I

(Resoluções, recomendações e pareceres)

PARECERES

AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS

Parecer da Autoridade Europeia para a Protecção de Dados sobre a proposta de directiva do Parlamento Europeu e do Conselho que altera, nomeadamente, 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).

(2008/C 181/01)

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 ([1]),

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 ([2]),

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 órgãos comunitários e à livre circulação desses dados ([3]), designadamente o artigo 41.º,

Tendo em conta o pedido de parecer nos termos do n.º 2 do artigo 28.º do Regulamento (CE) n.º 45/2001, recebido da Comissão Europeia em 16 de Novembro de 2007,

APROVOU O SEGUINTE PARECER:

I. INTRODUÇÃO

1. Em 13 de Novembro de 2007, a Comissão aprovou uma proposta de directiva que altera, nomeadamente, a Directiva 2002/58/CE relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (a seguir designada por «proposta» ou por «alterações propostas»). A actual versão da Directiva 2002/58/CE é habitualmente, e também no presente parecer, designada por Directiva Privacidade e Comunicações Electrónicas.

([1]) JO L 281 de 23.11.1995, p. 31.
([2]) JO L 201 de 31.7.2002, p. 37.
([3]) JO L 8 de 12.1.2001, p. 1.

2. A proposta destina-se a melhorar a protecção da privacidade de pessoas singulares e os dados pessoais no sector das comunicações electrónicas. Este objectivo é conseguido não por uma reformulação total da actual directiva Privacidade e Comunicações Electrónicas, mas mediante a proposta de alterações *ad hoc* à mesma com o principal objectivo de reforçar as disposições relativas à segurança e de melhorar os mecanismos de execução.

3. A proposta faz parte de uma reforma mais vasta das cinco directivas Telecom da UE («pacote Telecom»). Além das propostas para revisão do pacote Telecom ([1]), a Comissão aprovou também ao mesmo tempo uma proposta de regulamento que estabelece a Autoridade Europeia para o Mercado das Comunicações Electrónicas ([2]).

4. As observações incluídas no presente parecer limitam-se às alterações propostas à Directiva Privacidade e Comunicações Electrónicas a menos que essas mesmas alterações se baseiem em conceitos ou disposições incluídas em propostas de revisão do pacote Telecom. Além disso, algumas observações do presente parecer referem-se a disposições da Directiva Privacidade e Comunicações Electrónicas não alteradas pela proposta.

5. O parecer aborda os seguintes tópicos: i) âmbito da Directiva Privacidade e Comunicações Electrónicas, em especial, os serviços em questão (alteração proposta ao n.º 1 do artigo 3.º); ii) notificação das violações da segurança (alteração proposta que cria os n.ºs 3 e 4 do artigo 4.º); iii) disposições relativas aos testemunhos de conexão (cookies), software espião e outros dispositivos afins (alteração proposta ao n.º 3 do artigo 5.º); iv) acções jurídicas intentadas pelos prestadores de serviços de comunicações electrónicas e outras pessoas colectivas (alteração proposta que cria o n.º 6 do artigo 13.º e v) reforço das disposições de execução (alteração proposta que cria o artigo 15.ºA).

Consulta da AEPD e consulta pública mais vasta

6. A proposta foi enviada pela Comissão à AEPD em 16 de Novembro de 2007. A AEPD considera esta comunicação como um pedido para aconselhar as instituições e órgãos comunitários, como prevê o n.º 2 do artigo 28.º do Regulamento (CE) n.º 45/2001 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e órgãos comunitários e à livre circulação desses dados [a seguir denominado «Regulamento (CE) n.º 45/2001»].

7. Antes da aprovação da proposta, a Comissão consultou informalmente a AEPD sobre o projecto de proposta, que a AEPD recebeu com agrado pois lhe deu a oportunidade de apresentar algumas sugestões sobre o referido projecto antes de ser aprovado pela Comissão. A AEPD verifica com agrado que algumas das suas sugestões estão reflectidas na proposta.

8. A aprovação da proposta foi precedida por um vasto exercício de consulta pública, prática louvada pela AEPD. De facto, em Junho de 2006, a Comissão lançou uma consulta pública sobre a sua comunicação relativa à revisão do pacote Telecom em que a Comissão descreve a sua perspectiva da situação e apresenta algumas propostas de alteração ([3]). O Grupo do artigo 29.º de que a AEPD é membro, aproveitou o ensejo para apresentar a sua perspectiva sobre as alterações propostas num parecer aprovado em 26 de Setembro de 2006 ([4]).

([1]) As alterações propostas às Directivas Telecom são apresentadas nas seguintes propostas: i) Proposta de directiva do Parlamento Europeu e do Conselho que altera a Directiva 2002/21/CE relativa a um quadro regulamentar comum para as redes e serviços de comunicações electrónicas, a Directiva 2002/19/CE relativa ao acesso e interligação de redes de comunicações electrónicas e recursos conexos, e a Directiva 2002/20/CE relativa à autorização de redes e serviços de comunicações electrónicas, 13 de Novembro de 2007, COM(2007) 697 final; ii) 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, 13 de Novembro de 2007, COM(2007) 698 final.

([2]) Proposta de regulamento do Parlamento Europeu e do Conselho que institui a Autoridade Europeia para o Mercado das Comunicações Electrónicas, 13 de Novembro de 2007, COM(2007) 699 final.

([3]) Comunicação relativa ao quadro regulamentar comunitário das redes e serviços de comunicações electrónicas [SEC(2006) 816] aprovada em 29 de Junho de 2006. A comunicação era acompanhada por um documento de trabalho dos serviços de Comissão [COM(2006) 334 final].

([4]) Parecer n.º 8/2006 sobre a revisão do quadro regulamentar das comunicações e serviços electrónicos, que incide sobre a Directiva Privacidade e Comunicações Electrónicas, aprovado em 26 de Setembro de 2006.

Panorâmica da AEPD

9. Em geral, a perspectiva da AEPD sobre a proposta é positiva. A AEPD apoia totalmente os objectivos da Comissão de aprovar uma proposta que melhore a protecção da privacidade das pessoas singulares e dos dados pessoais no sector das comunicações electrónicas. A AEPD saúda em especial a aprovação de um sistema de notificação obrigatória das violações da segurança (alteração ao artigo 4.º da Directiva Privacidade e Comunicações Electrónicas, aditando os n.ºs 3 e 4). Quando ocorrem violações de dados, a notificação tem vantagens evidentes, reforça a responsabilidade das organizações, é um factor que impele as empresas a aplicar rigorosas medidas de segurança e permite a identificação das tecnologias mais fiáveis de protecção da informação. Além disso, dá às pessoas singulares afectadas a oportunidade de tomar medidas para se protegerem contra a usurpação de identidade ou outras utilizações abusivas das suas informações pessoais.

10. A AEPD saúda outras alterações da proposta como a possibilidade de as pessoas colectivas com interesse legítimo agirem contra quem infrinja algumas disposições da Directiva Privacidade e Comunicações Electrónicas (alteração ao artigo 13.º, que acrescenta o n.º 6). Também é positivo o reforço dos poderes de investigação das autoridades reguladoras nacionais, pois lhes permite avaliar se o processamento de dados é ou não realizado nos termos da legislação e identificar infractores (aditamento do n.º 3 do artigo 15.ºA). Ser capaz de parar o tratamento ilegal de dados pessoais e as violações da privacidade logo que possível é uma medida necessária para proteger os direitos e liberdades das pessoas. Para o efeito, a proposta de n.º 2 do artigo 15.ºA que reconhece a capacidade das autoridades reguladoras para impor a cessação das infracções é saudada por lhes permitir pôr imediatamente termo ao processamento ilegal grave.

11. A abordagem da proposta e da maioria das alterações propostas está de acordo com a perspectiva da futura política de protecção de dados apresentada em pareceres anteriores da AEPD como o parecer sobre a aplicação da directiva relativa à protecção de dados ([1]). A abordagem baseia-se, designadamente, na ideia de que embora não sejam necessários novos princípios de protecção de dados, há necessidade de regras mais específicas para tratar as questões suscitadas pelas novas tecnologias como a Internet, RFID, etc., bem como de instrumentos que contribuam para aplicar e tornar eficaz a legislação sobre protecção de dados, como permitir às entidades jurídicas intentar acções por violação da protecção de dados e obrigar os controladores de dados a notificar as violações da segurança.

12. Apesar da abordagem geral positiva da proposta, a AEPD lamenta que a proposta não seja suficientemente ambiciosa. De facto, desde 2003, a aplicação das disposições da Directiva Privacidade e Comunicações Electrónicas, bem como uma análise cuidada do assunto demonstrou que algumas destas disposições não são claras, e provocam incerteza jurídica e problemas de cumprimento. Por exemplo, isso acontece quanto a saber em que medida os prestadores de serviços parapúblicos de comunicações electrónicas estão cobertos pela Directiva Privacidade e Comunicações Electrónicas. Teria sido preferível a Comissão utilizar a revisão do pacote Telecom, e em especial da Directiva Privacidade e Comunicações Electrónicas, para resolver alguns dos problemas pendentes. Além disso, ao tratar as novas questões, como a criação de um sistema de notificação obrigatória das violações, a proposta apresenta apenas uma solução parcial, não incluindo no âmbito das organizações obrigadas a notificar as violações da segurança as entidades que processam tipos de dados muito sensíveis como os bancos em linha ou prestadores de serviços de saúde em linha. A AEPD lamenta esta abordagem.

13. A AEPD espera que à medida que a proposta avance no processo legislativo, o legislador tenha em conta as observações e propostas do presente parecer no sentido de resolver as questões que a proposta da Comissão não abordou.

([1]) Parecer da Autoridade Europeia para a Protecção de Dados de 25 de Julho de 2007 sobre a Comunicação da Comissão ao Parlamento Europeu e ao Conselho sobre o acompanhamento do programa de trabalho para uma melhor aplicação da directiva relativa à protecção de dados (JO C 255 de 27.10.2007, p. 1).

II. ANÁLISE DA PROPOSTA

II.1. Âmbito da Directiva Privacidade e Comunicações Electrónicas, em especial, serviços abrangidos

14. Uma questão principal na actual Directiva Privacidade e Comunicações Electrónicas é a do seu âmbito de aplicação. A proposta contém alguns elementos positivos para a definição e clarificação do âmbito da directiva, particularmente, os serviços abrangidos pela directiva, discutidos seguidamente na secção i). Infelizmente, as alterações propostas não resolvem todos os problemas existentes. Tal como discutido na secção ii) infra, as alterações infelizmente não procuram alargar o âmbito de aplicação da directiva para incluir os serviços de comunicações electrónicas nas redes privadas.

15. O artigo 3.º da Directiva Privacidade e Comunicações Electrónicas descreve os serviços abrangidos pela directiva, por outras palavras, os serviços aos quais se aplicam as obrigações estipuladas na directiva. «*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. Por conseguinte, os serviços abrangidos pela Directiva Privacidade e Comunicações Electrónicas são os prestadores de serviços públicos de comunicações electrónicas nas redes públicas («PPECS») A definição de PPECS é dada na alínea c) do artigo 2.º da Directiva-Quadro ([1]). As redes de comunicações públicas são definidas na alínea d) do artigo 2.º da Directiva-Quadro ([2]). Exemplos de actividades de PPECS incluem o fornecimento de acesso à Internet, transmissão de informações através das redes electrónicas, ligações móveis e de telefone, etc.

i) *Alteração proposta ao artigo 3.º da Directiva Privacidade e Comunicações Electrónicas: os serviços abrangidos incluem as redes de comunicações públicas que servem de suporte a dispositivos de recolha de dados e de identificação*

17. A proposta altera o artigo 3.º da Directiva Privacidade e Comunicações Electrónicas especificando que as redes de comunicações electrónicas públicas incluem «*as redes de comunicações públicas que servem de suporte a dispositivos de recolha de dados e de identificação*». O considerando 28 explica que o desenvolvimento de aplicações que impliquem a recolha de informações, incluindo de dados pessoais, utilizando frequências de rádio, como RFID, deve ficar sujeito ao disposto na Directiva Privacidade e Comunicações Electrónicas sempre que estejam ligados ou utilizem redes ou serviços de comunicações públicas.

18. A AEPD considera esta disposição positiva por esclarecer que várias aplicações RFID são abrangidas pelo âmbito da Directiva Privacidade e Comunicações Electrónicas, retirando alguma incerteza quanto a este ponto e suprimindo definitivamente mal-entendidos ou interpretações erradas da legislação.

19. De facto, nos termos do actual artigo 3.º da Directiva Privacidade e Comunicações Electrónicas, certas aplicações RFID estão já abrangidas pela directiva. Isto acontece por uma série de razões. Primeiro, porque as aplicações RFID são abrangidas pela definição de serviços de comunicações electrónicas. Segundo, porque são prestados numa rede de comunicações electrónicas na medida em que as aplicações têm o suporte de um sistema de transmissão sem fios que envia sinais. E, finalmente, a rede pode

([1]) Directiva 2002/21/CE do Parlamento Europeu e do Conselho, de 7 de Março de 2002, relativa a um quadro regulamentar comum para as redes e serviços de comunicações electrónicas (JO L 108 de 24.4.2002, p. 33). A Directiva-Quadro delimita o que se deve entender por serviço de comunicações electrónicas, ou seja: i) Um «serviço de comunicações electrónicas» é um serviço prestado em geral mediante remuneração, que consiste no envio de sinais através de redes e inclui serviços de telecomunicações e de transmissões em redes. ii) São excluídos da definição de serviços de comunicações electrónicas os serviços que fornecem conteúdos transmitidos através de redes e serviços de comunicações electrónicas. iii) Prestação de serviços, o estabelecimento, operação, controlo ou disponibilização de uma rede. iv) Os serviços de comunicações electrónicas não incluem os serviços da sociedade da informação, que são definidos na Directiva sobre comércio electrónico como serviço(s) prestado(s) normalmente mediante remuneração, à distância, por via electrónica e a pedido individual de um destinatário de serviços.

([2]) «Rede de comunicações pública», a rede de comunicações electrónicas utilizada total ou principalmente para o fornecimento de serviços de comunicações electrónicas acessíveis ao público.

ser pública e privada. Se for pública, as aplicações RFID serão consideradas «serviços abrangidos» e são assim do âmbito de aplicação da Directiva Privacidade e Comunicações Electrónicas. No entanto, a alteração proposta eliminará quaisquer dúvidas que persistam sobre a questão, proporcionando assim maior certeza jurídica.

20. É claro, como afirmava um parecer anterior da AEPD sobre RFID ([1]), que esta disposição não obsta à eventual necessidade de aprovar novos instrumentos legais, no que diz respeito às RFID. No entanto, essas medidas deviam ser aprovadas noutro contexto e não como parte da presente proposta.

ii) *Necessidade de incluir os serviços de comunicações electrónicas nas redes privadas ou semi privadas*

21. Embora a AEPD se congratule com o esclarecimento acima referido, lamenta que a proposta não tenha abordado a questão da distinção cada vez mais confusa entre redes privadas e públicas. Além disso, a AEPD lamenta que a definição dos serviços abrangidos pela Directiva Privacidade e Comunicações Electrónicas não tenha sido alargada para abranger as redes privadas. Na fase actual, o n.º 1 do artigo 3.º da Directiva Privacidade e Comunicações Electrónicas só se aplica aos *serviços de comunicações electrónicas nas redes públicas*.

22. A AEPD regista a tendência dos serviços para cada vez mais se tornarem um misto de privados e públicos. Note-se, por exemplo, o caso das universidades que permitem a milhares de estudantes utilizar a Internet e o correio electrónico. A possibilidade de esta rede semi-pública (ou semi-privada) interferir na privacidade individual é óbvia e exige, portanto, que este tipo de serviços seja sujeito ao mesmo conjunto de regras que se aplicam às redes puramente públicas. Além disso, as redes privadas, como as dos empregadores que proporcionam acesso à Internet aos empregados, dos proprietários de hotéis ou de apartamentos que proporcionam aos clientes telefone e correio electrónico e dos cibercafés têm um impacto na protecção de dados e na privacidade dos utilizadores, o que sugere que deviam ser também abrangidas pelo âmbito de aplicação da Directiva Privacidade e Comunicações Electrónicas.

23. De facto, a jurisprudência de alguns Estados-Membros considerou os serviços de comunicações electrónicas prestados em redes privadas sujeitos às mesmas obrigações dos prestados em redes públicas ([2]). Também na legislação alemã, as autoridades de protecção de dados consideraram que autorizar o uso de correio electrónico privado numa empresa pode fazer com que a empresa seja considerada um operador de serviços públicos de telecomunicações, ficando assim abrangida pelo disposto na Directiva Privacidade e Comunicações Electrónicas.

24. Resumindo, a importância crescente das redes mistas (privadas/públicas) e privadas no quotidiano, com o correspondente aumento dos riscos para os dados pessoais e a privacidade, justifica a necessidade de aplicar a esses serviços as mesmas regras que se aplicam aos serviços públicos de comunicações electrónicas. Para o efeito, a AEPD considera que a directiva devia ser alterada para alargar o seu âmbito de aplicação e incluir esse tipo de serviços privados; ponto de vista partilhado pelo Grupo do artigo 29.º ([3]).

II.2. **Notificação das Violações da Segurança: alteração ao artigo 4.º**

25. O artigo 4.º da Directiva Privacidade e Comunicações Electrónicas é alterado com a inclusão de dois novos números (3 e 4) que preconizam a obrigação de notificação das violações da segurança. De facto, nos termos do n.º 3 do artigo 4.º os PPECS são obrigados, por um lado, a notificar às autoridades reguladoras nacionais, sem atrasos injustificados, qualquer violação da segurança que provoque, de modo acidental ou ilegal, a destruição, a perda, a alteração ou a divulgação ou acesso não autorizados a dados pessoais transmitidos, armazenados ou de outro modo processados no contexto do fornecimento de serviços de comunicações electrónicas (colectivamente «dados comprometidos»); por outro, os PPECS são obrigados a notificar os clientes.

([1]) Parecer de 20 de Dezembro de 2007 sobre a Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões — Identificação por radiofrequências (RFID) na Europa: rumo a um quadro político, COM(2007) 96.

([2]) Por exemplo, o acórdão do Tribunal de Recurso de Paris no processo *BNP Paribas/World Press Online*, de 4 de Fevereiro de 2005, considerou que não havia distinção entre os prestadores de serviços de Internet que fornecem acesso à Internet mediante remuneração e os empregadores que dão acesso à Internet ao seu pessoal.

([3]) Parecer n.º 8/2006 sobre a revisão do quadro regulamentar das comunicações e serviços electrónicos, que incide sobre a Directiva Privacidade e Comunicações Electrónicas, aprovado em 26 de Setembro de 2006.

Vantagens desta obrigação

26. A AEPD saúda estas disposições (n.os 3 e 4 do artigo 4.º) que introduzem a obrigação de notificação das violações da segurança A notificação das violações da segurança traz vantagens na perspectiva da protecção dos dados pessoais e da privacidade que já foram testadas nos Estados Unidos em que a legislação sobre a notificação de violações a nível nacional está já em vigor há vários anos.

27. Em primeiro lugar, a legislação sobre notificação das violações aumenta a responsabilidade dos PPECS relativamente à informação comprometida. No quadro da política de protecção dos dados ou da privacidade, responsabilidade significa que cada organização é responsável pela informação sob o seu cuidado e controlo. A obrigação de notificar é equivalente a uma re-declaração, por um lado, que os dados comprometidos estavam sob o controlo do PPECS e, por outro, que é responsabilidade dessa organização tomar as medidas necessárias em relação a esses dados.

28. Em segundo lugar, verificou-se que a existência de uma notificação de violação da segurança incitava ao investimento na segurança por parte de organizações que tratam dados pessoais. Aliás, o simples facto de ter que notificar publicamente as violações da segurança leva as organizações a aplicar normas de segurança mais rigorosas que protegem as informações pessoais e impedem as violações. Além disso, a notificação das violações da segurança contribui para identificar e efectuar análises estatísticas fiáveis quanto às soluções e mecanismos de segurança mais eficazes. Durante muito tempo houve falta de dados concretos sobre as falhas na segurança das informações e as tecnologias mais adequadas para proteger as informações. Este problema pode ser agora resolvido com a obrigação de notificação da violação da segurança, como aconteceu nos EUA com a legislação sobre notificação da violação da segurança, porque a notificação dá informações sobre as tecnologias mais favoráveis às violações ([1]).

29. Finalmente, a notificação da violação da segurança torna as pessoas conscientes dos riscos que correm quando os seus dados pessoais são comprometidos e ajuda-as a tomar as medidas necessárias para reduzir esses riscos. Por exemplo, se os dados bancários foram comprometidos, a pessoa informada pode decidir alterar os seus elementos de acesso à conta bancária para impedir outrem de retirar essa informação, utilizando-a para fins ilegais (habitualmente designado por «usurpação de identidade»). Em suma, esta obrigação reduz a possibilidade de as pessoas serem vítimas de usurpação de identidade e pode também ajudar as vítimas a tomar as medidas necessárias para resolver problemas.

Défice da alteração proposta

30. Embora a AEPD esteja satisfeita com o sistema de notificação da violação da segurança estabelecido nos n.os 3 e 4 do artigo 4.º, preferia a sua aplicação em mais larga escala para incluir os prestadores de serviços da sociedade da informação. Isto significa que os bancos em linha, empresas em linha, prestadores de serviços de saúde em linha, etc. ficariam também abrangidos pela legislação ([2]).

31. As razões que justificam a imposição da notificação da violação da segurança aos prestadores de serviços públicos de comunicações electrónicas, i.e. PPECS, existem também em relação a outras organizações que tratam grandes quantidades de dados pessoais, cuja divulgação pode ser particularmente nefasta para as pessoas a que se referem os dados. Isto inclui bancos em linha, corretores de dados e outros prestadores em linha como os que tratam dados sensíveis (incluindo dados sanitários, opiniões políticas, etc.). Os dados comprometidos na posse de bancos em linha e empresas em linha que podem incluir não só números de contas bancárias, mas também dados de cartões de crédito podem dar lugar à usurpação de identidade, caso em que é essencial sensibilizar as pessoas para tomarem as medidas que se impõem. No último caso (saúde em linha), se não sofrem financeiramente, muito provavelmente sofrerão danos não económicos sempre que as informações sensíveis são comprometidas.

([1]) Ver relatório «*Security Economics and the Internal Market*», encomendado pela ENISA ao Prof. Ross Anderson, Rainer Böhme, Richard Clayton and Tyler Moore. O relatório está disponível no sítio: http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf

([2]) Os prestadores de serviços da sociedade da informação são definidos na Directiva sobre comércio electrónico como serviço(s) prestado(s) normalmente mediante remuneração, à distância, por via electrónica e a pedido individual de um destinatário de serviços.

32. Além disso, ao alargar o âmbito da obrigação, as vantagens acima descritas, decorrentes da imposição desta obrigação, não se limitam a um sector de actividade, o dos prestadores de serviços de comunicações publicamente disponíveis, mas serão alargadas aos serviços da sociedade da informação em geral. De facto, a imposição de obrigações de notificação da violação da segurança aos serviços da sociedade da informação, como bancos em linha, não só aumenta a sua responsabilidade como também motiva esses actores a reforçar as suas medidas de segurança evitando no futuro eventuais violações da segurança.

33. Existem outros precedentes em que a Directiva Privacidade e Comunicações Electrónicas é aplicada a entidades que não os PPECS, como o artigo 5.º relativo à confidencialidade das comunicações e o artigo 13.º sobre spam. Isto confirma que no passado o legislador, acertadamente, decidiu alargar o âmbito de aplicação de determinadas disposições da Directiva Privacidade e Comunicações Electrónicas por considerar adequado e necessário. A AEPD espera que actualmente o legislador não hesite em assumir uma abordagem semelhante sensata e flexível alargando o âmbito de aplicação do artigo 4.º para incluir os prestadores de serviços da sociedade da informação. Para tal, seria suficiente inserir no n.º 3 do artigo 4.º uma referência aos prestadores de serviços da sociedade da informação do seguinte teor: «*Em caso de violação da segurança que provoque, de modo acidental ou (…) o fornecedor dos serviços de comunicações electrónicas publicamente disponíveis e o prestador de serviços da sociedade da informação notificarão (…) essa violação ao assinante em causa e à autoridade reguladora nacional*».

34. A AEPD considera esta obrigação e a sua aplicação aos PPECS e aos prestadores de serviços da sociedade da informação como um primeiro passo para um desenvolvimento que pode eventualmente ser aplicado a todos os controladores de dados em geral.

Quadro jurídico específico para as violações da segurança a tratar através da comitologia

35. A proposta não aborda uma série de questões relacionadas com a obrigação de notificação das violações da segurança. Exemplos de questões que devem ser abordadas são as circunstâncias, o formato e os procedimentos aplicáveis à notificação da violação da segurança. Em contrapartida, o n.º 4 do artigo 4.º da proposta deixa essas decisões para aprovação através do comité «comitologia» ([1]), designadamente o Comité das Comunicações criado pelo artigo 22.º da Directiva-Quadro, nos termos da Decisão do Conselho de 28 de Junho de 1999. Em especial, essas medidas devem ser aprovadas de acordo com o artigo 5.º da Decisão do Conselho de 28 de Junho de 1999 que fixa regras para o processo de regulamentação, no que diz respeito às «*as medidas de âmbito geral que visam a aplicação de disposições essenciais de um acto de base*».

36. A AEPD não se opõe à escolha de deixar essas questões para a legislação de execução. A aprovação de legislação através da comitologia poderá reduzir o processo legislativo. A comitologia contribuirá também para garantir a harmonização que é um objectivo a procurar em definitivo.

37. Tendo em conta o grande número de questões que devem ser abordadas nas regras de execução e sua relevância, como indicado infra, afigura-se adequado tratá-las todas num único diploma legislativo e não por uma abordagem parcelar em que algumas questões seriam tratadas na Directiva Privacidade e Comunicações Electrónicas enquanto outras seriam deixadas para a legislação de execução. Assim, é de louvar a abordagem da Comissão que consiste em deixar essas decisões para a legislação de execução, a aprovar após consulta da AEPD e possivelmente de outras partes interessadas (ver ponto infra).

Questões que devem ser tratadas através de regras de execução

38. A relevância das regras de execução é salientada se se previrem com algum pormenor as questões a tratar através de regras de execução. De facto, as regras de execução podem determinar as normas a que devem obedecer as notificações. Por exemplo, especificam o que constitui uma violação da segurança, as condições em que devem ser enviadas as notificações às pessoas e às autoridades, os prazos da notificação.

([1]) Processos legislativos na CE que implicam comités compostos por representantes dos governos dos Estados-Membros a nível de funcionários.

39. A AEPD considera que a Directiva Privacidade e Comunicações Electrónicas, em especial o artigo 4.º, não devia conter excepções à obrigação de notificação. Neste aspecto, a AEPD regozija-se com a abordagem da Comissão inserida no artigo 4.º que estabelece uma obrigação de notificar e não prevê excepções, mas permite que essa e outras questões sejam tratadas na legislação de execução. Embora a AEPD esteja ciente dos argumentos que podem justificar algumas excepções à obrigação, preconiza que esta e outras questões sejam cuidadosamente tratadas através da legislação de execução, após um debate aprofundado e global de todas as questões em causa. Como se indica supra, a natureza complexa das questões relacionadas com a obrigação de notificação das violações da segurança, incluindo se são adequadas as excepções e limitações, exige que elas sejam tratadas de uma forma uniforme, ou seja, num diploma legislativo único que trate apenas desta questão.

Consulta da AEPD e necessidade de alargar a consulta

40. Tendo em conta a medida em que as regras de execução afectam a protecção dos dados pessoais dos indivíduos, importa que antes da aprovação destas regras a Comissão dê início a um exercício de consulta adequado. Por esse motivo, a AEPD saúda o n.º 4 do artigo 4.º da proposta que estabelece explicitamente que antes da aprovação das regras de execução a Comissão deve consultar a Autoridade Europeia para a Protecção de Dados. Essas regras não só dirão respeito, mas terão um impacto importante na protecção dos dados pessoais e na privacidade das pessoas. Assim, importa pedir o parecer da AEPD como exige o artigo 41.º do Regulamento (CE) n.º 45/2001.

41. Além da consulta da AEPD, pode ser adequado incluir uma disposição que estabeleça que o projecto de medidas de execução deve ser sujeito a consulta pública para obter parecer e incentivar a troca de experiências de melhores práticas nestas questões. Isto proporcionará um canal adequado para que não só a indústria, mas também outras partes interessadas, incluindo outras autoridades de protecção de dados e o Grupo do artigo 29.º, apresentem as suas opiniões. A necessidade de consulta pública é reforçada se se tiver em conta que o processo de aprovação da legislação é a comitologia, com uma intervenção limitada do Parlamento Europeu.

42. A AEPD regista que o n.º 4 do artigo 4.º da proposta prevê que a Comissão consulte também a Autoridade para o Mercado das Comunicações Electrónicas antes de aprovar regras de execução. Neste contexto, a AEPD valoriza o princípio da consulta da Autoridade para o Mercado das Comunicações Electrónicas como depositária da experiência e conhecimentos da ENISA sobre questões de redes e de segurança da informação. Até ser criada a Autoridade para o Mercado das Comunicações Electrónicas pode ser adequado prever na alteração proposta (n.º 4 do artigo 4.º) a consulta da ENISA, como solução provisória.

II.3. **Fornecimento de cookies (testemunhos de conexão), software espião e dispositivos afins: alteração ao n.º 3 do artigo 5.º**

43. O n.º 3 do artigo 5.º da Directiva Privacidade e Comunicações Electrónicas aborda a questão das tecnologias que permitem o acesso e o armazenamento de informação no equipamento terminal do utilizador, através de redes de comunicações electrónicas. Um exemplo da aplicação do n.º 3 do artigo 5.º é a utilização de cookies ([1]). Outros exemplos incluem a utilização de tecnologias como o software espião (programas de espionagem camuflados) e cavalos de Tróia (programas escondidos em mensagens ou noutro software aparentemente inofensivo). O objectivo dessas tecnologias e metas varia muito, enquanto algumas são perfeitamente inofensivas ou até úteis para o utilizador, outras são nitidamente muito prejudiciais e ameaçadoras.

([1]) Os cookies são colocados por ISSP (sítios Internet) nos equipamentos terminais dos utilizadores, para diversos fins, incluindo reconhecer um visitante quando ele/ela volta a entrar no sítio Internet Na prática, quando um sítio Internet envia um cookie a um utilizador de Internet, é atribuído ao computador um número único (ou seja, o computador que recebeu cookies do sítio Internet A passa a ser «computador com o cookie 111»). O sítio internet guarda este número como referência. Se o(s) utilizador(es) do computador que recebeu o cookie 111 não apagar o dossier cookie, na vez seguinte em que entre no mesmo sítio Internet, o sítio será capaz de identificar o computador como o computador com o cookie 111. O sítio Internet naturalmente deduz que este computador já o visitou anteriormente. O mecanismo que permite a um sítio Internet reconhecer um computador como visitante recorrente é simples. Quando o computador visitante tem cookies, como o cookie 111, e entra no sítio que numa visita anterior gerou o cookie, este procura no disco duro do utilizador o número de ficheiro do cookie. Se o navegador web do utilizador encontrar um ficheiro que corresponda ao número de referência guardado no sítio Internet, informa o sítio Internet de que o computador tem o cookie 111.

44. O n.º 3 do artigo 5.º da Directiva Privacidade e Comunicações Electrónicas estabelece as condições aplicáveis ao obter acesso ou ao armazenar informação no equipamento terminal dos utilizadores, nomeadamente, das tecnologias já mencionadas. Em especial, nos termos do n.º 3 do artigo 5.º i) deve ser dada aos utilizadores da Internet informação clara e completa, de acordo com a Directiva 95/46/CE, nomeadamente sobre os objectivos do tratamento; e ii) deve ser dada aos utilizadores da Internet a possibilidade de recusar esse tratamento, ou seja, não querer o tratamento da informação encontrada no seu equipamento terminal.

Vantagens da alteração proposta

45. O actual n.º 3 do artigo 5.º da Directiva Privacidade e Comunicações Electrónicas limita o seu âmbito de aplicação a situações em que o acesso à informação e a armazenagem de informação no equipamento terminal do utilizador é efectuado através de *redes de comunicações electrónicas*. Isto inclui a situação acima descrita relativa à utilização de cookies, bem como outras tecnologias como software espião enviado através de redes de comunicações electrónicas. No entanto, não é claro se o n.º 3 do artigo 5.º se aplica em situações em que tecnologias semelhantes (cookies/software espião e outros do mesmo género) são distribuídas através de software fornecido em suportes externos de armazenamento e descarregados para o equipamento terminal dos utilizadores. Uma vez que existe a ameaça à privacidade independentemente do canal de comunicação, a limitação do n.º 3 do artigo 5.º a apenas um canal de comunicação não tem razão de ser.

46. A AEPD acolhe portanto com agrado a alteração ao n.º 3 do artigo 5.º que, ao retirar a referência às «redes de comunicações electrónicas», alarga de facto o âmbito de aplicação do mesmo número. De facto, a versão alterada do n.º 3 do artigo 5.º abrange ambas as situações em que o acesso e o armazenamento da informação no equipamento terminal do utilizador é efectuado através de redes de comunicações electrónicas mas também através de outros suportes externos de armazenamento de dados, como CD, CD-ROM, chaves USB, etc.

Armazenagem técnica para facilidade de transmissão

47. A última frase do n.º 3 do artigo 5.º da Directiva Privacidade e Comunicações Electrónicas não sofreu modificação na versão alterada. De acordo com a última frase, os requisitos da primeira frase do n.º 3 do artigo 5.º «*não impedirão qualquer armazenamento técnico ou acesso que tenham como finalidade exclusiva efectuar ou facilitar a transmissão de uma comunicação através de uma rede de comunicações electrónicas, ou que sejam estritamente necessários para fornecer um serviço no âmbito da sociedade de informação (…)*». Assim, as regras obrigatórias da primeira frase do n.º 3 do artigo 5.º (necessidade de prestar informação e oferta da possibilidade de recusa) não se aplica quando o acesso ao equipamento terminal do utilizador ou o armazenamento de informação se destina apenas a *facilitar* a transmissão ou, quando estritamente necessário, para fornecer serviços da sociedade da informação solicitados pelo utilizador.

48. A directiva não descreve em que circunstâncias o acesso ou armazenamento de informação tem o objectivo exclusivo de facilitar a transmissão ou de dar informações. Uma situação que podia ser claramente abrangida por esta excepção é o estabelecimento de uma ligação Internet. Isto porque é necessário estabelecer uma ligação Internet para obter um endereço IP ([1]). É pedido ao computador do utilizador final que revele ao prestador de acesso à Internet determinadas informações sobre si próprio e em troca, o prestador de acesso à Internet atribui-lhe um endereço IP. Neste caso, a informação armazenada no equipamento terminal do utilizador final é transferida para o prestador de acesso à Internet para que o utilizador tenha acesso à Internet. Neste caso, o prestador de acesso à Internet é dispensado da obrigação de anunciar esta recolha de informação e de dar o direito de recusa na medida em que é necessário para fornecer o serviço.

49. Uma vez ligado à Internet, se o utilizador pretender ver um determinado sítio Internet, deve enviar um pedido ao servidor em que o sítio Internet está acolhido. Este responde se souber para onde enviar a informação, ou seja, se souber o endereço IP do utilizador. A maneira como este endereço está armazenado exige de novo que o sítio Internet que o utilizador pretende visitar tenha acesso a informação no equipamento terminal do utilizador da Internet. É evidente que esta transacção seria também abrangida pelo âmbito da excepção. De facto, nestes casos parece adequado não estar abrangido pelo âmbito de aplicação dos requisitos do n.º 3 do artigo 5.º.

([1]) Um endereço IP (Internet Protocol address) é um endereço único que determinados mecanismos electrónicos utilizam para identificar e comunicar entre si numa rede de computadores que utilizem a norma Internet Protocol (IP) — em termos mais simples, um endereço de computador. Qualquer dispositivoi que participe na rede — incluindo encaminhadores, interruptores, computadores, servidores de infra-estrutura (p.ex. NTP, DNS, DHCP, SNMP, etc.), impressoras, aparelhos de fax Internet e alguns telefones — tem o seu próprio endereço que é único na rede específica. Alguns endereços IP destinam-se a ser únicos no âmbito da Internet global, enquanto outros devem ser únicos apenas no âmbito de uma empresa.

50. A AEPD considera adequado isentar da necessidade de informar e dar a possibilidade de recusa em situações como as apresentadas supra quando a armazenagem técnica ou o acesso ao equipamento terminal do utilizador é *necessário* exclusivamente para a transmissão de uma comunicação numa rede de comunicações electrónicas. O mesmo se aplica quando a armazenagem técnica ou o acesso é estritamente necessário para fornecer um serviço da sociedade da informação. No entanto, a AEPD não vê a necessidade de excluir da obrigação de fornecer informação e de proporcionar o direito de recusa nas situações em que a armazenagem técnica ou o acesso se destinem apenas a *facilitar* a transmissão de uma comunicação. Por exemplo, nos termos da última frase do presente artigo, a pessoa a que se referem os dados pode não beneficiar da informação nem do direito de se opor ao tratamento dos seus dados se um cookie recolher a sua preferência linguística ou a sua localização (p.ex. Bélgica, China) pois este tipo de cookies podem ser apresentados como tendo por objectivo a facilitação da transmissão de uma comunicação. A AEPD está ciente de que a nível do software, na prática é dada à pessoa a que se referem os dados a possibilidade de recusar ou modular o armazenamento de cookies. No entanto, esta situação não está coberta com suficiente clareza por qualquer disposição jurídica que permita formalmente à pessoa a que se referem os dados defender os seus direitos no contexto acima descrito.

51. Para evitar esta situação, a AEPD sugere que se altere ligeiramente a última parte do n.º 3 do artigo 5.º que consiste em suprimir da frase a palavra «facilitar». «*Tal não impedirá o armazenamento técnico ou o acesso que tenha como única finalidade efectuar ou facilitar a transmissão de uma comunicação através de uma rede de comunicações electrónicas, ou que seja estritamente necessário para fornecer um serviço da sociedade da informação (…).*»

II.4. **Acções intentadas pelos PPECS e por pessoas colectivas: Aditamento de um n.º 6 ao artigo 13.º**

52. O n.º 6 do artigo 13.º proposto prevê soluções em matéria de direito civil para as pessoas ou as pessoas colectivas com interesse legítimo, em especial para os prestadores de serviços de comunicações electrónicas com interesse comercial para lutar contra os infractores ao disposto no artigo 13.º da Directiva Privacidade e Comunicações Electrónicas. Este artigo trata do envio de comunicações comerciais não solicitadas.

53. A alteração proposta permitirá, por exemplo, aos fornecedores de acesso à Internet confrontar os spammers por abusarem das suas redes, intentar acções contra entidades que falsifiquem endereços de remetentes ou ataquem servidores para os utilizar como retransmissores de spam.

54. Não é claro na Directiva Privacidade e Comunicações Electrónicas se esta confere aos PPECS o direito de intentar acções contra spammers e em algumas ocasiões os PPECS intentaram acções por infracção ao artigo 13.º implementado na legislação dos Estados-Membros ([1]). Ao reconhecer uma causa para acção judicial para os fornecedores de serviços de comunicações electrónicas protegerem os seus interesses comerciais, a proposta confirma que a Directiva Privacidade e Comunicações Electrónicas pretende não só proteger os assinantes individuais, mas também os prestadores de serviços de comunicações electrónicas.

55. A AEPD saúda o facto de a proposta introduzir a possibilidade de os fornecedores de serviços de comunicações electrónicas que tenham um interesse comercial intentarem acções judiciais contra os spammers. Salvo em circunstâncias excepcionais, os assinantes individuais não dispõem dos meios nem dos incentivos para intentar este tipo de acção judicial. Em contrapartida, os fornecedores de acesso à Internet e outros PPECS têm capacidade financeira e tecnológica para investigar campanhas de spam, identificar os autores desses delitos e, assim, é adequado que tenham o direito de intentar acções contra spammers.

56. A AEPD regozija-se, em particular, com a alteração proposta na medida em que permitirá também às associações de consumidores e aos sindicatos que representam os interesses dos consumidores alvo de spam intentar acções judiciais em seu nome. Tal como já descrito, o prejuízo causado à pessoa a que se referem os dados que sofreu o spam, considerado individualmente, não é em geral suficiente para intentar uma acção judicial. De facto, a AEPD propôs já esta medida em relação às infracções contra a privacidade e a protecção de dados em geral no parecer sobre o programa de trabalho para uma

([1]) Um caso em que isto acontece é o caso *Microsoft corporation/Paul McDonald t/a Bizards UK* [2006 All Er (D) 153].

melhor aplicação da Directiva relativa à Protecção de Dados ([1]). Na opinião da AEPD, a proposta podia ter ido mais além e propor acções colectivas, que permitam a grupos de cidadãos recorrer à justiça em matérias relativas à protecção de dados pessoais. No caso do spam, em que um grande número de pessoas recebem spam, existe potencial para que as pessoas se associem para intentar acções colectivas contra os spammers.

57. A AEPD lamenta especialmente que a proposta limite a possibilidade de as pessoas colectivas intentarem acções em situações em que se verifique a violação do artigo 13.º da directiva, ou seja, em situações em que seja violada a disposição sobre as comunicações de correio electrónico não solicitado. De facto, nos termos da alteração proposta, as pessoas colectivas não podem intentar acções relativas a infracções às outras disposições da Directiva Privacidade e Comunicações Electrónicas. Por exemplo, a disposição actual não permite a uma pessoa colectiva, como uma associação de consumidores, intentar uma acção contra um fornecedor de acesso à Internet que divulgou dados pessoais de milhões de clientes. A aplicação da Directiva Privacidade e Comunicações Electrónicas em geral, e não só de um determinado artigo, melhoraria bastante se o disposto no n.º 6 do artigo 13.º fosse generalizado para permitir às pessoas colectivas intentar acções por infracção a qualquer disposição da Directiva Privacidade e Comunicações Electrónicas.

58. Para resolver este problema, a AEPD sugere que se converta o n.º 6 do artigo 13.º num artigo separado (artigo 14.º). Além disso, a linguagem do n.º 6 do artigo 13.º deve ser ligeiramente alterada do seguinte modo: Onde se lê «*nos termos do presente artigo*» deve ler-se «nos termos da presente directiva».

II.5. **Reforço das disposições de execução: aditamento de um artigo 15.ºA**

59. A Directiva Privacidade e Comunicações Electrónicas não contém disposições de execução explícitas. Em vez disso, refere-se à secção de execução da Directiva relativa à Protecção de Dados ([2]). A AEPD saúda o novo artigo 15.ºA da proposta, que trata explicitamente de questões de execução no âmbito da presente directiva.

60. Em primeiro lugar, a AEPD regista que uma política de aplicação eficaz neste domínio parte do princípio, tal como exige o n.º 3 do artigo 15.ºA proposto, de que as autoridades nacionais dispõem de poderes de investigação para recolher as necessárias informações. Muitas vezes as provas da infracção ao disposto na Directiva Privacidade e Comunicações Electrónicas são de natureza electrónica e podem ser armazenadas em diferentes computadores e dispositivos ou redes. Neste contexto, importa que as agências de execução disponham da possibilidade de obter mandados de busca que lhes confiram poderes de invasão, busca e apreensão.

61. Em segundo lugar, a AEPD saúda em especial a alteração proposta, ou seja, o n.º 2 do artigo 15.ºA, segundo o qual as autoridades reguladoras nacionais devem dispor de poderes para ordenar medidas, como a cessação das infracções e dos necessários poderes de investigação e recursos. As autoridades reguladoras nacionais, incluindo as autoridades de protecção de dados nacionais, devem dispor de poderes para impor medidas que impeçam os delinquentes de prosseguir uma actividade que infringe a Directiva Privacidade e Comunicações Electrónicas. As injunções ou os poderes para ordenar a cessação de uma violação são um instrumento útil no caso de um procedimento que viole os direitos individuais. As injunções são muito úteis para pôr termo às violações da Directiva Privacidade e Comunicações Electrónicas, como a violação do artigo 13.º relativo às comunicações comerciais não solicitadas, que pela sua natureza é um comportamento continuado.

62. Em terceiro lugar, a proposta permite à Comissão tomar medidas técnicas de execução para garantir uma cooperação transfronteiriça mais eficaz na aplicação das legislações nacionais (alteração proposta n.º 4 do artigo 15.ºA). A experiência de cooperação até à data inclui o acordo aprovado por iniciativa da Comissão que estabelece um procedimento comum para tratar reclamações transfronteiriças sobre spam.

([1]) Parecer da Autoridade Europeia para a Protecção de Dados sobre a Comunicação da Comissão ao Parlamento Europeu e ao Conselho sobre o acompanhamento do programa de trabalho para uma melhor aplicação da Directiva relativa à Protecção de Dados (JO C 255 de 27.10.2007, p. 1).

([2]) 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.

63. A AEPD considera que, se a legislação apoiar os reguladores na assistência aos seus homólogos noutros países, assistirá sem dúvida a execução transfronteiriça. Por conseguinte, é adequado que a proposta permita à Comissão criar as condições para garantir a cooperação transfronteiriça, incluindo os procedimentos para o intercâmbio de informações.

III. **CONCLUSÕES E RECOMENDAÇÕES**

64. A AEPD dá o seu pleno apoio à proposta. As alterações propostas reforçam a protecção da privacidade das pessoas e dos dados pessoais no sector das comunicações electrónicas e isto com suavidade, sem criar encargos injustificados e desnecessários às organizações. Mais especificamente, a AEPD considera que na sua maioria as alterações propostas não devem ser alteradas na medida em que satisfaçam plenamente o seu objectivo. O ponto 69 infra, enumera as alterações que a AEPD prefere que não sejam modificadas.

65. Não obstante a sua posição em geral positiva sobre a proposta, a AEPD considera que algumas destas alterações podem ser melhoradas para garantir que proporcionem efectivamente uma protecção adequada dos dados pessoais e da privacidade das pessoas. Tal é em especial o caso das disposições sobre a notificação da violação da segurança e dos que tratem de acções intentadas pelos fornecedores de serviços de comunicações electrónicas por violação das disposições relativas ao spam. Além disso, a AEPD lamenta que a proposta não aborde algumas questões, que não foram tratadas de forma adequada na actual Directiva Privacidade e Comunicações Electrónicas, perdendo assim a oportunidade deste exercício de revisão para resolver os problemas em suspenso.

66. Para solucionar ambos os problemas, ou seja, as questões não tratadas adequadamente na proposta e as que não foram sequer tratadas, o presente parecer apresenta algumas propostas de redacção. Os pontos 67 e 68 resumem os problemas e propõem uma linguagem específica. A AEPD apela ao legislador para que tenha em conta esses problemas à medida que a proposta avançar no processo legislativo.

67. As alterações incluídas na proposta em que a AEPD é fortemente favorável a uma modificação são:

i) **Notificação da violação da segurança**: tal como formulada, a alteração proposta que adita o *n.º 4 do artigo 4.º* aplica-se aos fornecedores de serviços públicos de comunicações electrónicas nas redes públicas (FSI, operadores de rede) que são obrigados a notificar as autoridades reguladoras nacionais e os seus clientes das violações da segurança. A AEPD apoia plenamente esta obrigação. No entanto, considera que a obrigação devia também aplicar-se aos prestadores de serviços da sociedade da informação que muitas vezes tratam informações pessoais sensíveis. Assim, os bancos e seguradoras em linha, os prestadores de serviços de saúde em linha e outras empresas em linha teriam que cumprir essa obrigação.

Para tal, a AEPD sugere que se insira no n.º 3 do artigo 4.º uma referência aos prestadores de serviços da sociedade da informação do seguinte teor: «*Em caso de violação da segurança (…) o fornecedor dos serviços de comunicações electrónicas publicamente disponíveis e o prestador de serviços da sociedade da informação notificarão (…) essa violação ao assinante em causa e à autoridade reguladora nacional*.»

ii) **Acções intentadas pelos fornecedores de serviços públicos de comunicações electrónicas em redes públicas**: tal como formulada, a alteração proposta que adita o *n.º 6 do artigo 13.º* prevê soluções em matéria de direito civil para pessoas singulares ou colectivas, em especial para os prestadores de serviços de comunicações electrónicas para lutar contra as infracções ao artigo 13.º da Directiva Privacidade e Comunicações Electrónicas que trata de spam. A AEPD está satisfeita com esta disposição. No entanto, a AEPD não vê a lógica de esta capacidade se limitar à infracção ao artigo 13.º. A AEPD sugere que se permita às pessoas colectivas intentar acções por violação de qualquer disposição da Directiva Privacidade e Comunicações Electrónicas.

Para o conseguir, a AEPD sugere que se converta o n.º 6 do artigo 13.º num artigo separado (artigo 14.º). Além disso, a linguagem do n.º 6 do artigo 13.º deve ser ligeiramente alterada do seguinte modo: Onde se lê «*nos termos do presente artigo*» deve ler-se «nos termos da presente directiva».

68. O âmbito de aplicação da Directiva Privacidade e Comunicações Electrónicas, actualmente limitada aos fornecedores de redes públicas de comunicações electrónicas, é um dos problemas que a proposta não abordou. A AEPD considera que a directiva devia ser alterada para alargar a sua aplicação e incluir os prestadores de serviços de comunicações electrónicas também em redes mistas (privadas/públicas) e privadas.

69. As alterações que a AEPD preconiza não modificar são:

i) **RFID**: a alteração proposta ao *artigo 3.º* segundo a qual as redes de comunicações electrónicas incluem «*as redes públicas de comunicações que servem de suporte a dispositivos de recolha de dados e de identificação*» é plenamente satisfatória. Esta disposição é muito positiva pois esclarece que uma série de aplicações RFID devem cumprir o disposto na Directiva Privacidade e Comunicações Electrónicas, suprimindo assim alguma incerteza jurídica sobre este ponto.

ii) **Cookies/software espião**: a alteração proposta ao *n.º 3 do artigo 5.º* deve ser saudada pois daí resulta que a obrigação de informar e conceder o direito de se opor à armazenagem de cookies/ /software espião no seu equipamento terminal é também aplicável quando esses dispositivos são colocados através de suportes externos de armazenamento de dados, como CD-ROM e chaves USB. No entanto, a AEPD sugere uma ligeira alteração à última parte do n.º 3 do artigo 5.º que consiste em suprimir da frase a palavra «facilitar».

iii) **Escolha da comitologia com consulta à AEPD e condições/limitações à obrigação de notificação**: a alteração proposta de aditamento do n.º 4 do artigo 4.º relativo à notificação da violação da segurança deixa à comitologia, após pedido de parecer da AEPD, a decisão sobre questões complexas relativas a circunstâncias/formato/procedimentos do sistema de notificação da violação da segurança. A AEPD apoia vigorosamente esta abordagem unificada. A legislação sobre a notificação da violação da segurança é por si só um tópico que deve ser tratado após cuidado debate e análise.

Relacionado com esta matéria está o pedido de várias partes interessadas para estabelecer excepções à obrigação de notificação das violações da segurança no n.º 4 do artigo 4.º. A AEPD opõe-se vigorosamente a esta abordagem. Prefere que o tema geral da notificação, como notificar, em que circunstâncias a notificação pode ser reduzida ou de algum modo limitada, seja analisado globalmente após o debate respectivo.

iv) **Execução**: a alteração proposta que adita o *artigo 15.ºA* contém muitos elementos úteis que convém conservar que contribuem para garantir o cumprimento efectivo, incluindo o reforço dos poderes de investigação das autoridades reguladoras nacionais (n.º 3 do artigo 15.ºA) e a criação da capacidade das autoridades reguladoras nacionais para ordenar a cessação das infracções.

Feito em Bruxelas, em 10 de Abril de 2008.

Peter HUSTINX

Autoridade Europeia para a Protecção de Dados