicações públicas e privadas e as redes privadas acessíveis ao público. A este respeito, o PE e o Conselho deverão:

— *Manter* o espírito da emenda 121, mas *reformulando*-a de modo a que o âmbito de aplicação da Directiva «Privacidade e Comunicações Electrónicas» inclua apenas o «*tratamento de dados pessoais no contexto do fornecimento de serviços de comunicações electrónicas publicamente disponíveis em redes de comunicações públicas ou em redes de comunicações privadas acessíveis ao público na Comunidade*». As redes exclusivamente privadas (ao contrário das redes privadas acessíveis ao público) não serão assim explicitamente abrangidas;

— *Alterar* todas as disposições operacionais em conformidade, de modo que se refiram explicitamente não só às redes públicas como também às redes privadas acessíveis ao público;

— *Incluir uma alteração com a seguinte definição: «rede privada acessível ao público é uma rede operada por entidades privadas a que o público em geral tem normalmente acesso sem quaisquer restrições, a título oneroso ou gratuito, ou no contexto de outros serviços ou ofertas, sob reserva de aceitação dos termos e condições aplicáveis»*. Desse modo, reforçar-se-á a segurança jurídica no que se refere às entidades abrangidas pelo novo âmbito de aplicação;

— *Adoptar* um novo considerando segundo o qual a Comissão realizará uma consulta pública sobre a aplicação da Directiva «Privacidade e Comunicações Electrónicas» a todas as redes privadas, com o contributo da AEPD, do Grupo do Artigo 29.º e de outras partes interessadas pertinentes. Especificar que, na sequência dessa consulta pública, a Comissão deverá elaborar as propostas adequadas para alargar ou limitar os tipos de entidades a abranger pela Directiva «Privacidade e Comunicações Electrónicas».

Tratamento de dados de tráfego para fins de segurança

99. Em primeira leitura, o PE aprovou a emenda 181 (n.º 6 do artigo 6.º-A), que autoriza o tratamento dos dados de tráfego para fins de segurança. Na sua posição comum, o Conselho aprovou uma nova versão que enfraquece algumas das salvaguardas em matéria de privacidade. A este respeito, a AEPD recomenda que o PE e o Conselho:

— *Rejeitem* esta disposição na sua totalidade, uma vez que é desnecessária e que, em caso de utilização abusiva, poderá ameaçar indevidamente a protecção de dados e a privacidade das pessoas singulares;

— Em alternativa, caso seja aprovada uma variante da versão actual do n.º 6 do artigo 6.º-A, *incorporem* as salvaguardas em matéria de protecção de dados analisadas no presente parecer (semelhantes às constantes da emenda do PE).

Acções intentadas em caso de infracção à Directiva «Privacidade e Comunicações Electrónicas»

100. O Parlamento aprovou a emenda 133 (n.º 6 do artigo 13.º), que dá às entidades jurídicas a possibilidade de intentar acções junto dos tribunais contra os infractores de qualquer disposição da directiva. Infelizmente, o Conselho não manteve esta emenda. O Conselho e o PE deverão:

— *Aprovar* a disposição que confere às entidades jurídicas, tais como as associações de consumidores e associações profissionais, a possibilidade de intentar acções judiciais em caso de infracção a qualquer disposição da directiva (e não apenas em caso de infracção das disposições relativas ao *spam*, como prevêem actualmente a posição comum e a proposta alterada). O facto de dispor de uma mais ampla diversidade de mecanismos para fazer cumprir a lei estimulará um maior respeito da mesma e uma eficaz aplicação das disposições da Directiva «Privacidade e Comunicações Electrónicas» no seu conjunto.

Resposta ao desafio

101. Em todas as questões acima debatidas, o PE e o Conselho devem dar resposta ao desafio que consiste na definição de regras e disposições adequadas que sejam simultaneamente viáveis e funcionais e que respeitem os direitos das pessoas singulares em matéria de privacidade e protecção de dados. A AEPD espera que as partes envolvidas envidem os maiores esforços para responder a este desafio e que o presente parecer permita contribuir para esses esforços.

Feito em Bruxelas, em 9 de Janeiro de 2009.

Autoridade Europeia para a Protecção de Dados

Peter HUSTINX