I

(Resoluções, recomendações e pareceres)

PARECERES

AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS

Parecer da Autoridade Europeia para a Protecção de Dados sobre a promoção da confiança na sociedade da informação através do reforço da protecção dos dados e da privacidade

(2010/C 280/01)

A AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS,

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

Tendo em conta a Carta dos Direitos Fundamentais da União Europeia, nomeadamente os artigos 7.º e 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 pelos órgãos comunitários e à livre circulação desses dados ([3]), nomeadamente o artigo 41.º,

ADOPTOU O SEGUINTE PARECER:

I. INTRODUÇÃO

1. As tecnologias da informação e das comunicações (TIC) estão a permitir desenvolver capacidades extraordinárias em praticamente todos os aspectos da nossa vida — a forma como trabalhamos, nos divertimos, convivemos e educamos. Elas são essenciais para a actual economia da informação e para a sociedade em geral.

2. A União Europeia é uma potência mundial a nível das TIC avançadas e está decidida a continuar a sê-lo. Para responder a este desafio, prevê-se que a Comissão Europeia adopte em breve uma nova Agenda Digital Europeia, que a Comissária Kroes confirmou ser uma prioridade sua ([4]).

3. A AEPD reconhece os benefícios resultantes das TIC e concorda que a UE deve envidar os máximos esforços para estimular o seu desenvolvimento e adopção generalizada. Também apoia totalmente a opinião das Comissárias Kroes e Reding de que as pessoas devem estar no centro deste novo ambiente ([5]). As pessoas devem poder contar com a capacidade das TIC para manter as suas informações seguras e controlar a utilização que lhes é dada, bem como ter a certeza de que os seus direitos à privacidade e à protecção de dados serão respeitados no espaço digital. O respeito desses direitos é essencial para conquistar a confiança dos consumidores. E essa confiança é crucial para os cidadãos aderirem aos novos serviços ([6]).

([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.

([4]) Respostas ao Questionário do Parlamento Europeu à Comissária Neelie Kroes no contexto das audições do PE que antecederam a nomeação da Comissária.

([5]) Respostas ao Questionário do Parlamento Europeu à Comissária Neelie Kroes no contexto das audições do PE que antecederam a nomeação da Comissária; discurso da Comissária Viviane Reding subordinado ao tema «Uma Agenda Digital Europeia para o Novo Consumidor Digital», proferido no Fórum Multilateral do BEUC sobre a Privacidade dos Consumidores e Comercialização em Linha: Tendências de Mercado e Perspectivas Políticas, Bruxelas, 12 de Novembro de 2009.

([6]) Ver, por exemplo, Relatório RISEPTIS, «Trust in the Information Society», *A Report of the Advisory Board, RISEPTIS (Research and Innovation on Security, Privacy and Trustworthiness in the Information Society)*. Disponível em http://www.think-trust.eu/general/news-events/riseptis-report.html Ver também: J. B Horrigan, *Broadband Adoption and Use in America, FCC Omnibus Broadband Initiative, OBI Working Paper Series No 1*.

4. A UE dispõe de um forte quadro jurídico de protecção dos dados e da privacidade, cujos princípios permanecem totalmente válidos na nova era digital. Contudo, não podemos ser complacentes. Muitas vezes, as TIC suscitam novas preocupações que não são tidas em conta no quadro existente. Por conseguinte, são necessárias algumas medidas para garantir que os direitos individuais, consagrados no direito da UE, continuam a proporcionar uma protecção eficaz neste novo ambiente.

5. O presente parecer analisa as medidas que podem ser promovidas ou tomadas pela União Europeia com o intuito de garantir a privacidade e a protecção dos dados pessoais num mundo globalizado que continuará a basear-se na tecnologia. O parecer debruça-se sobre instrumentos legislativos e não legislativos.

6. Depois de apresentar uma panorâmica das TIC como novo desenvolvimento gerador de oportunidades, mas também de riscos, o parecer analisa a necessidade de integrar, a nível prático, a protecção de dados e a privacidade desde o início das novas tecnologias da informação e das comunicações (o denominado princípio de «privacidade desde a concepção»). A fim de impor o cumprimento deste princípio, o parecer analisa a necessidade de prever o princípio de «privacidade desde a concepção» no quadro jurídico relativo à protecção de dados pelo menos de duas formas diferentes. Em primeiro lugar, incorporando-o como princípio geral e vinculativo e, em segundo lugar, incorporando-o em determinados domínios das TIC, que apresentem riscos específicos em matéria de protecção de dados e de privacidade e que possam ser minimizados através de uma arquitectura e de uma concepção técnicas adequadas. Estes domínios são a identificação por radiofrequências (RFID), as aplicações de redes sociais e as aplicações de programas de navegação. Por último, o parecer apresenta sugestões a respeito de outros instrumentos e princípios destinados a proteger a privacidade e os dados das pessoas no sector das TIC.

7. Na abordagem das questões supramencionadas, o parecer desenvolve algumas das ideias apresentadas pelo Grupo do Artigo 29.º no seu contributo para a consulta pública sobre o futuro da privacidade ([1]). Desenvolve também anteriores pareceres da AEPD, como o Parecer de 25 de Julho de 2007 sobre a aplicação da Directiva relativa à protecção de dados, o parecer de 20 de Dezembro de 2007 sobre o RFID e os seus dois pareceres sobre a Directiva Privacidade e Comunicações Electrónicas ([2]).

II. AS TIC OFERECEM NOVAS OPORTUNIDADES MAS TAMBÉM APRESENTAM NOVOS RISCOS

8. As TIC têm sido comparadas a outras invenções importantes do passado, como a electricidade. Embora possa ser demasiado cedo para avaliar o seu verdadeiro impacto histórico, há uma clara ligação entre as TIC e o crescimento económico nos países desenvolvidos. As TIC geraram emprego e benefícios económicos, além de contribuírem para o bem-estar geral. O impacto das TIC não é exclusivamente económico, uma vez que têm desempenhado um papel importante no estímulo à inovação e à criatividade.

9. Além disso, as TIC transformaram a forma como as pessoas trabalham, convivem e interagem, dependendo cada vez mais das TIC, por exemplo, para as interacções sociais e económicas. As pessoas podem utilizar uma vasta gama de novas aplicações das TIC, como a saúde em linha, o transporte em linha e o governo em linha, bem como sistemas interactivos inovadores nos domínios do entretenimento e da aprendizagem.

10. Atendendo a tais benefícios, todas as Instituições Europeias exprimiram o seu compromisso de apoiar as TIC como um instrumento necessário para melhorar a competitividade da indústria europeia e acelerar o relançamento da economia da Europa. Na verdade, em Agosto de 2009, a Comissão adoptou o Relatório sobre a Competitividade Digital da Europa ([3]) e lançou uma consulta pública sobre as estratégias futuras adequadas para estimular as TIC. Em 7 de Dezembro de 2009, o Conselho apresentou uma contribuição para esta consulta, intitulada «Estratégia pós i2010 — rumo a uma sociedade do conhecimento aberta, ecológica e competitiva» ([4]). O

([1]) Parecer 168 do Grupo do Artigo 29.º «The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data» [O futuro da privacidade, contribuição conjunta para a consulta da Comissão Europeia sobre o quadro jurídico relativo ao direito fundamental à protecção dos dados pessoais], adoptado em 1 de Dezembro de 2009.

([2]) Parecer de 25 de Julho de 2007 respeitante à 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; 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 sobre «Identificação por radiofrequências (RFID) na Europa: rumo a um quadro político» [COM(2007) 96], JO C 101 de 23.4.2008, p. 1; Parecer de 10 de Abril de 2008 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), JO C 181 de 18.7.2008, p. 1; Segundo Parecer de 9 de Janeiro de 2009 sobre a revisão da Directiva 2002/58/CE relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas.

([3]) *Europe's Digital Competitiveness Report-Main achievements of the i-2010 strategy 2005-2009*, [SEC(2009) 1060].

([4]) Conclusões do Conselho «Estratégia pós i-2010 — rumo a uma sociedade do conhecimento aberta, ecológica e competitiva». (17107/09), adoptado em 18.12.2009.

Parlamento Europeu acaba de adoptar um relatório destinado a fornecer orientações à Comissão na definição de uma agenda digital ([1]).

11. Juntamente com as oportunidades e os benefícios associados ao desenvolvimento das TIC vêm novos riscos, sobretudo para a privacidade e a protecção dos dados pessoais dos indivíduos. As TIC conduzem frequentemente a uma proliferação (muitas vezes de formas de que as pessoas não se apercebem) da quantidade de informações que são recolhidas, triadas, filtradas, transferidas ou conservadas, e os riscos para esses dados multiplicam-se em consequência.

12. Por exemplo, os *chips* RFID estão a substituir os códigos de barras em (alguns) produtos de consumo. Ao melhorar o fluxo de informação na cadeia de abastecimento (e ao reduzir, desse modo, a necessidade de existências de precaução, fornecendo previsões mais precisas, etc.), o novo sistema beneficia, supostamente, as empresas e os consumidores. Contudo, ele suscita, simultaneamente, a possibilidade inquietante de se ser localizado, para diversos fins e por diferentes entidades, através dos bens pessoais com etiquetas electrónicas.

13. Outro exemplo é a «nebulosa computacional», essencialmente a prestação de serviços domiciliados de aplicações destinadas ou não aos consumidores através da Internet. Esses serviços vão desde fototecas, calendários, «webmail» e ficheiros de clientes até outros serviços mais complexos às empresas. Os benefícios tanto para as empresas como para as pessoas singulares são claros: redução dos custos (os custos são incrementais), independência em relação à localização (fácil acesso às informações em qualquer parte do mundo), automatização (não há necessidade de recursos informáticos dedicados nem de uma actualização constante do *software*), etc. Ao mesmo tempo, os riscos de ocorrência de falhas de segurança e de pirataria informática existem e são muito reais. A perda de acesso aos próprios dados e de controlo sobre os mesmos é outro motivo de preocupação.

14. Também foi demonstrada a coexistência de benefícios e riscos noutros domínios que utilizam aplicações de TIC, como é o caso da saúde em linha, que pode aumentar a eficácia, reduzir custos, aumentar a acessibilidade e melhorar a qualidade dos serviços de saúde em geral. Contudo, a saúde em linha suscita frequentemente a questão de legitimidade das utilizações secundárias das informações a ela referentes, exigindo uma análise cuidadosa dos fins a que se destinam as potenciais utilizações secundárias ([2]). Além disso, à medida que os registos de saúde electrónicos vão sendo mais utilizados, os próprios sistemas têm sido prejudicados por escândalos que revelam muitos casos de pirataria informática dos registos de saúde electrónicos.

15. Em suma, é provável que persistam riscos residuais, mesmo depois de se terem efectuado as devidas avaliações e aplicado as medidas necessárias. Uma situação de «risco zero» não seria realista. Todavia, tal como é a seguir referido, podem e devem ser aplicadas medidas para reduzir esses riscos para níveis apropriados.

III. PRIVACIDADE DESDE A CONCEPÇÃO COMO INSTRUMENTO FUNDAMENTAL PARA QUE AS PESSOAS CONFIEM NAS TIC

16. Só é possível usufruir efectivamente dos potenciais benefícios das TIC se estas conseguirem suscitar confiança, ou seja, se conseguirem garantir a disponibilidade dos utilizadores para confiarem nas TIC devido às características e aos benefícios das mesmas. Essa confiança só será conquistada se as TIC forem fiáveis e seguras, se as pessoas sentirem que elas estão sob o seu controlo e que a protecção da sua privacidade e dos seus dados pessoais está garantida.

17. Riscos e falhas comuns, como os acima mencionados, principalmente quando implicam a utilização indevida ou violações dos dados pessoais que exponham a privacidade das pessoas, são susceptíveis de pôr em risco a confiança dos utilizadores na sociedade da informação. Isto poderia prejudicar gravemente o desenvolvimento das TIC e os benefícios que elas podem originar.

18. No entanto, a forma de solucionar estes riscos para a privacidade e a protecção dos dados não poderá ser eliminar, excluir ou recusar a utilização ou a promoção das TIC. Isso não seria viável nem realista; impediria as pessoas de usufruírem dos benefícios das TIC e limitaria seriamente as vantagens que elas permitem obter, de um modo geral.

19. A AEPD entende que uma solução mais positiva será conceber e desenvolver as TIC de uma forma que respeite a privacidade e a protecção dos dados. Por conseguinte, é crucial que estas últimas sejam inseridas em todo o ciclo de vida da tecnologia, desde a fase inicial de concepção, até à sua instalação, utilização e eliminação finais. Esta abordagem é normalmente designada por «privacidade desde a concepção», sendo adiante analisada com mais pormenor.

20. A privacidade desde a concepção pode implicar diversas acções, consoante o caso ou a aplicação em concreto. Por exemplo, em alguns casos, pode exigir a eliminação/redução dos dados pessoais ou a prevenção de um tratamento

([1]) Relatório sobre uma nova agenda digital para a Europa: 2015.eu [2009/2225 (INI)], adoptado em 18.3.2010.

([2]) Por exemplo, a venda ou a utilização de informações de saúde recolhidas para efeitos de tratamento, tendo em vista a escolha de localizações de clínicas satélite, a instalação de centros de cirurgia em regime ambulatório ou outras formas de planeamento de actividades futuras com implicações financeiras, exigiriam uma exame cuidadoso.

desnecessário e/ou indesejado. Noutros casos, pode implicar a oferta de instrumentos para aumentar o controlo das pessoas sobre os seus dados pessoais. Tais medidas devem ser ponderadas na altura em que as normas e/ou melhores práticas são definidas. Também podem ser integradas na arquitectura dos sistemas de informação e comunicação, ou nas estruturas organizativas das entidades que tratam dados pessoais.

III.1. **Princípio da privacidade desde a concepção aplicável em diferentes ambientes de TIC e o impacto destas**

21. A necessidade do princípio de privacidade desde a concepção pode constatar-se em muitos e diferentes ambientes de TIC. Por exemplo, o sector da saúde depende cada vez mais de infra-estruturas de TIC que frequentemente implicam um armazenamento centralizado das informações de saúde dos pacientes. A aplicação deste princípio nesse sector exigiria que se avaliasse a adequação de diversas medidas, tais como a possibilidade de minimizar os dados armazenados a nível central ou de os limitar a um índice, a utilização de ferramentas de cifragem, direitos de acesso estritamente limitados à necessidade de informação, o anonimato dos dados logo que deixam de ser necessários, etc.

22. Do mesmo modo, os sistemas de transporte são cada vez mais equipados de origem com aplicações de TIC avançadas que interagem com o veículo e o seu ambiente para diversas finalidades e funções. Por exemplo, os automóveis são crescentemente equipados com novas funcionalidades de TIC (GPS, GSM, rede de sensores, etc.), que indicam não só a sua localização, mas também as suas condições técnicas, em tempo real. Estas informações poderiam ser utilizadas, por exemplo, para substituir o actual sistema de tarifas rodoviárias por uma taxa rodoviária dependente da utilização. A aplicação da privacidade desde a concepção no processo de definição da arquitectura desses sistemas contribuiria para o tratamento e posterior transferência do menor número possível de dados pessoais ([1]). Em conformidade com este princípio, as arquitecturas descentralizadas ou semi-centralizadas, que limitam a transmissão dos dados de localização para um ponto central, seriam preferíveis às arquitecturas centralizadas.

23. Os exemplos supramencionados mostram que, quando as tecnologias da informação e das comunicações são arquitectadas de acordo com o princípio da privacidade desde a concepção, os riscos para a privacidade e a protecção dos dados podem ser significativamente minimizados.

III.2. **Insuficiente implantação das TIC que aplicam a privacidade desde a concepção**

24. Uma questão importante é a de saber se os operadores económicos, fabricantes/fornecedores de TIC e responsáveis pelo tratamento de dados estão interessados na comercialização e aplicação do princípio de privacidade desde a concepção nas TIC. Neste contexto, também é importante avaliar a procura dos utilizadores nesta matéria.

25. Em 2007, a Comissão emitiu uma comunicação em que convidava as empresas a utilizarem as suas capacidades de inovação para criarem e implementarem tecnologias de protecção da privacidade como forma de melhorarem a protecção da privacidade e dos dados pessoais desde a fase inicial do ciclo de desenvolvimento ([2]).

26. Até agora, porém, os dados disponíveis mostram que nem os fabricantes de TIC nem os responsáveis pelo tratamento (tanto no sector privado como no sector público) conseguiram aplicar ou comercializar a privacidade desde a concepção de uma forma coerente. Têm sido apontados diversos motivos para que isto aconteça, incluindo falta de incentivos económicos ou de apoio institucional e uma procura insuficiente, entre outros ([3]).

27. Ao mesmo tempo, a procura de privacidade desde a concepção por parte dos utilizadores tem sido bastante baixa. Os utilizadores de produtos e serviços TIC podem partir do princípio de que a sua privacidade e os seus dados pessoais estão protegidos *de facto*, quando em muitos casos não estão. Por vezes, não estão pura e simplesmente em condições de tomar as medidas de segurança necessárias para proteger os seus próprios dados pessoais ou os dados de outras pessoas. Frequentemente, isto deve-se ao facto de não terem um conhecimento completo ou mesmo parcial dos riscos. Por exemplo, em geral, os jovens menosprezam os riscos para a privacidade associados à revelação de informações pessoais nas redes sociais e ignoram, com frequência, as definições de privacidade. Outros utilizadores, ainda, estão cientes dos riscos, mas podem não ter os conhecimentos técnicos necessários para aplicar tecnologias de salvaguarda, como as que protegem a sua ligação à Internet, ou para alterar as definições do programa de navegação de modo a minimizar a definição do seu perfil com base na monitorização das suas actividades de navegação na Internet.

28. Todavia, os riscos para a protecção da privacidade e dos dados são muito reais. Se a privacidade e a protecção dos

([1]) Ver Parecer da Autoridade Europeia para a Protecção de Dados, de 22 de Julho de 2009, sobre a comunicação da Comissão relativa a um plano de acção para a implantação de sistemas de transporte inteligentes na Europa e sobre a proposta (que acompanha a comunicação) de directiva do Parlamento Europeu e do Conselho que estabelece um quadro para a implantação de sistemas de transporte inteligentes (STI) no transporte rodoviário, inclusive nas interfaces com outros modos de transporte, disponível no endereço Internet: http://www.edps.europa.eu/edpsWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_EN.pdf

([2]) Comunicação de 2.5.2007. COM(2007) 228 final da Comissão ao Parlamento Europeu e ao Conselho relativa à promoção da protecção de dados através de tecnologias de protecção da privacidade.

([3]) Estudo sobre os benefícios económicos das tecnologias de protecção da privacidade jls/2008/D4/036.

dados não forem tidas em conta desde o início, depois é, frequentemente, tarde de mais para corrigir os sistemas, ou essa correcção é excessivamente onerosa, e demasiado tarde para reparar os danos já causados. O número crescente de violações de dados nos últimos anos ilustra perfeitamente este problema e aumenta a necessidade de privacidade desde a concepção.

29. O que precede sugere claramente que os fabricantes e fornecedores de tecnologias TIC destinadas a tratar dados pessoais devem assumir, conjuntamente com os responsáveis pelo tratamento, a responsabilidade de as conceber com garantias de protecção dos dados e da privacidade já incorporadas. Em muitos casos, isto significa que elas devem ser concebidas com definições de privacidade por defeito.

30. Nestas condições, temos de estudar que medidas devem ser tomadas pelos decisores políticos para promover a privacidade desde a concepção no desenvolvimento das TIC. Uma primeira questão que se coloca é a de saber se o actual quadro jurídico relativo à protecção dos dados contém disposições adequadas para garantir a aplicação do princípio de privacidade desde a concepção tanto pelos responsáveis pelo tratamento como pelos fabricantes/criadores. Uma segunda questão é o que se deverá fazer no contexto da Agenda Digital Europeia para que o sector das TIC conquiste a confiança dos consumidores.

IV. **INSERÇÃO DO PRINCÍPIO DE PRIVACIDADE DESDE A CONCEPÇÃO NA LEGISLAÇÃO E NAS POLÍTICAS DA UE**

IV.1. **Actual quadro jurídico relativo à protecção de dados e à privacidade**

31. A União Europeia possui um sólido quadro em matéria de protecção dos dados e de privacidade consagrado na Directiva 95/46/CE ([1]), na Directiva 2002/58/CE ([2]) e na jurisprudência do Tribunal Europeu dos Direitos do Homem ([3]) e do Tribunal de Justiça.

32. A Directiva relativa à protecção de dados é aplicável a «qualquer operação ou conjunto de operações efectuadas sobre dados pessoais» (recolha, conservação, comunicação, etc.). Ela impõe o cumprimento de determinados princípios e obrigações às entidades que tratam dados pessoais («responsáveis pelo tratamento») e define os direitos individuais, como o direito de acesso aos dados pessoais. A Directiva Privacidade e Comunicações Electrónicas ocupa-se especificamente da protecção da privacidade no sector das comunicações electrónicas ([4]).

33. A actual Directiva relativa à protecção de dados não contém uma exigência explícita de privacidade desde a concepção, mas inclui disposições que de forma indirecta podem exigir a aplicação deste princípio em diversas situações. Nomeadamente, o artigo 17.º determina que os responsáveis pelo tratamento devem pôr em prática medidas técnicas e organizativas adequadas para prevenir o tratamento ilícito dos dados ([5]). A privacidade desde a concepção encontra-se, assim, abrangida de forma muito genérica. Além disso, as disposições da directiva visam principalmente os responsáveis pelo tratamento e a forma como tratam os dados pessoais. Não exigem explicitamente que as tecnologias da informação e das comunicações cumpram os requisitos de privacidade e protecção de dados, o que também envolveria os conceptores e os fabricantes de TIC, incluindo as actividades realizadas na fase de normalização.

34. A Directiva Privacidade e Comunicações Electrónicas é mais explícita. O artigo 14.º, n.º 3, dispõe que «Caso seja necessário, poderão ser adoptadas medidas para garantir que o equipamento terminal seja construído de uma forma compatível com o direito de os utilizadores protegerem e controlarem a utilização dos seus dados pessoais, em conformidade com o disposto na Directiva 1999/5/CE e na Decisão 87/95/CEE do Conselho, de 22 de Dezembro de 1986, relativa à normalização no domínio das tecnologias da informação e das telecomunicações». Contudo, esta disposição nunca foi utilizada ([6]).

35. Não obstante as supracitadas disposições das duas directivas serem úteis para a *promoção* da privacidade desde a concepção, na prática não foram suficientes para *garantir* a incorporação da privacidade nas TIC.

36. Em consequência da situação acima descrita, a lei não exige de forma suficientemente precisa que as TIC sejam concebidas de acordo com o princípio de privacidade

([1]) Directiva 95/46/CE do Parlamento Europeu e do Conselho, (a seguir designada por «Directiva relativa à protecção de dados»).

([2]) Directiva 2002/58/CE do Parlamento Europeu e do Conselho, (a seguir designada por Directiva «Privacidade e Comunicações Electrónicas»).

([3]) Interpretando os principais elementos e condições estabelecidos no artigo 8.º da Convenção Europeia para a Protecção dos Direitos do Homem e das Liberdade Fundamentais (CEDH), adoptada em Roma, em 4 de Novembro de 1950, consoante a sua aplicação a diferentes domínios.

([4]) O Tratado de Lisboa reforçou esta protecção ao reconhecer o respeito da vida privada e da protecção dos dados pessoais como direitos fundamentais distintos, nos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia. A Carta tornou-se vinculativa quando o Tratado de Lisboa entrou em vigor.

([5]) O artigo 17.º dispõe o seguinte: «Os Estados-membros estabelecerão que o responsável pelo tratamento deve pôr em prática medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição acidental ou ilícita, a perda acidental, a alteração, a difusão ou acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito». O considerando 46 complementa esta disposição afirmando «Considerando que a protecção dos direitos e liberdades das pessoas em causa relativamente ao tratamento de dados pessoais exige que sejam tomadas medidas técnicas e organizacionais adequadas tanto aquando da concepção do sistema de tratamento como da realização do próprio tratamento, a fim de manter em especial a segurança e impedir assim qualquer tratamento não autorizado».

([6]) A Comissão anunciou que tenciona actualizar a Directiva 1999/5/CE em finais de 2010.

desde a concepção. Além disso, as autoridades responsáveis pela protecção dos dados não possuem competências suficientes para garantir a incorporação desse princípio, o que gera ineficácia. Por exemplo, as autoridades responsáveis pela protecção dos dados podem ter condições para impor sanções por ausência de resposta aos pedidos de acesso apresentados por pessoas singulares e possuir as competências necessárias para exigir a aplicação de medidas que impeçam o tratamento ilícito dos dados. Todavia, nem sempre é suficientemente claro se os seus poderes incluem a possibilidade de exigir que um sistema seja concebido de forma a facilitar os direitos de protecção de dados das pessoas singulares ([1]). Por exemplo, com base nas actuais disposições jurídicas, não é claro que se possa exigir que a arquitectura de um sistema de informação seja concebida de modo a facilitar a resposta das empresas aos pedidos de acesso apresentados por pessoas singulares, para que esses pedidos possam ser tratados de forma automática e mais rápida. Além disso, as tentativas de alterar uma tecnologia depois de esta ter sido desenvolvida ou implantada podem originar uma amálgama de soluções que não funcionam inteiramente, para além de serem onerosas do ponto de vista económico.

37. Na opinião da AEPD, partilhada pelo Grupo do Artigo 29.º ([2]), o actual quadro jurídico deixa margem para um apoio mais explícito ao princípio de privacidade desde a concepção.

IV.2. **Integração da privacidade desde a concepção a diversos níveis**

38. Tendo em conta o que foi dito, a AEPD recomenda à Comissão que siga quatro linhas de acção:

a) Propor a inclusão de uma disposição geral referente à privacidade desde a concepção no quadro jurídico relativo à protecção de dados;

b) Desenvolver esta disposição geral de modo a formular disposições específicas, quando forem propostos instrumentos jurídicos específicos em diversos sectores. Essas disposições específicas já podem ser incluídas nos instrumentos jurídicos com base no artigo 17.º da Directiva relativa à protecção de dados (e noutra legislação existente);

c) Incluir a privacidade desde a concepção como princípio orientador na Agenda Digital Europeia;

d) Introduzir o princípio da privacidade desde a concepção noutras iniciativas da UE (principalmente não legislativas).

Uma disposição geral sobre a privacidade desde a concepção

39. A AEPD propõe que se inclua o princípio da privacidade desde a concepção, de forma inequívoca e explícita, no actual quadro regulamentar relativo à protecção de dados. Essa medida tornaria o dito princípio mais forte, mais explícito, e imporia a sua aplicação efectiva, além de conferir maior legitimidade às autoridades responsáveis pela aplicação da lei para exigirem a sua aplicação *de facto* na prática. Isto é particularmente necessário tendo em conta os factos acima descritos, não só pela importância do princípio em si mesmo como instrumento para favorecer a confiança, mas também como incentivo para as partes interessadas implementarem a privacidade desde a concepção e reforçarem as garantias previstas no quadro jurídico existente.

40. A presente proposta assenta na recomendação do Grupo do Artigo 29.º para que se introduza o princípio de «privacidade desde a concepção» como princípio geral no quadro jurídico relativo à protecção de dados, nomeadamente na Directiva relativa à protecção de dados. Segundo o Grupo do Artigo 29.º: «Este princípio deve ser vinculativo para os conceptores das tecnologias e para os seus produtores, bem como para os responsáveis pelo tratamento que têm de decidir sobre a aquisição e a utilização das TIC. Eles devem ser obrigados a ter a protecção tecnológica dos dados em conta logo na fase de planeamento dos procedimentos e sistemas das tecnologias da informação. Os fornecedores desses sistemas ou serviços, bem como os responsáveis pelo tratamento, devem demonstrar que tomaram todas as medidas necessárias para cumprir estes requisitos».

41. A AEPD também se congratula com o apoio dado pela Comissária Viviane Reding ao princípio da privacidade desde a concepção, no contexto do anúncio da revisão da Directiva relativa à protecção de dados ([3]).

42. A este propósito, importa abordar o conteúdo dessa regulamentação. Em primeiro lugar, e mais importante, um princípio geral de privacidade desde a concepção deve ser tecnologicamente neutro. Não deve pretender regulamentar a tecnologia, isto é, não deve prescrever soluções técnicas específicas. Em vez disso, deve estipular que os princípios de privacidade e protecção de dados existentes

([1]) Ver Relatório do Gabinete do Comissário da Informação do Reino Unido intitulado «Privacy by Design», publicado em Novembro de 2008.

([2]) Ver Parecer 168 do Grupo do Artigo 29.º «The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data», adoptado em 1 de Dezembro de 2009.

([3]) «A privacidade desde a fase de concepção é um princípio que interessa tanto aos cidadãos como às empresas. A privacidade desde a fase de concepção permitirá uma protecção mais eficaz das pessoas singulares e aumentará a confiança nos novos serviços e produtos, a qual terá, por sua vez, um impacto positivo na economia. Vi alguns exemplos animadores, mas ainda há muito a fazer». Discurso de Fundo no Dia da Protecção de Dados, 28 de Janeiro de 2010, no Parlamento Europeu, em Bruxelas.

sejam integrados nos sistemas e soluções de informação e comunicação. Deste modo, as partes interessadas, fabricantes, responsáveis pelo tratamento e autoridades responsáveis pela protecção de dados poderiam interpretar o significado do princípio em cada caso. Em segundo lugar, o cumprimento do princípio deve ser obrigatório em diversas fases, desde a criação de normas e da concepção da arquitectura até à sua aplicação pelo responsável pelo tratamento.

Disposições em instrumentos jurídicos específicos

43. Os instrumentos legislativos actuais e futuros devem integrar o princípio da privacidade desde a concepção com base no quadro jurídico actual e, após a adopção da disposição geral acima proposta, com base nesta última. Por exemplo, segundo as actuais iniciativas relativas aos sistemas de transporte inteligentes, a Comissão terá uma responsabilidade inicial específica na definição de medidas, iniciativas de normalização, procedimentos e melhores práticas. A privacidade desde a concepção deve ser um princípio orientador na realização destas tarefas.

44. A AEPD constata ainda que o princípio de privacidade desde a concepção também se reveste de uma importância específica no espaço de liberdade, de segurança e de justiça, sobretudo no que diz respeito aos objectivos da Estratégia de Gestão da Informação, prevista no Programa de Estocolmo ([1]). No seu parecer relativo ao Programa de Estocolmo, a AEPD destaca que a arquitectura do intercâmbio de informação se deve basear na «privacidade na concepção» ([2]): «Significa isto, em concreto, que a arquitectura dos sistemas de informação concebidos para efeitos de segurança pública deve sempre obedecer ao princípio da "privacidade na concepção"».

45. O Parecer do Grupo do Artigo 29.º sobre o futuro da privacidade ([3]) insiste em termos ainda mais precisos que, no espaço de liberdade, de segurança e de justiça — onde as autoridades públicas são os principais agentes e onde as medidas de aumento da vigilância afectam directamente os direitos fundamentais à privacidade e à protecção de dados — os requisitos de privacidade desde a concepção devem ser tornados obrigatórios. Ao introduzir estes requisitos nos sistemas de informação, os governos estimulariam também a privacidade desde a concepção na sua qualidade de «clientes pioneiros».

Privacidade desde a concepção como princípio orientador na Agenda Digital Europeia

46. As tecnologias de informação e comunicação são cada vez mais complexas e implicam maiores riscos para a privacidade e a protecção de dados. De um modo geral, a informação digitalizada, que é mais fácil de aceder, copiar e transmitir, está exposta a riscos muito maiores do que a informação em suporte papel. À medida que avançarmos para as redes de objectos interligados, esses riscos aumentarão. Quanto maiores forem os riscos para a privacidade e a protecção dos dados, maior será a procura de garantias reforçadas em matéria de protecção dos dados e de privacidade. Em consequência, a necessidade de aplicar a privacidade desde a concepção justifica-se mais fortemente no sector das TIC. Além disso, como já foi dito, a confiança das pessoas nas TIC é fundamental para os cidadãos aderirem aos novos serviços, sendo a privacidade e a protecção de dados elementos essenciais dessa confiança.

47. As considerações anteriores sublinham que a estratégia de desenvolvimento das TIC deve confirmar a necessidade de incluir na concepção das mesmas um elemento inerente de privacidade e protecção de dados, isto é, de tomar em consideração o princípio da privacidade desde a concepção.

48. Por conseguinte, a Agenda Digital Europeia deve apoiar explicitamente o princípio da privacidade desde a concepção como um elemento necessário para assegurar a confiança dos cidadãos nas TIC e nos serviços em linha. Ela deve reconhecer que a privacidade e a confiança estão associadas e que a privacidade desde a concepção deve ser um factor determinante no desenvolvimento de um sector das TIC digno de confiança.

A privacidade desde a concepção como princípio noutras iniciativas da UE

49. A Comissão deve adoptar a privacidade desde a concepção como princípio orientador na implementação de políticas, actividades e iniciativas em sectores específicos das TIC, incluindo a saúde em linha, os contratos públicos electrónicos, a segurança social em linha, a aprendizagem em linha, etc. Muitas dessas iniciativas figurarão entre as medidas previstas na Agenda Digital Europeia.

50. Isto significa, por exemplo, que as iniciativas para garantir aplicações governamentais mais eficientes e modernas, de modo a que as pessoas singulares possam interagir com as administrações, devem incluir a necessidade de que elas sejam concebidas e funcionem em conformidade com o princípio da privacidade desde a concepção. O mesmo se aplica às políticas e actividades da Comissão que promovem uma Internet mais rápida e determinados conteúdos digitais ou que, de um modo geral, incentivam as comunicações fixas e sem fios e a transmissão de dados.

([1]) Programa de Estocolmo — Uma Europa aberta e segura que sirva e proteja os cidadãos, aprovado pelo Conselho Europeu em Dezembro de 2009.

([2]) Parecer de 10 de Julho de 2009 sobre a Comunicação da Comissão ao Parlamento Europeu e ao Conselho «Um espaço de liberdade, de segurança e de justiça ao serviço dos cidadãos», JO C 276 de 17.11.2009, p. 8, ponto 60.

([3]) Parecer 168 do Grupo do Artigo 29.º: «The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data», adoptado em 1 de Dezembro de 2009.

51. O que foi dito inclui também os domínios em que a Comissão é responsável pelos sistemas informáticos em ampla escala, como o SIS e o VIS, bem como os casos em que a responsabilidade da Comissão está limitada ao desenvolvimento e à manutenção da infra-estrutura comum de um sistema desse tipo, como o Sistema Europeu de Informação sobre os Registos Criminais (ECRIS).

52. A forma exacta como o princípio de privacidade desde a concepção será desenvolvido dependerá de cada sector ou situação específicos. Por exemplo, quando as iniciativas da Comissão são acompanhadas por propostas legislativas relativas a um sector específico das TIC, em muitos casos será adequado incluir uma referência explícita ao conceito de privacidade desde a concepção aplicável à concepção dessa aplicação/sistema de TIC em particular. Se forem concebidos planos de acção para um domínio específico, eles devem assegurar a aplicação do quadro jurídico de forma sistemática e, mais especificamente, garantir que a criação da tecnologia de TIC em causa tem em conta a privacidade desde a concepção.

53. No que diz respeito à investigação, o Sétimo Programa-Quadro e os seguintes devem ser utilizados como um instrumento de apoio aos projectos que visam analisar as normas, as tecnologias e a arquitectura das TIC mais propícias à privacidade e, muito em especial, ao princípio da privacidade desde a concepção. Este último também deve ser um elemento imprescindível a ter em conta nos projectos mais vastos de TIC relativos ao tratamento dos dados pessoais dos cidadãos.

Domínios que suscitam preocupações específicas

54. Em alguns casos, devido aos riscos particulares que apresentam para a privacidade e a protecção de dados das pessoas ou a outros factores (resistência da indústria a fornecer produtos que incluam a privacidade desde a concepção, procura dos consumidores, etc.), pode ser necessário definir de forma mais explícita e específica as medidas de privacidade desde a concepção que devem ser integradas num dado tipo de produto/tecnologia da comunicação, em instrumentos legislativos ou não.

55. A AEPD identificou vários domínios (RFID, aplicações de redes sociais e de programas de navegação) que, no seu entender, merecem, nesta fase, uma análise cuidadosa da Comissão e a intervenção de carácter mais prático acima preconizada. Estes três domínios são a seguir analisados.

V. **IDENTIFICAÇÃO POR RADIOFREQUÊNCIAS**

56. As etiquetas RFID podem ser integradas em objectos, animais e pessoas. Podem ser utilizadas para recolher e armazenar dados pessoais tais como registos médicos, seguir os movimentos das pessoas ou caracterizar o comportamento destas para diversos fins. Todas estas acções podem ser efectuadas sem que as pessoas em causa tenham consciência disso ([1]).

57. É essencial que existam garantias eficazes em relação à protecção de dados, à privacidade e a todas as dimensões éticas associadas para que os cidadãos confiem na RFID e numa futura Internet das Coisas. Só então essa tecnologia poderá concretizar os seus numerosos benefícios económicos e societais.

V.1. **As lacunas do quadro jurídico de protecção de dados aplicável**

58. A Directiva relativa à protecção de dados e a Directiva Privacidade e Comunicações Electrónicas são aplicáveis à recolha de dados realizada através de aplicações RFID ([2]). Elas exigem, nomeadamente, que sejam adoptadas garantias de privacidade adequadas para utilizar as aplicações RFID ([3]).

59. Contudo, este quadro jurídico não aborda todas as preocupações em matéria de protecção de dados e de privacidade suscitadas por esta tecnologia. Isto deve-se ao facto de as directivas não serem suficientemente específicas

([1]) RFID significa «identificação por radiofrequências». As principais componentes da tecnologia *ou* da infra-estrutura de identificação por radiofrequências são uma *etiqueta* (isto é, um *microchip*), um leitor e uma aplicação ligada às etiquetas e aos leitores através do *middleware* (*software* da configuração) e do tratamento dos dados produzidos. A etiqueta consiste num circuito electrónico que armazena os dados e numa antena que os comunica através de ondas radioeléctricas. O leitor possui uma antena e um desmodulador que traduz as informações analógicas transmitidas pela ligação rádio em dados digitais. As informações podem ser depois enviadas através de redes para bases de dados e servidores, a fim de serem tratadas por computador.

([2]) A Directiva Privacidade e Comunicações Electrónicas refere-se à RFID no artigo 3.º «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 da Comunidade, nomeadamente nas redes públicas de comunicações que servem de suporte a dispositivos de recolha de dados e de identificação». Esta disposição é complementada pelo considerando 56): «O progresso tecnológico permite o desenvolvimento de novas aplicações com base em dispositivos de recolha de dados e identificação, nomeadamente dispositivos sem contacto que utilizam radiofrequências. Por exemplo, os dispositivos de identificação por radiofrequências (RFID) utilizam radiofrequências para captar dados provenientes de etiquetas inequivocamente identificadas, que podem em seguida ser transferidos através das redes de comunicações existentes. A utilização generalizada destas tecnologias pode proporcionar benefícios económicos e sociais consideráveis, contribuindo assim fortemente para o mercado interno, caso a sua utilização seja aceitável para os cidadãos. Para tal, é necessário assegurar a protecção dos direitos fundamentais dos cidadãos, nomeadamente a protecção da privacidade e dos dados pessoais. Quando tais dispositivos são ligados a redes de comunicações electrónicas acessíveis ao público ou utilizam serviços de comunicações electrónicas como infra-estrutura de base, deverão aplicar-se as disposições aplicáveis da Directiva 2002/58/CE (Directiva "Privacidade e Comunicações Electrónicas"), nomeadamente as respeitantes aos dados sobre segurança, tráfego e localização e à confidencialidade».

([3]) Por exemplo, o artigo 17.º da Directiva relativa à protecção de dados impõe a obrigação de pôr em prática medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição acidental ou ilícita, ou a difusão não autorizada.

quanto ao tipo de garantias que devem ser postas em prática nas aplicações RFID. As regras existentes têm de ser complementadas por outras regras que imponham garantias específicas, nomeadamente a obrigatoriedade de incorporar soluções técnicas (privacidade desde a concepção) na tecnologia RFID. Isto aplica-se às etiquetas que armazenam informações pessoais, as quais devem conter comandos de interrupção e utilizar criptografia nas etiquetas que armazenem certos tipos de dados pessoais.

V.2. **Auto-regulação como primeiro passo**

60. Em Março de 2007, a Comissão adoptou uma Comunicação ([1]) que reconhece, nomeadamente, a necessidade de orientações pormenorizadas para a utilização, na prática, da RFID e a conveniência de adoptar critérios de concepção que evitem riscos no domínio da privacidade e da segurança.

61. Para atingir estes objectivos, em Maio de 2009, a Comissão adoptou uma recomendação relativa à aplicação dos princípios de protecção da privacidade e dos dados nas aplicações RFID ([2]). Nas aplicações usadas no comércio retalhista, a recomendação requer que as etiquetas sejam desactivadas no ponto de venda, a menos que os consumidores consintam em mantê-las operacionais. Esta medida é aplicável a não ser que uma avaliação do impacto sobre a privacidade e a protecção dos dados demonstre que as etiquetas não constituem uma ameaça provável à privacidade ou à protecção dos dados pessoais, permanecendo, neste caso, operacionais após o ponto de venda, salvo se os cidadãos as quiserem desactivar, gratuitamente.

62. A AEPD concorda com a abordagem da Comissão à utilização de instrumentos de auto-regulação. No entanto, como se refere mais adiante, é concebível que a auto-regulação não produza os resultados esperados; apela, por isso, à Comissão que se prepare para adoptar medidas alternativas.

V.3. **Domínios de preocupação e possíveis medidas suplementares se a auto-regulação falhar**

63. A AEPD receia que as organizações que exploram as aplicações RFID no sector retalhista ignorem a possibilidade de as etiquetas RFID serem monitorizadas por terceiros indesejados. Essa monitorização pode revelar dados pessoais armazenados na etiqueta (caso existam), bem como permitir que um terceiro siga ou reconheça uma pessoa ao longo do tempo utilizando simplesmente os identificadores únicos contidos em uma ou mais etiquetas transportadas pela pessoa em causa, num ambiente que até pode estar fora do perímetro operacional da aplicação RFID. Está igualmente preocupada com a possibilidade de os operadores de aplicações RFID se sentirem tentados a recorrer indevidamente à excepção prevista, deixando, assim, a etiqueta operacional após o ponto de venda.

64. Se isso acontecer, poderá ser demasiado tarde para atenuar os riscos para a protecção dos dados e da privacidade dos cidadãos, que já poderá ter sido afectada. Além disso, dado o carácter da auto-regulação, as autoridades nacionais responsáveis pela aplicação da lei podem estar numa posição mais fraca para exigir às organizações operadoras das aplicações RFID que apliquem medidas específicas de privacidade desde a concepção.

65. Atendendo às considerações anteriores, a AEPD exorta a Comissão a preparar-se para propor instrumentos legislativos que regulem as principais questões de utilização da RFID, caso a aplicação efectiva do actual quadro jurídico falhe. A avaliação da Comissão não deve ser excessivamente adiada; esse adiamento poria as pessoas em risco, além de ser contraproducente para a indústria, pois as incertezas jurídicas são demasiado grandes e a correcção dos problemas, depois de estes se enraizarem, será provavelmente mais difícil e mais dispendiosa.

66. Entre as medidas que poderá ser necessário propor, a AEPD recomenda a previsão do princípio da opção de inclusão no ponto de venda, segundo o qual todas as etiquetas RFID apostas aos produtos de consumo devem ser sistematicamente desactivadas no ponto de venda. Poderá não ser necessário, ou adequado, que a Comissão especifique a tecnologia a utilizar em concreto, mas o direito da União deve estabelecer a obrigação legal de obter o consentimento dos consumidores para as etiquetas permanecerem activadas, permitindo que os operadores decidam a forma como irão cumprir esse requisito.

V.4. **Outras questões a considerar: o governo da Internet das coisas**

67. As informações produzidas pelas etiquetas RFID — por exemplo, informações sobre os produtos — podem vir a ser interligadas numa rede global de infra-estruturas de comunicação. Essa rede é normalmente designada por «Internet das coisas». As questões de protecção de dados e de privacidade surgem porque os objectos do mundo real podem ser identificados por etiquetas RFID que, adicionalmente às informações sobre os produtos, podem incluir dados pessoais.

68. Há muitas questões em aberto sobre quem irá gerir o armazenamento de informações relativas aos objectos etiquetados. Como serão organizadas? Quem terá acesso a elas? Em Junho de 2009, a Comissão adoptou uma Comunicação sobre a Internet das coisas ([3]) que identificou explicitamente os potenciais problemas de protecção de dados e de privacidade associados a este fenómeno.

([1]) Comunicação da Comissão, de 15.3.2007, 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 final.

([2]) Recomendação da Comissão, de 12.5.2009, relativa à aplicação dos princípios de protecção da privacidade e dos dados nas aplicações assentes na identificação por radiofrequências [C(2009) 3200 final].

([3]) Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões «A Internet das coisas — um plano de acção para a Europa», 18.6.2009, COM(2009) 278 final.

69. A AEPD gostaria de realçar algumas das questões levantadas pela comunicação e que, no seu entender, merecem ser atentamente acompanhadas à medida que a Internet das Coisas se desenvolve. Em primeiro lugar, a necessidade de uma arquitectura descentralizada pode facilitar a responsabilidade e a força executória do quadro jurídico da UE. Em segundo lugar, o direito das pessoas a não serem seguidas deve ser preservado, na medida do possível. Por outras palavras, o número de casos em que as pessoas são seguidas através de etiquetas RFID, sem o seu consentimento, deve ser muito limitado. Esse consentimento deve ser explícito. Isto é normalmente designado por «silêncio dos *chips*» e por direito a não ser incomodado. Por último, o princípio da privacidade desde a concepção deve ser um princípio orientador na concepção da Internet das coisas. Isso exige, por exemplo, que as aplicações concretas de RFID com mecanismos incorporados para possibilitar o controlo pelos utilizadores sejam concebidas com definições de privacidade por defeito.

70. A AEPD espera ser consultada quando a Comissão puser em prática as acções previstas na Comunicação, sobretudo sobre a elaboração da Comunicação sobre a privacidade e a confiança numa sociedade da informação omnipresente.

VI. AS REDES SOCIAIS E A NECESSIDADE DE DEFINIÇÕES DE PRIVACIDADE POR DEFEITO

71. As redes sociais estão na moda, parecendo ter ultrapassado o correio electrónico em termos de popularidade. Essas redes interligam pessoas que partilham interesses e/ou actividades semelhantes. As pessoas podem colocar os seus perfis em linha e partilhar ficheiros multimédia, como vídeos, fotografias e música, bem como os seus perfis profissionais.

72. Os jovens aderiram rapidamente às redes sociais e esta tendência continua. A média de idades dos utilizadores da Internet na Europa diminuiu nos últimos anos: as crianças de 9-10 anos ligam-se à Internet diversas vezes por semana e os jovens de 12-14 anos fazem-no diariamente, muitas vezes por uma a três horas.

VI.1. As redes sociais e o quadro jurídico aplicável em matéria de protecção de dados e privacidade

73. O desenvolvimento das redes sociais permitiu que os utilizadores carreguem para a Internet informações sobre eles próprios e sobre terceiros. Ao fazê-lo, no entender do Grupo do Artigo 29.º ([1]), os utilizadores da Internet actuam como responsáveis pelo tratamento, ex artigo 2,º, alínea d), da Directiva relativa à protecção de dados, relativamente aos dados que carregam ([2]). Contudo, na maioria dos casos, esse tratamento está abrangido pela excepção relativa às actividades domésticas ex artigo 3.º, n.º 2 da Directiva. Simultaneamente, os serviços das redes sociais são considerados como responsáveis pelo tratamento na medida em que fornecem os meios para o tratamento dos dados dos utilizadores e prestam todos os serviços básicos relacionados com a gestão dos utilizadores (por exemplo, registo e eliminação de contas).

74. Em termos jurídicos, isto significa que os utilizadores da Internet e os serviços de redes sociais partilham uma responsabilidade conjunta pelo tratamento de dados pessoais enquanto «responsáveis pelo tratamento» na acepção do artigo 2.º, alínea d), da Directiva, se bem que em diferentes graus e com tipos de obrigações diferentes.

75. Em consequência, os utilizadores devem saber e compreender que, ao tratarem as suas informações pessoais e as de outras pessoas, ficam abrangidos pelas disposições legislativas da UE em matéria de protecção de dados, as quais exigem, nomeadamente, que se obtenha o consentimento informado das pessoas cujas informações são carregadas e que se conceda a essas pessoas o direito de rectificação, oposição, etc. Do mesmo modo, os serviços de redes sociais devem, nomeadamente, pôr em prática as medidas técnicas e organizativas adequadas para prevenir o tratamento não autorizado, tendo em conta os riscos apresentados pelo tratamento e a natureza dos dados. Isto significa, por sua vez, que os serviços de redes sociais devem assegurar definições por defeito respeitadoras da privacidade, incluindo definições que restrinjam o acesso ao perfil do utilizador aos contactos escolhidos por ele próprio. As definições também devem exigir o consentimento prévio do utilizador antes de qualquer perfil ficar acessível a terceiros, não devendo os perfis de acesso restrito ser detectáveis por motores de pesquisa internos.

76. Infelizmente, existe uma discrepância entre os requisitos jurídicos e o seu cumprimento na prática. Apesar de, em termos jurídicos, os utilizadores da Internet serem considerados responsáveis pelo tratamento e terem a obrigação de respeitar o quadro da UE relativo à protecção dos dados e à privacidade, na realidade, estão frequentemente inconscientes desse seu papel. Geralmente, não entendem bem que estão a tratar dados pessoais e que a publicação dessas informações envolve riscos para a privacidade e a protecção de dados. Os jovens, em particular, colocam conteúdos em linha subestimando as eventuais consequências para si próprios e para os outros, por exemplo, no contexto de posteriores inscrições em estabelecimentos de ensino ou candidaturas a empregos.

([1]) Ver Parecer 163 do Grupo do Artigo 29.º, 5/2009 sobre as redes sociais em linha, adoptado em 12 de Junho de 2009.

([2]) «Responsável pelo tratamento», a pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais; sempre que as finalidades e os meios do tratamento sejam determinadas por disposições legislativas ou regulamentares nacionais ou comunitárias, o responsável pelo tratamento ou os critérios específicos para a sua nomeação podem ser indicados pelo direito nacional ou comunitário.

77. Ao mesmo tempo, os fornecedores de redes sociais pré-seleccionam, com frequência, as definições por defeito com base em derrogações, facilitando desse modo a difusão de informações pessoais. Alguns permitem que os perfis estejam por defeito disponíveis para os motores de pesquisa comuns. Esta situação põe em dúvida que as pessoas tenham efectivamente consentido na difusão dos seus dados e também que as redes sociais tenham cumprido o artigo 17.º da Directiva (acima referido), que as obriga a pôr em prática medidas técnicas e organizativas adequadas para prevenir o tratamento não autorizado.

VI.2. **Riscos gerados pelas redes sociais e acções sugeridas para os enfrentar**

78. A situação acima descrita origina um risco acrescido para a privacidade dos cidadãos e para a protecção dos seus dados. Ela expõe os utilizadores da Internet e as pessoas cujos dados foram carregados a violações flagrantes da sua privacidade e da protecção dos seus dados.

79. Neste contexto, a questão que a Comissão tem de analisar é o que deve e pode ser feito para pôr fim a essa situação. O presente parecer não dá uma resposta exaustiva a esta pergunta, mas apresenta várias sugestões para análise futura.

Investir na educação dos utilizadores da Internet

80. A primeira sugestão é de que se invista na educação dos utilizadores. Neste aspecto, as instituições da UE e as autoridades nacionais devem investir na sua educação e sensibilização para as ameaças colocadas pelos sítios de redes sociais. Por exemplo, a DG Sociedade da Informação tem vindo a gerir o Programa «Para uma Internet mais segura», cujo objectivo é capacitar e proteger as crianças e os jovens através, por exemplo, de actividades de sensibilização ([1]). Recentemente, as instituições da UE lançaram a campanha «Think before you post», que visa sensibilizá-los para os riscos de partilhar informações pessoais com estranhos.

81. A AEPD incentiva a Comissão a continuar a apoiar este tipo de actividades. Contudo, os próprios fornecedores de redes sociais também devem desempenhar um papel activo nesta matéria, visto terem a responsabilidade legal e social de ensinar os utilizadores a usarem os seus serviços de forma segura e respeitadora da privacidade.

82. Como já foi mencionado, quando são colocadas nas redes sociais, as informações podem ficar implicitamente disponíveis de várias maneiras. Por exemplo, podem ficar ao dispor do público em geral, incluindo motores de pesquisa, os quais as podem indexar e criar, assim, ligações directas às mesmas. Em contrapartida, as informações podem ficar restringidas ao acesso de «amigos seleccionados» ou permanecer totalmente privadas. Como é evidente, as autorizações de acesso aos perfis e a terminologia utilizada variam de sítio para sítio.

83. Contudo, como já foi dito, muito poucos utilizadores dos serviços de redes sociais sabem controlar o acesso à informação que colocam na Internet ou alterar as definições de privacidade por defeito. As definições de privacidade permanecem normalmente inalteradas porque os utilizadores desconhecem as consequências de não as alterarem ou não sabem como fazê-lo. Na maioria dos casos, portanto, a não alteração das definições de privacidade não significa que as pessoas tenham tomado uma decisão esclarecida de aceitar a partilha de informações. Nestas condições, é particularmente importante que terceiros como os motores de pesquisa não criem ligações a perfis individuais, no pressuposto de que os utilizadores (ao não alterarem as definições de privacidade) consentiram implicitamente em disponibilizar as informações de forma irrestrita.

84. Embora a educação dos utilizadores possa contribuir para solucionar esta situação, não é só por si suficiente para o fazer. Tal como recomenda o Grupo do Artigo 29.º no seu parecer sobre as redes sociais, os fornecedores destas últimas devem oferecer definições de privacidade, ou favoráveis à privacidade, a título gratuito. Deste modo, os utilizadores ficarão mais conscientes das suas acções e poderão fazer melhores escolhas sobre se querem partilhar informações e com quem.

Papel da auto-regulação

85. A Comissão estabeleceu um acordo com vinte fornecedores de redes sociais denominado «Safer Social Networking Principles for the EU» (Princípios para redes sociais mais seguras na UE) ([2]). O objectivo do acordo é melhorar a segurança dos menores quando utilizam sítios de redes sociais na Europa. Esses princípios incluem muitos dos requisitos resultantes da aplicação do quadro jurídico relativo à protecção de dados atrás descrito. Incluem, por exemplo, o requisito de oferecer aos utilizadores ferramentas e tecnologias que lhes permitam controlar a utilização e a difusão das suas informações pessoais, bem como a necessidade de fornecer definições de privacidade por defeito.

86. No início de Janeiro de 2010, a Comissão divulgou as conclusões de um relatório em que se avaliava a aplicação dos princípios ([3]). A AEPD está preocupada com o facto de este relatório demonstrar que, embora tenham sido tomadas algumas medidas, muitas outras não o foram.

([1]) Estão disponíveis informações sobre esse programa no endereço Internet: http://ec.europa.eu/information_society/activities/sip/index_en.htm

([2]) Os princípios estão disponíveis no endereço Internet: http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

([3]) «Report on the assessment of the implementation of the Safer Social Network Principles for the EU», disponível no endereço Internet: http://ec.europa.eu/information_society/activities/social_networking//docs/final_report/first_part.pdf

Por exemplo, o relatório encontrou problemas no tocante à comunicação das medidas e ferramentas de segurança disponíveis nos sítios. Constatou igualmente que menos de metade dos signatários do acordo restringem o acesso aos perfis dos menores apenas aos amigos destes.

Necessidade de definições de privacidade por defeito obrigatórias

87. Neste contexto, a questão fundamental é saber se são ou não necessárias medidas políticas adicionais para garantir que as redes sociais inserem definições de privacidade por defeito nos seus serviços. Esta questão foi levantada pela ex-Comissária para a Sociedade da Informação, Viviane Reding, que fez notar que poderá ser necessária legislação ([1]). Na mesma linha, o Comité Económico e Social Europeu afirmou que, paralelamente à auto-regulação, a legislação deveria impor normas de protecção mínimas ([2]).

88. Como foi acima mencionado, a obrigação dos fornecedores de redes sociais de aplicarem definições de privacidade por defeito pode ser indirectamente deduzida do artigo 17.º da Directiva relativa à protecção de dados ([3]), que obriga os responsáveis pelo tratamento a tomarem as medidas técnicas e organizativas adequadas («tanto aquando da concepção do sistema de tratamento como da realização do próprio tratamento») para manter a segurança e prevenir o tratamento não autorizado, tendo em conta os riscos que o tratamento apresenta e a natureza dos dados.

89. Contudo, este artigo é demasiado geral e pouco específico, também neste contexto. Ele não refere claramente o que se entende por medidas técnicas e organizativas adequadas no contexto das redes sociais. Deste modo, a situação actual carece de segurança jurídica, o que causa problemas tanto às entidades reguladoras como aos cidadãos cujos dados pessoais e privacidade não estão suficientemente protegidos.

90. Tendo em conta o que precede, a AEPD insta a Comissão a preparar legislação que inclua, no mínimo, um dever geral de introdução de definições de privacidade obrigatórias, associado a requisitos mais precisos:

a) Estabelecendo definições que restrinjam o acesso ao perfil do utilizador aos contactos que ele próprio escolheu. As definições também devem exigir o consentimento do utilizador antes de qualquer perfil ficar acessível a terceiros;

b) Determinando que os perfis de acesso restrito não devam ser detectáveis por motores de pesquisa internos ou externos.

91. Para além de se preverem definições obrigatórias de privacidade por defeito, resta saber se também seria adequado tomar medidas específicas de protecção de dados ou de outro tipo (por exemplo, em matéria de protecção de menores). Esta questão suscita outra mais vasta a respeito da conveniência de se criar um quadro específico para estes tipos de serviços que, além de prever definições de privacidade obrigatórias, regule outros aspectos. A AEPD solicita à Comissão que tome esta questão em consideração.

VII. **DEFINIÇÕES DE PRIVACIDADE POR DEFEITO NOS PROGRAMAS DE NAVEGAÇÃO PARA GARANTIR UM CONSENTIMENTO INFORMADO RELATIVAMENTE À RECEPÇÃO DE PUBLICIDADE**

92. Os fornecedores de redes de publicidade utilizam «cookies» (testemunhos de conexão) e outros dispositivos para monitorizar o comportamento dos utilizadores individuais quando navegam na Internet, a fim de catalogar os seus interesses e criar perfis. Estas informações são depois utilizadas para lhes enviar mensagens publicitárias direccionadas ([4]).

VII.1. **Desafios e riscos remanescentes no âmbito do actual quadro jurídico relativo à protecção de dados e à privacidade**

93. Este tratamento está abrangido pela Directiva relativa à protecção de dados (quando estão em causa dados pessoais) e também pelo artigo 5.º, n.º 3, da Directiva Privacidade e Comunicações Electrónicas. Este artigo exige especificamente que o utilizador seja informado e tenha a oportunidade de reagir consentindo ou rejeitando o armazenamento de dispositivos como os *cookies* no seu computador ou noutro equipamento ([5]).

94. Até à data, os fornecedores de redes de publicidade têm utilizado as definições dos programas de navegação e as declarações de privacidade para informar os utilizadores e

([1]) Viviane Reding, Comissária da Comissão Europeia responsável pela Sociedade da Informação e os Meios de Comunicação Social «Think before you post! How to make social networking sites safer for children and teenagers?» (Pensa antes de publicares informações! Como tornar os sítios de redes sociais mais seguros para as crianças e os adolescentes?) Dia da Internet mais Segura, Estrasburgo, 9 de Fevereiro de 2010.

([2]) Parecer do Comité Económico e Social Europeu sobre o impacto dos sítios de redes sociais nos cidadãos/consumidores, 4 de Novembro de 2009.

([3]) Também aprofundado no ponto 33 do presente documento.

([4]) Os testemunhos de conexão são pequenos ficheiros de texto que contêm um identificador único. Normalmente, os fornecedores de redes de publicidade (bem como os operadores ou editores de sítios Internet) colocam *cookies* no disco rígido dos visitantes, sobretudo no programa de navegação dos utilizadores da Internet, quando estes acedem pela primeira vez a sítios Internet que contêm anúncios que fazem parte da sua rede. O *cookie* permitirá que o fornecedor da rede de publicidade reconheça um antigo visitante que regresse a esse sítio Internet ou visite qualquer outro sítio Internet que seja parceiro da rede. Essas visitas repetidas permitirão que o fornecedor de redes crie um perfil do visitante.

([5]) O artigo 5.º, n.º 3, da Directiva Privacidade e Comunicações Electrónicas foi recentemente alterado no sentido de reforçar a protecção contra a intercepção das comunicações dos utilizadores através do recurso a, por exemplo, *software* espião (*spyware*) e *cookies* armazenados no computador de um utilizador ou noutro dispositivo. Nos termos da nova directiva, deve oferecer-se aos utilizadores uma melhor informação e formas mais fáceis de controlar se querem ou não *cookies* armazenados nos seus equipamentos terminais.

lhes permitir consentir ou rejeitar os *cookies*. Têm explicado nas declarações de privacidade dos editores como optar por não receber *cookies* nenhuns ou aceitá-los apenas em certos casos. Ao procederem deste modo, pretendem cumprir a sua obrigação de oferecer aos utilizadores o direito de recusar os *cookies*.

95. Embora teoricamente este método (através do programa de navegação) possa, na verdade, proporcionar um consentimento informado significativo, a realidade é muito diferente. De um modo geral, os utilizadores não têm conhecimentos básicos sobre a recolha de quaisquer dados, muito menos de terceiros, o valor desses dados, as suas utilizações, o funcionamento da tecnologia e, muito em especial, como e quando se podem auto-excluir. As medidas que os utilizadores devem tomar para se auto-excluírem afiguram-se não só complicadas mas também excessivas (em primeiro lugar, o utilizador deve definir o seu programa de navegação para aceitar os *cookies* e depois exercer a opção de auto-exclusão).

96. Em consequência, na prática, muito poucas pessoas exercem esta opção, não por terem tomado uma decisão informada de aceitar a publicidade comportamental, mas sim por não se aperceberem de que, ao não utilizarem a opção de auto-exclusão, estão de facto a aceitar essa publicidade.

97. Por conseguinte, embora em termos jurídicos o artigo 5.º, n.º 3, da Directiva Privacidade e Comunicações Electrónicas preveja uma protecção jurídica efectiva, na prática, considera-se que os utilizadores da Internet consentem ser monitorizados para fins de envio de publicidade comportamental quando, de facto, em muitos casos, se não na maioria deles, estão totalmente inconscientes de que essa monitorização está a ter lugar.

98. O Grupo do Artigo 29.º está a elaborar um parecer destinado a clarificar os requisitos legais da prática de publicidade comportamental, o que é positivo. No entanto, a interpretação pode não ser, só por si, suficiente para resolver esta situação e possivelmente será necessário que a União Europeia tome medidas adicionais.

VII.2. **Necessidade de medidas complementares, nomeadamente a previsão de definições de privacidade por defeito obrigatórias**

99. Tal como foi acima descrito, os programas de navegação na Internet permitem, normalmente, um certo nível de controlo sobre alguns tipos de *cookies*. Actualmente, as definições por defeito da maioria desses programas aceitam todos os *cookies*. Por outras palavras, por defeito, os programas de navegação estão definidos para aceitar todos os *cookies*, independentemente da finalidade destes últimos. O utilizador só deixará de receber *cookies* se alterar as definições da sua aplicação de navegação para eles serem recusados, o que, como já foi referido, muito poucos utilizadores fazem. Além disso, não existe um assistente de privacidade na primeira instalação ou actualização das aplicações dos programas de navegação.

100. Uma forma de mitigar o problema supramencionado consistiria em dotar os programas de navegação com definições de privacidade por defeito, ou seja, dotá-los da definição de «não-aceitação de *cookies* de terceiros». Para complementar esta medida e torná-la mais eficaz, os programas de navegação deveriam exigir que os utilizadores passassem por um assistente de privacidade quando instalam ou actualizam o programa de navegação. Há necessidade de informações mais pormenorizadas e claras sobre os tipos de *cookies* e a utilidade de alguns deles. Os utilizadores que queiram ser monitorizados para receberem publicidade serão devidamente informados e terão de alterar as definições dos programas de navegação. Deste modo, obterão maior controlo sobre os seus dados pessoais e a sua privacidade. No entender da AEPD, esta seria uma forma eficaz de respeitar e preservar o consentimento dos utilizadores ([1]).

101. Tendo em conta, por um lado, a amplitude do problema, isto é, o número de utilizadores da Internet que são actualmente monitorizados com base num consentimento que é ilusório, e, por outro lado, a escala dos interesses em causa, a necessidade de garantias suplementares torna-se mais premente. A aplicação do princípio de privacidade desde a concepção nas aplicações dos programas de navegação poderia fazer uma enorme diferença no sentido de dar controlo aos cidadãos sobre as práticas de recolha de dados utilizadas para fins publicitários.

102. Por estes motivos, a AEPD insta a Comissão a ponderar a adopção de medidas legislativas que exijam a introdução de definições de privacidade por defeito obrigatórias nos programas de navegação e o fornecimento de informações a esse respeito.

VIII. **OUTROS PRINCÍPIOS DESTINADOS A PROTEGER A PRIVACIDADE E OS DADOS PESSOAIS**

103. Embora o princípio de privacidade desde a concepção tenha um grande potencial para melhorar a protecção dos dados pessoais e da privacidade dos cidadãos, é necessário formular e aplicar na legislação princípios complementares que visem garantir a confiança dos consumidores nas TIC. É neste contexto que a AEPD aborda o princípio de responsabilidade e a conclusão de um quadro relativo às violações da segurança de carácter obrigatório e aplicável a nível intersectorial.

VIII.1. **O princípio de responsabilidade para garantir o cumprimento do princípio de privacidade desde a concepção**

104. O documento do Grupo do Artigo 29.º intitulado «O futuro da privacidade» ([2]) recomendou a inclusão do princípio de responsabilidade na Directiva relativa à protecção

([1]) Simultaneamente, a AEPD está ciente de que ela não resolveria completamente o problema, na medida em que há *cookies* que não podem ser controlados através do programa de navegação, como é o caso dos denominados «flash *cookies*». Para estes últimos, seria necessário que os criadores dos programas de navegação integrassem controlos «flash» nos seus controlos dos cookies por defeito nas versões dos novos programas de navegação.

([2]) Parecer 168 do Grupo do Artigo 29.º: «The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data», adoptado em 1 de Dezembro de 2009.

de dados. Este princípio, que é reconhecido em alguns instrumentos plurinacionais de protecção dos dados [1], exige que as organizações implementem processos para dar cumprimento às leis existentes e instituam métodos de avaliação e demonstração da conformidade com a lei e com outros instrumentos vinculativos.

105. A AEPD apoia inteiramente a recomendação do Grupo do Artigo 29.º. Considera que este princípio será muito relevante para promover a aplicação efectiva dos princípios e obrigações de protecção dos dados. Ele exigirá que os responsáveis pelo tratamento demonstrem ter adoptado o mecanismo necessário para dar cumprimento à legislação de protecção dos dados aplicável. É provável que isso contribua para uma aplicação efectiva da privacidade desde a concepção nas tecnologias TIC, como elemento particularmente apropriado para demonstrar responsabilidade.

106. Para avaliar e demonstrar a responsabilidade, os responsáveis pelo tratamento podem recorrer a procedimentos internos e a terceiros que realizem auditorias ou outros tipos de controlos e verificações, em resultado das quais podem ser concedidos chancelas ou prémios. Neste contexto, a AEPD insta a Comissão a ponderar se, para além de um princípio de responsabilidade geral, poderá ser útil que a legislação exija medidas de responsabilidade específicas, como a necessidade de realizar avaliações de impacto em matéria de privacidade e protecção de dados, e em que circunstâncias.

VIII.2. **Violação da segurança: completar o quadro jurídico**

107. As alterações à Directiva Privacidade e Comunicações Electrónicas adoptadas no ano passado introduziram um requisito de notificação das violações de dados às pessoas afectadas e também às autoridades competentes. Em termos gerais, entende-se por violação de dados qualquer violação que provoque a destruição, a perda, a divulgação, etc., de dados pessoais transmitidos, armazenados ou de outro modo tratados no contexto da prestação de serviços. As pessoas terão de ser notificadas se os seus dados pessoais ou a sua privacidade puderem ser afectados negativamente por uma tal violação. É o que acontece sempre que esta última possa resultar em roubo de identidade, humilhações ou danos significativos à reputação. Todas as violações de dados devem ser notificadas às autoridades competentes, independentemente de haver ou não risco para as pessoas.

Aplicação intersectorial das obrigações relativas à violação da segurança

108. Infelizmente, esta obrigação só é aplicável aos prestadores de serviços de comunicações electrónicas acessíveis ao público, como as sociedades prestadoras de serviços telefónicos, os fornecedores de acesso à Internet, os fornecedores de serviços de *Webmail*, etc. A AEPD insta a Comissão a apresentar propostas relativas à violação da segurança aplicáveis a nível intersectorial. Quanto ao conteúdo desse enquadramento, a AEPD considera que o quadro jurídico relativo às violações da segurança adoptado na Directiva Privacidade e Comunicações Electrónicas estabelece um equilíbrio adequado entre a protecção dos direitos dos cidadãos, incluindo os seus direitos aos dados pessoais e à privacidade, e as obrigações impostas às entidades abrangidas. Além disso é um quadro verdadeiramente sólido, uma vez que conta com o apoio de importantes disposições executórias, que dotam as autoridades de suficientes poderes de investigação e de sanção em caso de incumprimento.

109. A AEPD insta, assim, a Comissão a adoptar uma proposta legislativa que aplique este quadro a nível intersectorial, se necessário com os devidos ajustamentos. Além do mais, essa medida garantiria a aplicação das mesmas normas e procedimentos a todos os sectores.

Completar o quadro jurídico incorporado na Directiva Privacidade e Comunicações Electrónicas através do procedimento de comitologia

110. A Directiva Privacidade e Comunicações Electrónicas atribui competências à Comissão para adoptar medidas técnicas de execução, isto é, medidas pormenorizadas relativas à notificação das violações de segurança, através de um procedimento de comitologia [2]. Esta atribuição de competências justifica-se para garantir a execução e a aplicação coerentes do quadro jurídico relativo às violações da segurança. Uma execução coerente contribui para garantir que os cidadãos de toda a Comunidade usufruem de um nível igualmente elevado de protecção e que as entidades abrangidas não são sobrecarregadas com requisitos de notificação divergentes.

111. A Directiva Privacidade e Comunicações Electrónicas foi adoptada em Novembro de 2009. Não parece existir nenhuma razão que justifique o adiamento do início dos trabalhos com vista à adopção das medidas técnicas de execução. A AEPD organizou dois seminários com o objectivo de partilhar e recolher experiências em matéria de notificação de violações dos dados. Ela gostaria de partilhar os resultados desse exercício e aguarda com expectativa a colaboração com a Comissão e outras partes interessadas no aperfeiçoamento do quadro jurídico global relativo às violações de dados.

112. A AEPD exorta a Comissão a tomar as medidas necessárias com brevidade. Antes de adoptar as medidas técnicas de execução, a Comissão deve realizar uma ampla consulta, nomeadamente à ENISA, à AEPD e ao Grupo do Artigo 29.º. Essa consulta também deve incluir outros «interessados», sobretudo com vista a reunir informações sobre os melhores meios técnicos e económicos disponíveis para essa execução.

---

[1] OCDE, 1980, Linhas de orientação sobre a protecção da privacidade e os fluxos transfronteiras de dados pessoais; Declaração de Madrid sobre a protecção da privacidade resultante da conferência «Global Privacy Standards for a Global World», de 3 de Novembro de 2009.

[2] O procedimento de comitologia envolve a adopção de medidas técnicas de execução através de um comité de representantes dos Estados-Membros presidido pela Comissão. Para a Directiva Privacidade e Comunicações Electrónicas, é aplicável o denominado procedimento de regulamentação com controlo, o que significa que o Parlamento Europeu, bem como o Conselho, podem opor-se às medidas propostas pela Comissão. Ver ainda: http://europa.eu/scadplus/glossary/comitology_en.htm

IX. **CONCLUSÕES**

113. A confiança, ou melhor a ausência desta, foi identificada como uma questão fundamental para a emergência e a implantação bem sucedida das tecnologias da informação e das comunicações. Se as pessoas não confiarem nas TIC, é provável que estas falhem. A confiança nas TIC depende de diversos factores, sendo fundamental garantir que essas tecnologias não afectam os direitos fundamentais das pessoas à privacidade e à protecção dos dados pessoais.

114. A fim de reforçar ainda mais o quadro jurídico relativo à protecção dos dados e à privacidade, cujos princípios permanecem totalmente válidos na sociedade da informação, a AEPD propõe que a Comissão integre a privacidade desde a concepção nos diversos níveis legislativos e de elaboração de políticas.

115. Recomenda à Comissão que siga quatro eixos de acção:

a) Propor a inclusão de uma disposição geral relativa à privacidade desde a concepção no quadro jurídico relativo à protecção de dados. Esta disposição deve ser neutra do ponto de vista tecnológico e o seu cumprimento deve ser obrigatório nas diversas etapas;

b) Desenvolver esta disposição de carácter geral em disposições específicas, quando forem propostos instrumentos jurídicos específicos nos diferentes sectores. Estas disposições específicas já podem ser incluídas nos instrumentos jurídicos, com base no artigo 17.º da Directiva relativa à protecção de dados (e noutra legislação existente);

c) Incluir a privacidade desde a concepção como princípio orientador na Agenda Digital Europeia;

d) Introduzir o princípio da privacidade desde a concepção noutras iniciativas da UE (sobretudo não legislativas).

116. Nos três domínios das TIC designados, a AEPD recomenda à Comissão que avalie a necessidade de apresentar propostas de aplicação do princípio da privacidade desde a concepção de formas específicas:

a) Em relação à RFID, propor medidas legislativas que regulem os principais problemas suscitados pela utilização da RFID, caso a aplicação efectiva do actual quadro jurídico através da auto-regulação falhe. Em especial, prever o princípio de inclusão no ponto de venda, segundo o qual todas as etiquetas RFID apostas a produtos de consumo são desactivadas por defeito no ponto de venda;

b) Em relação às redes sociais, elaborar legislação que inclua, no mínimo, um dever geral de adopção de definições de privacidade obrigatórias, associado a requisitos mais precisos, relativos à restrição do acesso aos perfis dos utilizadores aos contactos escolhidos por eles próprios, e que determine que os perfis de acesso restrito não sejam detectáveis por motores de pesquisa internos ou externos;

c) Em relação à publicidade direccionada, ponderar a adopção de legislação que obrigue as definições dos programas de navegação a rejeitarem os *cookies* de terceiros por defeito e exija que os utilizadores passem por um assistente de privacidade quando instalam ou actualizam o programa de navegação.

117. Por último, a AEPD sugere à Comissão que:

a) Pondere a aplicação do princípio de responsabilidade na actual Directiva relativa à protecção dos dados; e

b) Desenvolva um quadro de regras e procedimentos de execução das disposições da Directiva Privacidade e Comunicações Electrónicas relativas à notificação de violações da segurança, alargando o seu âmbito de modo a serem aplicáveis a todos os responsáveis pelo tratamento.

Feito em Bruxelas, em 18 de Março de 2010.

Peter HUSTINX

Autoridade Europeia para a Protecção de Dados