I

(Resoluções, recomendações e pareceres)

PARECERES

AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS

Parecer da Autoridade Europeia para a Protecção de Dados 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

(2008/C 101/01)

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,

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

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

ADOPTOU O SEGUINTE PARECER:

I. **INTRODUÇÃO**

1. Em 15 de Março de 2007, a Comissão aprovou uma comunicação intitulada «Identificação por radiofrequências (RFID) na Europa: rumo a um quadro político» ([1]) (a seguir designada «Comunicação»). Nos termos do artigo 41.º do Regulamento (CE) n.º 45/2001, a AEPD é responsável por aconselhar as instituições e órgãos comunitários sobre todas as questões relativas ao tratamento de dados pessoais. Em conformidade com o referido artigo, a AEPD apresenta o presente parecer.

2. O presente parecer deve ser encarado como uma reacção da AEPD à referida Comunicação e a outras medidas no domínio da RFID tomadas desde a aprovação da Comunicação. Eis as outras medidas pertinentes tidas em conta no presente parecer:

   — Decisão da Comissão, de 28 de Junho de 2007, que cria um Grupo de Peritos para a Identificação por Radiofrequências ([2]), que constitui uma consequência directa da Comunicação. Este grupo é também conhecido por Grupo das Partes Interessadas na RFID. Em conformidade com a alínea b) do n.º 4 do artigo 4.º da decisão, a AEPD participa nas actividades do grupo na qualidade de observadora,

   — Resolução do Conselho, de 22 de Março de 2007, sobre a estratégia para uma sociedade da informação segura na Europa ([3]),

   — projecto «RFID e gestão da identidade», lançado pelo Parlamento Europeu ([4]),

([1]) COM(2007) 96 final.
([2]) Decisão n.º 467/2007/CE (JO L 176 de 6.7.2007, p. 25).
([3]) JO C 68 de 24.3.2007, p. 1.
([4]) Projecto «*RFID and identity management — Case studies from the frontline of the development towards ambient intelligence*» [«RFID e gestão da identidade — Estudos de caso da vanguarda do desenvolvimento rumo à inteligência ambiente»], encomendado pelo Serviço de Avaliação das Opções Científicas e Técnicas (STOA) do Parlamento Europeu e levado a cabo pelo ETAG (Grupo Europeu de Avaliação Tecnológica): http://www.europarl.europa.eu/stoa/default_en.htm

— aprovação, pelo Grupo do artigo 29.º para a protecção de dados, do parecer n.º 4/2007, de Junho de 2007, sobre o conceito de «dados pessoais» ([1]),

— 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 ([2]), e parecer da AEPD sobre esta comunicação, emitido em 25 de Julho de 2007 ([3]),

— aprovação pela Comissão de 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 ([4]).

3. A AEPD congratula-se com a Comunicação da Comissão sobre a RFID, por esta tratar das principais questões colocadas pela implantação da tecnologia RFID sem descurar as questões determinantes relacionadas com a privacidade e a protecção de dados. Esta Comunicação beneficiou de um trabalho preparatório coerente e rigoroso. Com efeito, foi precedida de cinco seminários temáticos e de uma consulta pública em linha ([5]) lançada pela Comissão.

4. A AEPD concorda com a opinião segundo a qual os sistemas RFID poderão desempenhar um papel-chave no desenvolvimento da Sociedade da Informação, habitualmente denominada «Internet das coisas», e partilha plenamente das preocupações mencionadas no ponto 3.2 da Comunicação quanto à possibilidade de os sistemas RFID virem ameaçar a privacidade individual e os direitos em matéria de protecção de dados. De facto, no seu Relatório Anual de 2005 a AEPD incluiu a RFID, juntamente com a biometria, os ambientes inteligentes e os sistemas de gestão da identidade no grupo dos desenvolvimentos tecnológicos que, segundo se prevê, irão ter um grande impacto na protecção de dados.

5. No entender da AEPD, para a utilização das tecnologias RFID na vida quotidiana e a sua aceitação pelo público em geral não contribuirá apenas a atracção que representam a sua comodidade e os novos serviços oferecidos, mas também as vantagens conferidas por garantias de protecção de dados adaptadas e coerentes.

6. Resumindo, a AEPD considera que a RFID constitui um avanço tecnológico fundamentalmente novo, designado com razão pela Comissão como porta de entrada para uma nova fase de desenvolvimento da Sociedade da Informação.

7. Este avanço levanta importantes questões em diversos domínios, entre os quais o da protecção de dados e da privacidade. O presente parecer da AEPD limita-se a este último domínio.

II. TEMA FULCRAL DO PARECER

8. O presente parecer focaliza-se, em particular, nas possíveis consequências destes desenvolvimentos para a protecção de dados e a privacidade. De momento, ainda não se sabe bem ao certo quais serão essas consequências, em parte devido ao facto de o desenvolvimento dos sistemas RFID e a sua utilização na vida quotidiana se encontrarem em plena evolução e de não se ver claramente onde tudo isso irá dar.

9. Nesta perspectiva, a AEPD adopta a seguinte abordagem:

— em primeiro lugar, é necessário clarificar as consequências práticas que a implantação dos sistemas RFID terá para a protecção de dados e a privacidade,

— em segundo lugar, há que especificar essas consequências, no contexto do quadro jurídico existente em matéria de protecção de dados e privacidade,

— em terceiro lugar, a AEPD aborda a questão de saber se essas consequências requerem regras mais específicas para enfrentar as questões de protecção de dados suscitadas pela utilização das tecnologias RFID. Esta questão, que já foi abordada pela AEPD no seu parecer sobre a Comunicação referente à Directiva «Protecção de Dados», será tratada em maior profundidade no presente parecer.

10. Ao seguir esta abordagem, a AEPD visa contribuir para que o desenvolvimento dos sistemas RFID e a sua utilização na vida quotidiana atendam às legítimas preocupações surgidas quanto à necessidade de assegurar a protecção de dados e a privacidade.

III. CLARIFICAÇÃO DAS CONSEQUÊNCIAS

Sistemas e etiquetas RFID

11. Apesar do facto — já referido — de a situação se encontrar em plena evolução e de não haver certeza quanto aos resultados, é perfeitamente possível descrever as principais características destes desenvolvimentos do ponto de vista das suas consequências em matéria de protecção de dados.

([1]) Documento WP 136, publicado no sítio Web do Grupo.
([2]) 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, de 7 de Março de 2007 [COM(2007) 87 final].
([3]) JO C 255 de 27.10.2007, p 1. A seguir designado: «Parecer referente à Comunicação sobre a Directiva "Protecção de Dados"».
([4]) Proposta de directiva do Parlamento Europeu e do Conselho, de 13 de Novembro de 2007, 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 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 e o Regulamento (CE) n.º 2006/2004 relativo à cooperação no domínio da defesa do consumidor [COM(2007) 698 final]. A Directiva 2002/58/CE será designada a seguir por «Directiva "Privacidade e Comunicações Electrónicas"».
([5]) http://www.rfidconsultation.eu/

12. Ao avaliar os aspectos da tecnologia RFID com potenciais incidências para a protecção de dados e a privacidade, é extremamente importante não ter só em conta as etiquetas RFID, mas considerar a totalidade da infra-estrutura RFID: a etiqueta, o leitor, a sede, a base de dados de referência e a base de dados em que estão armazenados os dados produzidos pela associação etiqueta/leitor. Tal como salientado sucintamente na introdução da Comunicação, os dispositivos RFID não são apenas «etiquetas electrónicas», pelo que as questões relacionadas com a protecção de dados não se limitam exclusivamente às etiquetas, antes abarcando todas as partes da infra-estrutura RFID em geral. Na verdade, cada um desses elementos desempenha o seu papel, contribuindo para a implementação do quadro jurídico europeu em matéria de protecção de dados, quando necessário. Estes elementos serão estimulados pelas principais tendências verificadas na Sociedade da Informação em desenvolvimento: uma largura de banda quase ilimitada, uma rede universal de comunicação e uma infinita capacidade de armazenamento.

Impacto dos sistemas e etiquetas RFID

13. Não obstante a necessidade de adoptar uma abordagem mais ampla, como salientado no ponto anterior, justifica-se por várias razões que nos centremos primeiro na utilização da RFID na etiquetagem a nível de artigo nos produtos de consumo, como por exemplo no sector retalhista. A razão óbvia reside no facto de se prever um aumento cada vez maior da sua utilização, que parece caminhar para uma aplicação generalizada. Contrariamente a outras aplicações RFID de uso circunscrito ou limitado, a etiquetagem a nível de artigo poderá tornar-se uma aplicação de mercado de massa. Actualmente, já muitos produtos de consumo estão equipados com uma etiqueta RFID. Acresce que essa utilização pode vir a afectar um enorme número de pessoas cujos dados pessoais são susceptíveis de ser tratados de cada vez que adquiram um produto no qual esteja incorporada uma etiqueta RFID.

14. Haverá que dar uma atenção específica às consequências da etiquetagem RFID para os donos dos artigos. Os sistemas RFID poderão expandir a relação entre um artigo e o seu dono. Na sequência disso, o dono pode ser digitalizado e classificado como «de poucas posses» ou «alvo interessante» para futuras transacções; uma excessiva atribuição um-para-um ([1]) poderá conduzir a uma «punição» automática de determinado comportamento (obrigação de reciclagem, desperdício, etc.). As pessoas não deverão estar sujeitas ao processo de tomada de decisões automatizadas contra elas. Esta capacidade da RFID faz aumentar o risco de a Sociedade da Informação se aproximar cada vez mais de uma situação em que sejam tomadas decisões automatizadas e em que se utilize abusivamente a tecnologia para regular o comportamento humano.

15. Os dados armazenados numa etiqueta RFID ou por ela produzidos podem ser dados pessoais na acepção do artigo 2.º da Directiva «Protecção de Dados». Por exemplo, os cartões inteligentes utilizados para viajar podem conter informações de identificação e informações sobre as viagens recentes do titular. Se um indivíduo sem escrúpulos quisesse seguir a pista de determinadas pessoas, bastaria colocar estrategicamente leitores que fornecessem informações sobre os movimentos dos titulares dos cartões, violando assim a sua privacidade e os seus dados pessoais.

16. Poderão verificar-se idênticas ameaças à privacidade mesmo que as informações armazenadas na etiqueta RFID não incluam nomes de pessoas. As etiquetas RFID contêm identificações únicas associadas a produtos de consumo: se cada etiqueta tem uma identificação única, essa identificação pode ser utilizada para efeitos de vigilância. Por exemplo, se alguém usar um relógio que tenha uma etiqueta RFID com um número de identificação, este último poderá servir de identificador único para o portador do relógio, mesmo que a sua identidade não seja conhecida. Consoante o modo como a informação for utilizada — e posta em relação com o relógio propriamente dito ou com a pessoa — a directiva poderá ser ou não aplicável. Será aplicável, por exemplo, se for gerada informação acerca do paradeiro das pessoas que possa ser utilizada para controlar o seu comportamento, ou por exemplo para efeitos de diferenciação de preço, recusa de acesso ou exposição involuntária à publicidade.

17. Neste contexto, é necessário assegurar que as aplicações RFID sejam implantadas com as medidas tecnológicas necessárias para minimizar o risco de divulgação indesejada de informações. Essas medidas podem incluir a exigência de conceber a infra-estrutura RFID, em especial as etiquetas RFID, de forma a evitar esse resultado. Por exemplo, as etiquetas RFID podem ser implantadas com um «comando de interrupção» (*kill command*) que permita a sua desactivação. Esta opção voltará a ser debatida no capítulo IV do presente parecer.

18. Ao oferecer a possibilidade de seguir o rasto dos produtos após o ponto de venda, os sistemas RFID introduzem novas questões no debate sobre a privacidade. De facto, na análise do impacto desses sistemas haverá que ter em conta dois elementos: em que medida se considera que o artigo tem carácter pessoal, e qual a mobilidade do artigo ([2]).

19. O ciclo de vida de um objecto poderá também completar a análise de risco exigida e contribuir para a avaliação quantitativa das potenciais ameaças à privacidade. Considerando que uma etiqueta pode não ser desactivada, um produto de consumo final com um ciclo de vida longo poderá reunir um maior número de dados sobre o seu dono e permitir a formação de um perfil mais preciso. Por outro lado, um artigo com um ciclo de vida curto, como uma lata de refrigerante, que dura desde a produção até à fase de reciclagem, poderá apresentar menores riscos e requerer portanto medidas mais leves do que um produto com um ciclo de vida muito mais longo.

([1]) Dr.ª Sarah Spiekermann, Directora do Centro de Investigação sobre Economia da Internet, de Berlim: seminário sobre RFID e utilização omnipresente dos computadores, organizado pelo Diálogo Transatlântico dos Consumidores, 13 de Março de 2007.

([2]) Dara J. Glasser, Kenneth W. Goodman and Norman G. Einspruch, Chips, tags and scanners: Ethical challenges for radio frequency identification, Ethics and Information Technology [«Micropastilhas, etiquetas e scâneres: Desafios éticos para a identificação por radiofrequências, Ética e Tecnologia da Informação»], Volume 9, No 2/2007.

Questões de privacidade e protecção de dados colocadas pela implantação de um sistema RFID

20. Para compreender melhor as consequências dos sistemas RFID para a privacidade e a protecção de dados, podem distinguir-se cinco questões fundamentais.

21. A primeira questão prende-se com a identificação da pessoa em causa. Há mais de sessenta anos, o objectivo da etiqueta RFID era «Identificar o Amigo ou o Inimigo» que aí vinha. Hoje em dia, os sistemas RFID podem não só identificar elementos gerais de um objecto, mas também, em última instância, conduzir à identificação de uma pessoa, pelo que devem fazê-lo de uma forma que atenda às exigências da protecção de dados.

22. A segunda questão é a da identificação do(s) responsável(-eis) pelo tratamento. No caso dos sistemas RFID, a identificação do responsável pelo tratamento, tal como definido na alínea d) do artigo 2.º da Directiva «Protecção de Dados», poderá ser mais difícil, pelo que precisa de ser examinada mais atentamente. No entanto, a identificação do responsável pelo tratamento não deixa de ser uma fase crucial para o estabelecimento das responsabilidades de cada um dos intervenientes que deverão respeitar o quadro jurídico em matéria de protecção de dados. Durante o ciclo de vida da etiqueta, o responsável pelo tratamento dos dados poderá mudar várias vezes em função dos serviços adicionais susceptíveis de ser fornecidos em função do objecto etiquetado.

23. A terceira questão prende-se com o decrescente significado da distinção tradicional entre esfera privada e esfera pública. Embora no passado a distinção entre espaços privado e público também nem sempre tenha sido muito nítida, a maioria das pessoas tem consciência das fronteiras entre eles (e das zonas cinzentas) e toma decisões informadas ou intuitivas sobre a maneira de agir em conformidade. Segundo Hall ([1]), o espaço pessoal é habitualmente traduzido por distância física em relação aos outros. A gestão da privacidade pode ser também considerada como um processo dinâmico de regulação de fronteiras ([2]). Por conseguinte, não é de espantar que o carácter «sem fios» da comunicação a partir da etiqueta e a capacidade de leitura desta última para além do alcance da vista levantem problemas para a privacidade, diluindo essas fronteiras tradicionais e perturbando a sua gestão. Com efeito, receia-se que a pessoa possa perder algum ou todo o controlo sobre a gestão da distância de que beneficiava até agora. Assim, a distância de leitura dos primeiros sistemas RFID tem sido apontada tanto pelos defensores como pelos detractores desses sistemas.

24. A quarta questão prende-se com o tamanho e as propriedades físicas das etiquetas RFID. Dado que a etiqueta deve ser pequena e barata, as medidas de segurança que poderão ser aplicadas a este elemento do sistema RFID serão, por definição, limitadas. No entanto, o facto de a comunicação ser «sem fios» acrescenta mais uma série de riscos em comparação com uma comunicação por cabo, pelo que torna necessário aplicar requisitos de segurança adicionais.

25. A quinta questão reside na falta de transparência do tratamento. Os sistemas RFID podem conduzir à recolha e tratamento furtivos de informações susceptíveis de ser utilizadas para elaborar o perfil de uma pessoa. Para ilustrar esta consequência, basta comparar os sistemas RFID com o telemóvel, como já tem sido feito muitas vezes. Por um lado, o telemóvel beneficiou de um elevado nível de aceitação tecnológica, independentemente dos potenciais riscos de intrusão na privacidade. Poder-se-ia concluir que a RFID seria aceite da mesma maneira. Mas, por outro lado, há que salientar que o telemóvel é um objecto visível que ainda está sujeito ao controlo do utilizador final, uma vez que pode ser apagado. O mesmo não acontece com os sistemas RFID.

26. Embora a recolha e tratamento furtivos das informações possam ser legítimos, pode também acontecer, e em várias circunstâncias é mesmo muito provável que aconteça, que a recolha e tratamento desses dados sejam ilegítimos.

27. Os esclarecimentos dados neste capítulo permitem concluir o seguinte: a utilização em larga escala da tecnologia RFID é um facto fundamentalmente novo que pode ter um impacto capital na nossa sociedade e na protecção de direitos fundamentais da nossa sociedade, como a privacidade e a protecção de dados. A RFID pode trazer consigo uma mudança qualitativa.

IV. ESPECIFICAÇÃO DAS CONSEQUÊNCIAS

Introdução

28. O presente capítulo centrar-se-á principalmente no impacto da RFID na protecção de direitos fundamentais da nossa sociedade, como a privacidade e a protecção de dados. Este tema será abordado em duas partes, a primeira das quais consistirá numa breve descrição da forma como esses direitos fundamentais são protegidos ao abrigo do quadro jurídico em vigor. Numa segunda parte, a AEPD debruçar-se-á sobre as possibilidades de utilizar plenamente esse quadro jurídico. Esta aspiração foi introduzida no parecer referente à Comunicação sobre a Directiva «Protecção de Dados», que fala da necessidade de uma «plena aplicação das actuais disposições da directiva».

29. O ponto de partida é o seguinte: os novos avanços tecnológicos, designadamente os sistemas RFID, têm repercussões claras nos requisitos aplicáveis a um quadro jurídico eficaz para a protecção de dados. De igual modo, a necessidade de proteger eficazmente os dados pessoais de uma pessoa pode impor restrições à utilização destas novas tecnologias, pelo que a interacção tem duas faces: a tecnologia influencia a legislação e a legislação influencia a tecnologia ([3]).

([1]) Hall, E.T., 1966, The Hidden Dimension [«A dimensão escondida»] (1.ª ed.), Garden City, N.Y.: Doubleday.

([2]) Altman, I., 1975, The Environment and Social Behaviour [«O ambiente e o comportamento social»], Brooks/Cole Monterrey.

([3]) Ver observações da AEPD, de Março de 2006, sobre a comunicação da Comissão relativa à interoperabilidade das bases de dados europeias, publicadas no sítio Web da AEPD.

Protecção dos direitos fundamentais

30. A protecção dos direitos fundamentais à privacidade e à protecção de dados na União Europeia é em primeiro lugar garantida por um quadro legislativo tornado necessário pelo facto de se tratar de direitos reconhecidos no artigo 8.º da Convenção Europeia dos Direitos do Homem e das Liberdades Fundamentais e no artigo 7.º da Carta dos Direitos Fundamentais da União Europeia. O quadro legislativo relevante para a protecção de dados e a RFID consiste basicamente na Directiva 95/46/CE relativa à protecção de dados e na Directiva 2002/58/CE sobre privacidade e comunicações electrónicas ([1]).

31. O quadro legislativo geral para a protecção de dados estabelecido na Directiva 95/46/CE é aplicável à RFID na medida em que os dados tratados pelos sistemas RFID sejam abrangidos pela definição de dados pessoais. Em certos casos as aplicações RFID tratam claramente dados pessoais e são indubitavelmente abrangidas pela Directiva «Protecção de Dados», mas há também situações em que a aplicabilidade da referida directiva pode não ser tão óbvia. O parecer n.º 4/2007 do Grupo do artigo 29.º para a Protecção de Dados, relativo ao conceito de «dados pessoais», visa contribuir para uma definição mais clara e comummente aceite da noção de dados pessoais e atenuar, deste modo, essa incerteza ([2]).

32. No que respeita à Directiva «Privacidade e Comunicações Electrónicas», a situação é a que a seguir se descreve. Até à data, não está claramente determinado se esta directiva abrange as aplicações RFID. Por este motivo, a proposta de alteração da directiva, apresentada pela Comissão em 13 de Novembro de 2007, contém uma disposição destinada a especificar que a directiva abrange efectivamente determinadas aplicações RFID. No entanto, há outras aplicações RFID que poderão não estar abrangidas devido ao facto de esta directiva se limitar ao tratamento dos dados pessoais no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis em redes de comunicações públicas.

33. A protecção dos dados pessoais pode ser complementada por uma série de instrumentos de auto-regulação (quadro não legislativo). A utilização desses instrumentos é activamente promovida por ambas as directivas, em especial no artigo 27.º da Directiva relativa à Protecção de Dados, que estipula que os Estados-Membros e a Comissão promoverão a elaboração de códigos de conduta destinados a contribuir para a boa execução da directiva. Além disso, os instrumentos de auto-regulação poderão contribuir eficazmente para a execução das medidas de segurança exigidas pelo artigo 17.º da Directiva «Protecção de Dados» e pelo artigo 14.º da Directiva «Privacidade e Comunicações Electrónicas».

([1]) No ponto 59 do presente parecer será debatida a pertinência de uma terceira directiva, a saber, a Directiva 1999/5/CE do Parlamento Europeu e do Conselho, de 9 de Março de 1999, relativa aos equipamentos de rádio e equipamentos terminais de telecomunicações e ao reconhecimento mútuo da sua conformidade (JO L 91 de 7.4.1999, p. 10).

([2]) Ver, nomeadamente, p. 10 do parecer, citado na nota 5.

Plena aplicação do quadro existente

34. O parecer referente à Comunicação sobre a Directiva «Protecção de Dados» enumera uma série de instrumentos disponíveis para uma melhor aplicação da directiva. Os instrumentos não vinculativos enumerados nesse parecer são, na sua maioria, aplicáveis à RFID, nomeadamente as comunicações interpretativas ou outras comunicações, a promoção das melhores práticas, a utilização de rótulos de protecção da privacidade e o recurso a auditorias do respeito da privacidade realizadas por terceiros. No capítulo V será debatida a possibilidade de adoptar regras específicas para a RFID, ainda que seja também possível obter melhoramentos dentro do quadro actual.

Instrumentos de auto-regulação

35. A AEPD concorda com a Comissão em que, numa primeira fase, é conveniente deixar margem para a auto-regulação, permitindo às partes interessadas criarem rapidamente um enquadramento conforme com as disposições legais e contribuindo assim para criar um enquadramento jurídico mais seguro.

36. Espera-se que a Comissão, em consulta com o Grupo das Partes Interessadas na RFID, estimule e dirija este processo de auto-regulação. Neste contexto, a AEPD congratula-se por a Comissão anunciar, na Comunicação, que apresentará uma recomendação com orientações específicas que estabeleçam «*os princípios a aplicar pelas autoridades e outras partes interessadas no que respeita à utilização da RFID*».

37. A Comunicação prevê que a auto-regulação assuma a forma de um código de conduta ou de um código de boas práticas. No entender da AEPD, independentemente da forma que vier a assumir, a auto-regulação deverá:

— dar orientações concretas e práticas sobre os tipos específicos de aplicações RFID, contribuindo assim para a observância do quadro jurídico em matéria de protecção de dados,

— abordar as questões e problemas específicos que se levantam em matéria de protecção de dados no contexto das aplicações RFID em geral,

— contribuir para uma aplicação uniforme e harmonizada da Directiva «Protecção de Dados» à escala da UE, precisamente num sector em que é provável a utilização do mesmo tipo de aplicações RFID em toda a UE,

— ser aplicada por todas as partes interessadas relevantes. A não observância deverá ter consequências negativas (eventualmente financeiras).

38. A AEPD chama a atenção para uma questão em que a auto-regulação terá uma utilidade específica. Em relação às aplicações RFID que impliquem o tratamento de dados pessoais, a Directiva «Protecção de Dados» impõe aos responsáveis pelo tratamento uma série de obrigações, nomeadamente no artigo 17.º (segurança do tratamento) e no artigo 7.º (necessidade de o tratamento de dados só ser efectuado se houver fundamentos jurídicos apropriados). Nos termos dessas disposições, os responsáveis pelo tratamento devem, por um lado, estabelecer medidas contra a divulgação não autorizada dos dados. Por outro lado, os responsáveis pelo tratamento devem assegurar que o tratamento, como por exemplo a divulgação de informações através dos leitores, quando seja caso disso, só se efectue com o consentimento informado da pessoa à qual os dados se referem.

39. Estas disposições da Directiva «Protecção de Dados» podem ser interpretadas como exigindo que as aplicações RFID sejam implantadas com as soluções técnicas necessárias para prevenir ou minimizar os riscos de uma divulgação indesejada e assegurar que o tratamento ou a transferência de dados só se efectuem mediante um consentimento informado, se for caso disso. No entender da AEPD, a existência de tal obrigação (ou seja, a de aplicar as soluções técnicas necessárias para prevenir ou minimizar os riscos de uma divulgação indesejada) e a sua natureza vinculativa para os responsáveis pela implantação das aplicações RFID passará a ser ainda mais forte e mais clara se for incluída no futuro código de conduta ou código de boas práticas acima mencionado. Por estes motivos, a AEPD aconselha vivamente que a recomendação da Comissão inclua essa interpretação da Directiva «Protecção de Dados», salientando a existência da obrigação de, ao implantar as aplicações RFID, tomar as medidas tecnológicas necessárias para prevenir a indesejada recolha ou divulgação de informações.

Necessidade de orientações

40. A AEPD recomenda que a Comissão, em estreita cooperação com o Grupo de Peritos para a Identificação por Radiofrequências, elabore um ou mais documentos com orientações claras sobre a forma de aplicar o actual quadro jurídico ao ambiente RFID. As orientações deverão prever as formas de aplicar na prática os princípios estabelecidos na Directiva «Protecção de Dados» e na Directiva «Privacidade e Comunicações Electrónicas». No que se refere à abordagem global das orientações e ao seu conteúdo concreto, a AEPD tem a fazer as sugestões a seguir enunciadas.

41. As orientações que definirem os princípios aplicáveis à utilização da RFID deverão ser suficientemente focalizadas e adoptar uma abordagem sectorial. Uma abordagem única para todos os casos não permitirá alcançar o objectivo pretendido de assegurar um quadro claro e coerente. O âmbito das orientações deve antes limitar-se a aplicações sectoriais RFID bem definidas.

42. Além disso, as orientações devem propor métodos práticos e eficazes para elaborar técnicas e normas que possam contribuir para a conformidade dos sistemas RFID com o quadro jurídico em matéria de protecção de dados e que impliquem a utilização de uma tecnologia de «respeito da privacidade desde a concepção».

43. Ao aplicar o actual quadro jurídico ao ambiente RFID, deve ser dada especial atenção aos princípios e obrigações a que estão subordinados, em matéria de protecção de dados os responsáveis pelo tratamento das aplicações RFID. Assumem particular relevância as seguintes obrigações e princípios:

— o princípio do direito à informação, incluindo o direito de saber em que momento são recolhidos os dados, através de leitores, e, nos casos apropriados, o direito de saber que os produtos estão etiquetados,

— a noção de consentimento, que constitui um dos fundamentos jurídicos para o processamento dos dados. Esta noção traduz-se na obrigação de desactivar as etiquetas RFID no ponto de venda, a menos que a pessoa em causa tenha dado o seu consentimento ([1]). O direito de desactivar as etiquetas RFID também serve o objectivo de garantir a segurança da informação, ou seja, de assegurar que os dados tratados através de etiquetas RFID não sejam divulgados a terceiros indesejados,

— o direito de não ser objecto de decisões adversas baseadas unicamente no tratamento automatizado de um perfil pessoal definido.

44. No que respeita ao direito à informação, as orientações deverão estabelecer que as pessoas devem receber informações relativas ao tratamento dos seus dados pessoais. Em particular, as pessoas devem ser alertadas nomeadamente para i) a presença de leitores e de etiquetas RFID activadas nos produtos ou nas respectivas embalagens; ii) as consequências dessa presença em termos de recolha de informações, e iii) os fins para os quais serão utilizadas as informações recolhidas.

45. Poderá ser adequado utilizar logotipos como meio de informação. Os logotipos podem ser utilizados para alertar para a presença de leitores e etiquetas RFID destinados em princípio a permanecer activos. No entanto, a utilização de logotipos não será suficiente, por si só, para assegurar o tratamento leal dos dados, que exige que as pessoas em causa sejam informadas de uma forma clara e compreensível. A utilização de logotipos deverá ser considerada uma medida para completar outras informações mais pormenorizadas.

([1]) Para mais pormenores, ver pontos 46-50 do presente parecer.

Pedra angular: o princípio da opção de inclusão

46. Em relação a todas as aplicações RFID relevantes, as soluções deverão respeitar e implementar, como requisito prévio, o princípio da opção de inclusão no ponto de venda. Deixar que as etiquetas RFID continuem a transmitir informações após o ponto de venda deverá ser ilegal, a menos que o responsável pelo tratamento tenha fundamentos jurídicos apropriados para tal. Em princípio, os fundamentos jurídicos apropriados só serão a) o consentimento da pessoa em causa, ou b) o facto de essa divulgação ser necessária para fornecer um serviço, em resposta a um pedido específico e livre apresentado pela referida pessoa ([1]). Nestes casos, ambos os fundamentos jurídicos seriam válidos para justificar a opção de inclusão.

47. De acordo com o princípio da opção de inclusão, as etiquetas deverão ser desactivadas no ponto de venda, a menos que a pessoa que comprou o produto ao qual está associada a etiqueta manifeste o desejo de manter esta última activada. Ao exercer o direito de deixar a etiqueta activada, a pessoa estará a dar o seu consentimento ao posterior tratamento dos dados que lhe dizem respeito, consentindo por exemplo na transmissão dos dados ao leitor por ocasião da sua próxima visita ao responsável pelo tratamento.

48. Para fazer face à crescente diversidade das aplicações RFID e facilitar o desenvolvimento de novos modelos comerciais inovadores, a AEPD salienta que importa adoptar uma abordagem flexível. O princípio da opção de inclusão deve ser aplicado com flexibilidade.

49. Para aplicar o princípio da opção de inclusão existem várias possibilidades. Por exemplo, como alternativa à remoção da etiqueta, poder-se-á prever que a etiqueta seja bloqueada, temporariamente desactivada ou, de acordo com um modelo de política de segurança designado por «modelo do patinho ressuscitado» ([2]), fechada para um utilizador específico. No caso de uma etiqueta com um ciclo de vida curto, o endereço da etiqueta que aponta para informações armazenadas numa base de dados pode também ser apagado da base de dados de referência, evitando o posterior tratamento dos dados adicionais recolhidos pela etiqueta.

50. Para concluir, embora a AEPD alegue que a aplicação do «princípio da opção de inclusão» no ponto de venda constitui uma obrigação jurídica que já existe na maior parte das situações ao abrigo da Directiva «Protecção de Dados», há boas razões para especificar esta obrigação nos instrumentos de auto-regulação, inclusive para assegurar que o princípio seja aplicado da forma mais adequada. De qualquer modo, é necessário aplicá-lo especificamente no que se refere às aplicações RFID não abrangidas pela Directiva «Protecção de Dados».

Necessidade do «respeito da privacidade desde a concepção»

51. Para minimizar as ameaças à privacidade e à protecção de dados, a Comunicação da Comissão subscreve, no ponto 3.2, página 7, a ideia da especificação e adopção de critérios de concepção numa fase precoce. A AEPD congratula-se com esta abordagem. Com efeito, a adopção de especificações e critérios de concepção, também designada por «Melhores Técnicas Disponíveis» («MTD») contribuirá eficazmente para a regulamentação da protecção de dados e para os requisitos de segurança. Se for frequentemente reexaminada, esta identificação dos critérios tecnológicos e organizacionais irá reforçar o modelo de simbiose da privacidade com os requisitos de segurança que a União Europeia está a desenvolver.

52. A correcta definição de MTD em matéria de privacidade e segurança para os sistemas RFID será igualmente decisiva para a criação de um ambiente digno de confiança que reforce a ampla aceitação desses sistemas pelos utilizadores finais, bem como para a competitividade da indústria europeia.

53. O processo de selecção das MTD para os sistemas RFID deverá ser apoiado por avaliações em termos de privacidade e de segurança, sendo ainda necessário investir esforços nesse sentido. A AEPD considera que a Agência Europeia para a Segurança das Redes e da Informação (ENISA) e os Centros Comuns de Investigação da Comissão Europeia, associados às partes interessadas da indústria do sector, poderão contribuir para a identificação das melhores práticas e para a elaboração das metodologias neste domínio. Com o recente lançamento do projecto «Orientações técnicas em matéria de RFID», o Serviço Federal Alemão para a Segurança da Informação (BSI) deu um bom exemplo ilustrativo ([3]) das MTD que deverão agora ser desenvolvidas a nível europeu.

54. As normas podem também desempenhar um papel decisivo na adopção em fase precoce do princípio do «respeito da privacidade desde a concepção». Por conseguinte, a Comissão deverá contribuir para a adopção de salvaguardas em matéria de privacidade e protecção de dados na elaboração das normas internacionais aplicáveis à RFID. No seu documento de trabalho ([4]) sobre a RFID, o Grupo do artigo 29.º ilustrou claramente como as normas podem contribuir para um desenvolvimento de sistemas RFID respeitador da privacidade.

([1]) Nalgumas aplicações RFID, pode ser possível basear-se noutros fundamentos, com a alínea f) do artigo 7.º (interesses legítimos do responsável pelo tratamento, sob reserva de salvaguardas adequadas).

([2]) O nome deste modelo criado por Frank Stajano e Ross Anderson, da Universidade de Cambridge inspira-se no comportamento dos gansos recém-nascidos, que partem do princípio de que o primeiro objecto em movimento que vêem deve ser a mãe.

([3]) http://www.bsi.bund.de/veranst/rfid/index.htm

([4]) Documento de trabalho (WP 105) sobre as questões de protecção de dados relacionadas com a tecnologia RFID, 19 de Janeiro de 2005.

55. Além disso, a AEPD congratula-se com a posição adoptada pela Comissão no que respeita à investigação e desenvolvimento de novas tecnologias RFID e à necessidade de atenuar os riscos para a privacidade. De facto, o princípio de «respeito da privacidade desde a concepção» deve ser introduzido na fase mais precoce possível da elaboração das tecnologias, o que contribuirá melhor para a conformidade destas últimas com o quadro jurídico em matéria de protecção de dados. Como já anunciou no seu Relatório Anual de 2006, a AEPD vai associar-se a este esforço emitindo, caso a caso, pareceres e conselhos sobre os projectos do 7.º Programa-Quadro (2007-2013).

V. SÃO NECESSÁRIAS MEDIDAS LEGISLATIVAS ESPECÍFICAS?

56. A auto-regulação pode não ser um meio suficiente para assegurar a plena aplicação do quadro existente em matéria de protecção de dados e privacidade. Mesmo que a auto-regulação preencha os requisitos acima mencionados, a sua aplicação é facultativa e a não observância nem sempre pode ser punida eficazmente. Além disso, pode ser ainda necessário adoptar medidas legislativas vinculativas a fim de assegurar a protecção dos direitos das pessoas à privacidade e à protecção de dados. Essa necessidade será ainda maior em caso de insuficiência da abordagem de auto-regulação.

57. Uma das principais questões está em determinar os instrumentos jurídicos necessários para assegurar que as aplicações RFID sejam eficazmente implantadas com as soluções técnicas necessárias para prevenir ou minimizar os riscos para a protecção de dados e a privacidade, e que os responsáveis pelo tratamento tomem as medidas adequadas para cumprir as obrigações que lhes são impostas pelos quadros jurídicos existentes. Esta questão levanta algumas questões adicionais:

— são necessárias regras específicas?

— na afirmativa, podem essas regras ser adoptadas no âmbito do quadro legislativo em vigor, por exemplo recorrendo aos procedimentos comitológicos existentes?

— ou será necessário prever um novo instrumento legislativo para assegurar a eficaz implantação de aplicações RFID que incorporem tecnologias destinadas a reforçar a privacidade?

58. No presente capítulo estudaremos as possibilidades de estabelecer medidas legislativas vinculativas no âmbito do quadro jurídico existente, ao passo que no capítulo VI debateremos, visto tratar-se de uma questão separada, a necessidade de prever um novo instrumento legislativo.

59. Em primeiro lugar, há que dar uma atenção específica ao disposto no artigo 17.º da Directiva 95/46/CE, no n.º 3 do artigo 14.º da Directiva 2002/58/CE e na alínea c) do n.º 3 do artigo 3.º da Directiva 1999/5/CE. O n.º 3 do artigo 14.º da Directiva 2002/58/CE autoriza os Estados-Membros a adoptarem medidas para assegurar 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 ([1]). A Directiva 1999/5/CE prevê, na alínea c) do n.º 3 do artigo 3.º, que, de acordo com um procedimento de comitologia, a Comissão pode decidir que os aparelhos de certas classes de equipamento ou determinados tipos de aparelhos sejam construídos por forma a incluírem salvaguardas que assegurem a protecção dos dados pessoais e da privacidade do utilizador e do assinante. Até à data, a alínea c) do n.º 3 do artigo 3.º da Directiva 1999/5/CE ainda não foi aplicada.

60. Estas disposições dão ao legislador — a nível nacional e a nível comunitário — poderes para estipular que sejam incluídas no fabrico dos sistemas RFID salvaguardas em matéria de privacidade e protecção de dados, conceito conhecido por «respeito da privacidade desde a concepção» ([2]). É também preconizado o recurso às Melhores Técnicas Disponíveis.

61. Tendo em vista tornar obrigatória a utilização do conceito de «respeito da privacidade desde a concepção», a AEPD recomenda que a Comissão recorra ao mecanismo previsto na alínea c) do n.º 3 do artigo 3.º da Directiva 1999/5/CE, em consulta com o Grupo de Peritos para a Identificação de Radiofrequências.

62. Em segundo lugar, é possível especificar a aplicação à RFID do quadro legislativo em vigor, através da alteração das próprias directivas. Como já foi referido, a Comissão acaba de apresentar uma proposta de alteração da Directiva «Privacidade e Comunicações Electrónicas» que contém uma nova disposição nesse sentido. A AEPD congratula-se com esta primeira confirmação da aplicabilidade da directiva às aplicações RFID. No seu parecer sobre a proposta de alteração, a publicar nos princípios de 2008, a AEPD abordará as questões específicas levantadas pela relação entre a Directiva «Privacidade e Comunicações Electrónicas» e a RFID.

63. Atendendo a que a Comissão não prevê alterar, num futuro próximo, a Directiva «Protecção de Dados» ([3]), são limitadas as possibilidades de especificar que o quadro legislativo existente se aplica à RFID.

VI. É NECESSÁRIO UM QUADRO JURÍDICO ESPECÍFICO PARA A RFID?

Intenções da Comissão

64. A Comunicação salienta a importância da «segurança e privacidade asseguradas de raiz» ([4]). Preconiza também o envolvimento de todas as partes interessadas. O principal

([1]) E em conformidade com a Decisão 87/95/CEE do Conselho, de 22 de Dezembro de 1986, relativa à normalização no domínio das tecnologias da informação e das telecomunicações (JO L 36 de 7.2.1987, p. 31).
([2]) Ver capítulo IV.
([3]) A AEPD apoia esta abordagem: ver ponto 64.
([4]) Cf. ponto 4.1 da comunicação.

resultado das actividades da Comissão será «*uma recomendação que estabelece os princípios a aplicar pelas autoridades e outras partes interessadas no que respeita à utilização da RFID*». A referida recomendação será provavelmente adoptada na Primavera de 2008. A Comunicação menciona as ambições da Comissão em matéria legislativa, que apresentam duas vertentes. A Comissão:

— ponderará a inclusão de disposições adequadas em matéria de RFID na próxima proposta de alteração da Directiva «Privacidade e Comunicações Electrónicas». Tal como já foi referido, a Comissão propôs, em Novembro de 2007, uma alteração da Directiva «Privacidade e Comunicações Electrónicas» nesse sentido, confirmando a aplicabilidade da directiva às aplicações RFID ([1]), mas sem propor o alargamento do âmbito da directiva às redes privadas,

— avaliará a necessidade de novas medidas legislativas para assegurar a protecção dos dados e a privacidade.

65. De acordo com esta política, é de supor que a Comissão não preveja — pelo menos a curto prazo — propor nova legislação específica para assegurar a protecção de dados e a privacidade no domínio da RFID.

Parâmetros para o legislador

66. No seu parecer referente à Comunicação sobre a Directiva «Protecção de Dados», a AEPD apresentou algumas ideias gerais sobre as actividades legislativas relacionadas com o tratamento de dados pessoais, que passamos a resumir:

— em primeiro lugar, deverão ser mantidos os princípios essenciais da protecção de dados: «*Não são necessários novos princípios, embora sejam claramente necessários outros mecanismos administrativos que, por um lado, sejam eficazes e adequados a uma sociedade em rede e, por outro, minimizem os custos administrativos.*» ([2]),

— em segundo lugar, só devem ser apresentadas as propostas legislativas cuja necessidade e proporcionalidade estiverem suficientemente comprovadas. Por este motivo, a curto prazo não é de alterar o quadro legislativo geral aplicável à protecção de dados,

— em terceiro lugar, a evolução da sociedade poderá conduzir a quadros jurídicos específicos, a fim de adaptar os princípios da Directiva «Protecção de Dados» às questões suscitadas por tecnologias específicas como a RFID. É óbvio que também neste contexto deverão estar preenchidas as condições da necessidade e proporcionalidade.

67. Em seguida, será útil especificar as expectativas que o legislador deverá enfrentar no domínio da RFID:

— a legislação deverá ser flexível e deixar margem para as inovações e o desenvolvimento tecnológico. Tal deverá conduzir a uma legislação suficientemente neutra do ponto de vista tecnológico,

— em segundo lugar, é necessário que a legislação proporcione segurança jurídica. Tal deverá conduzir a uma legislação suficientemente específica. É imperioso que as partes interessadas saibam precisamente de que forma se encontra regulamentado o seu comportamento,

— em terceiro lugar, a legislação deve proteger eficazmente todos os legítimos interesses em jogo. Tal exige, em todas as circunstâncias, a execução da legislação e uma clara definição das responsabilidades: que parte é responsável por que comportamento? ([3]) Estes requisitos são ainda mais importantes quando estão em jogo a privacidade e a protecção de dados, direitos fundamentais das pessoas nos termos da Convenção Europeia dos Direitos do Homem e das Liberdades Fundamentais e da Carta dos Direitos Fundamentais da União Europeia.

Ponto de vista da AEPD

68. No entender da AEPD, é óbvio que nem todos os desenvolvimentos tecnológicos deverão conduzir a reacções por parte do legislador europeu. A evolução tecnológica pode ser rápida, ao passo que a adopção e entrada em vigor de legislação leva — e deve levar — tempo. A legislação deve resultar do equilíbrio entre todos os interesses em jogo. Quando o instrumento escolhido é a directiva, é necessário ainda mais tempo, uma vez que as directivas devem ser integralmente transpostas para os sistemas jurídicos dos Estados-Membros.

69. No entanto, tal como salientado em diversas partes do presente parecer, a RFID não é apenas mais um desenvolvimento tecnológico. A Comunicação refere-se à RFID como porta de entrada para uma nova fase de desenvolvimento da Sociedade da Informação, muitas vezes designada por «Internet das coisas», e as etiquetas RFID vão constituir elementos-chave dos ambientes de «inteligência ambiente». Esses ambientes constituem também passos importantes no desenvolvimento daquilo que muitas vezes é designado por «Sociedade da Vigilância» ([4]). Assim sendo, pode justificar-se uma acção legislativa no domínio da RFID. A RFID pode trazer consigo uma mudança qualitativa.

([1]) Ver proposta de novo artigo 3.º da Directiva 2002/58/CE.
([2]) Ponto 24 do parecer referente à Comunicação sobre a Directiva «Protecção de Dados».
([3]) Na terminologia da protecção de dados, isto implica a identificação do «responsável pelo tratamento».
([4]) Esta mensagem foi repetida numa declaração das autoridades para a protecção de dados adoptada em 2 de Novembro de 2006, em Londres, a consultar no sítio Web da AEPD: http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/51

70. Nesta perspectiva, a AEPD recomenda que se pondere a adopção (ou a proposta) de legislação comunitária que regulamente as principais questões ligadas à utilização da RFID nos sectores relevantes, no caso de não se verificar uma correcta aplicação do quadro jurídico existente. Após a sua entrada em vigor, essa medida legislativa deve ser considerada como *lex specialis* em relação ao quadro jurídico geral da protecção de dados.

71. A adopção desse instrumento jurídico teria as seguintes vantagens:

— o instrumento poderia estabelecer parâmetros substantivos para os mecanismos de auto-regulação,

— a perspectiva da adopção de um instrumento legislativo poderia revelar-se um incentivo eficaz para levar as partes interessadas a estabelecerem mecanismos de auto-regulação que ofereçam uma protecção especificamente adaptada.

72. Em termos mais práticos, para facilitar, a Comissão poderia ser convidada a elaborar um documento de consulta sobre os prós e os contras de uma legislação específica e dos principais elementos dessa legislação. Naturalmente, as partes interessadas poderiam ser convidadas a dar o seu contributo para essa consulta. De igual modo, o Grupo do artigo 29.º poderia também participar neste processo.

Eventuais modalidades

73. A intervenção do legislador poderá proporcionar um quadro jurídico concebido por medida, constituído por uma combinação de instrumentos regulamentares que especifiquem e complementem o quadro jurídico existente. Esse quadro jurídico por medida deverá basear-se nos princípios consagrados em matéria de protecção de dados, e centrar-se na repartição das responsabilidades e na eficácia dos mecanismos de controlo.

74. Uma das razões específicas para a necessidade dessa legislação por medida prende-se com o facto de nem todas as aplicações RFID implicarem o tratamento de dados pessoais. Por outras palavras, se as aplicações RFID não implicarem o tratamento de dados pessoais, as partes envolvidas no fabrico e na venda de produtos equipados com aplicações RFID não estão juridicamente vinculadas à obrigação de aplicarem medidas tecnológicas para prevenir escutas ou a instalação de leitores sem a devida informação às pessoas em causa. No entanto, como já ficou demonstrado, mesmo com essas aplicações RFID existem riscos para a privacidade decorrentes da possibilidade de exercer vigilância sobre as pessoas, o que requer o mesmo tipo de salvaguardas em matéria de privacidade. Pode ser precisamente o caso da etiquetagem a nível de artigo nos produtos de consumo antes do ponto de venda. Em suma, as aplicações RFID que não processam dados pessoais podem mesmo assim ameaçar a privacidade das pessoas ao permitir uma vigilância sub-reptícia e a utilização das informações para fins inaceitáveis.

75. A AEPD considera que se deve evitar este resultado pouco feliz. Dado que a actual legislação só parcialmente permite contrariar esta ameaça à privacidade, não permitindo evitá-la, por exemplo, no caso das aplicações RFID que não processam dados pessoais, e tendo em conta as insuficiências das soluções legislativas não vinculativas, afigura-se necessário recorrer a medidas legislativas obrigatórias para assegurar um resultado satisfatório.

76. Tais medidas deverão, de qualquer forma:

— estabelecer que o princípio da opção de inclusão no ponto de venda constitui uma obrigação precisa e irrecusável, inclusive para as aplicações RFID não abrangidas pela Directiva «Protecção de Dados» ([1]),

— assegurar que a implantação das aplicações RFID obedeça obrigatoriamente às características técnicas adequadas, que implicam o «respeito da privacidade desde a concepção».

VII. **QUESTÃO DA GOVERNAÇÃO**

77. Embora a dimensão «inerentemente transfronteiriça» dos sistemas RFID seja encarada na Comunicação apenas a nível do Mercado Interno, a AEPD considera que esta dimensão tem de ser enfrentada a um nível mais internacional. Numa loja, os sistemas RFID já são «transfronteiriços», atendendo a que a actividade da etiqueta pode não cessar no ponto de venda. Ao nível do sistema RFID em geral, estas tecnologias tornam-se também «transfronteiriças» nos casos em que pode ocorrer uma transferência de dados pessoais para um país terceiro por o produtor do artigo etiquetado, que faz parte do sistema RFID, se encontrar estabelecido fora do território da União Europeia ([2]).

78. De um ponto de vista mais prospectivo, a governação das bases de dados de identidades RFID de referência representa também uma dimensão crítica para uma correcta execução do quadro jurídico europeu em matéria de protecção de dados. A AEPD insta a que seja encontrada uma solução, já que não seria aceitável deixar que este quadro continuasse a desgastar-se.

79. A AEPD prevê que a questão da governação da RFID venha a constituir um enorme desafio que exigirá investimentos consideráveis. Haverá que encontrar a instância de negociação apropriada e a infra-estrutura de gestão mais indicada para assegurar que os direitos à protecção de dados sejam adequadamente respeitados nestes ambientes internacionais.

([1]) No capítulo IV é defendida a ideia de que o princípio da opção de inclusão no ponto de venda é uma obrigação jurídica que já existe nos termos da Directiva «Protecção de Dados».

([2]) As obrigações ligadas à transferência de dados pessoais são abordadas nos artigos 25.º e 26.º da Directiva «Protecção de Dados».

80. Nesta perspectiva, a AEPD convida a Comissão a apresentar os seus pontos de vista sobre a questão da governação, eventualmente em consulta com o Grupo das Partes Interessadas na RFID.

VIII. **CONCLUSÃO**

81. A AEPD congratula-se com a Comunicação da Comissão sobre a RFID, por esta tratar das principais questões colocadas pela implantação da tecnologia RFID sem descurar as questões determinantes relacionadas com a privacidade e a protecção de dados. A AEPD concorda com a opinião segundo a qual os sistemas RFID poderão desempenhar um papel-chave no desenvolvimento da Sociedade da Informação, habitualmente denominada «Internet das coisas».

Clarificação das consequências

82. A utilização em larga escala da tecnologia RFID é um facto fundamentalmente novo que pode ter um impacto capital na nossa sociedade e na protecção de direitos fundamentais, como a privacidade e a protecção de dados. A RFID pode trazer consigo uma mudança qualitativa.

83. Em matéria de privacidade e segurança, podem distinguir-se cinco questões fundamentais:

— a identificação da pessoa em causa,

— a identificação do(s) responsável(eis) pelo tratamento dos dados,

— o decrescente significado da distinção entre esfera pessoal e esfera pública,

— As consequências do tamanho e das propriedades físicas das etiquetas RFID,

— a falta de transparência do tratamento.

Especificação das consequências

84. O quadro legislativo geral para a protecção de dados estabelecido na Directiva 95/46/CE é aplicável à RFID na medida em que os dados tratados pelos sistemas RFID sejam abrangidos pela definição de dados pessoais.

85. No que respeita à Directiva «Privacidade e Comunicações Electrónicas»: a proposta de alteração da directiva, apresentada pela Comissão em 13 de Novembro de 2007, contém uma disposição destinada a especificar que a directiva abrange efectivamente determinadas aplicações RFID. No entanto, há algumas outras aplicações RFID que poderão não estar abrangidas devido ao facto de esta directiva se limitar ao tratamento dos dados pessoais no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis em redes de comunicações públicas.

86. A protecção dos dados pessoais pode ser complementada por uma série de instrumentos de auto-regulação. É conveniente deixar margem para a auto-regulação, desde que esta:

— dê orientações concretas e práticas sobre os tipos específicos de aplicações RFID,

— aborde as questões e problemas específicos que se levantam em matéria de protecção de dados no contexto das aplicações RFID em geral,

— contribua para uma aplicação uniforme e harmonizada da Directiva «Protecção de Dados» em toda a UE,

— seja aplicada por todas as partes interessadas relevantes.

87. A AEPD recomenda que a Comissão, em estreita cooperação com o Grupo de Peritos para a Identificação por Radiofrequências, elabore um ou mais documentos com orientações claras sobre a forma de aplicar o actual quadro jurídico ao ambiente RFID.

88. As orientações que definirem os princípios aplicáveis à utilização da RFID deverão ser suficientemente focalizadas e adoptar uma abordagem sectorial. As orientações devem propor métodos práticos e eficazes para elaborar técnicas e normas que possam contribuir para a conformidade dos sistemas RFID com o quadro jurídico em matéria de protecção de dados e que impliquem a utilização de tecnologia de «respeito da privacidade desde a concepção».

89. A AEPD congratula-se por a Comunicação da Comissão subscrever a ideia da especificação e adopção de critérios de concepção numa fase precoce.

90. Embora a AEPD considere que a aplicação do princípio da opção de inclusão no ponto de venda constitui uma obrigação jurídica que já existe na maior parte das situações ao abrigo da Directiva «Protecção de Dados», esta obrigação deverá ser especificada nos instrumentos de auto-regulação.

São necessárias medidas específicas?

91. Tendo em vista tornar obrigatória a utilização do conceito de «privacidade desde a concepção», a AEPD recomenda que a Comissão recorra ao mecanismo previsto na alínea c) do n.º 3 do artigo 3.º da Directiva 1999/5/CE, em consulta com o Grupo de Peritos para a Identificação de Radiofrequências.

92. A AEPD recomenda que se pondere a adopção (ou a proposta) de legislação comunitária que regulamente as principais questões ligadas à utilização da RFID nos sectores relevantes, no caso de não se verificar uma correcta aplicação do quadro jurídico existente. Após a sua entrada em vigor, essa medida legislativa deve ser considerada como *lex specialis* em relação ao quadro jurídico geral da protecção de dados. Essa medida legislativa deverá também responder às preocupações suscitadas por certas aplicações RFID no que se refere à privacidade e à protecção de dados, como no caso da etiquetagem a nível de artigo antes do ponto de venda, que pode não envolver necessariamente o tratamento de dados pessoais.

93. A Comissão deverá elaborar um documento de consulta sobre os prós e os contras de uma legislação específica e dos principais elementos dessa legislação.

94. A intervenção do legislador poderá proporcionar um quadro jurídico concebido por medida, constituído por uma combinação de instrumentos regulamentares que especifiquem e complementem o quadro jurídico existente. As medidas deverão, de qualquer forma:

— estabelecer que o princípio da opção de inclusão no ponto de venda constitui uma obrigação precisa e irrecusável, inclusive para as aplicações RFID não abrangidas pela Directiva «Protecção de Dados» ([1]),

— assegurar que a implantação das aplicações RFID obedeça obrigatoriamente às características técnicas adequadas, que implicam o «respeito da privacidade desde a concepção».

Questão da governação

95. A AEPD convida a Comissão a apresentar os seus pontos de vista sobre a questão da governação, eventualmente em consulta com o Grupo das Partes Interessadas na RFID.

Feito em Bruxelas, em 20 de Dezembro de 2007.

Peter HUSTINX

Autoridade Europeia para a Protecção de Dados

([1]) No capítulo IV é defendida a ideia de que o princípio da opção de inclusão no ponto de venda é uma obrigação jurídica que já existe nos termos da Directiva «Protecção de Dados».