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 — «Uma abordagem global da protecção de dados pessoais na União Europeia»

(2011/C 181/01)

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 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 [2], nomeadamente o seu artigo 41.º,

ADOPTOU O SEGUINTE PARECER

A. PARTE GERAL

1. Introdução

1.1. *Uma primeira avaliação geral*

1. Em 4 de Novembro de 2010, a Comissão adoptou uma Comunicação intitulada «Uma abordagem global da protecção de dados pessoais na União Europeia» (a seguir denominada a «Comunicação») [3], a qual foi enviada à EDPS para consulta. A EDPS congratula-se com o facto de ter sido consultada pela Comissão em conformidade com o artigo 41.º do Regulamento (CE) n.º 45/2001. Antes da adopção da Comunicação, já lhe tinha sido oferecida a possibilidade de formular observações informais, algumas das quais foram tidas em conta na versão final do documento.

2. A Comunicação destina-se a definir a abordagem seguida pela Comissão para rever o quadro normativo da UE em matéria de protecção de dados em todos os domínios de actividade da União, tendo particularmente em conta os desafios resultantes da globalização e das novas tecnologias [4].

3. A EDPS congratula-se com a Comunicação, em termos gerais, visto estar convicta da necessidade de rever o actual quadro normativo da UE em matéria de protecção de dados para garantir uma protecção eficaz numa sociedade da informação em contínuo desenvolvimento. No seu parecer de 25 de Julho de 2007 sobre a aplicação da Directiva relativa à protecção de dados [5] já tinha concluído que, a longo prazo, parece inevitável a introdução de alterações na Directiva 95/46/CE.

4. A Comunicação representa um importante passo em frente para essa alteração legislativa que, por sua vez, constituiria a evolução mais importante no domínio da protecção de dados da UE desde a adopção da Directiva 95/46/CE, geralmente considerada como a pedra angular da protecção de dados na União Europeia (e também no Espaço Económico Europeu).

5. A Comunicação oferece o enquadramento adequado para uma revisão bem orientada, nomeadamente porque identifica, de um modo geral, as questões e desafios principais. A EDPS concorda com a perspectiva da Comissão de que, no futuro, continuará a ser necessário um sistema de protecção de dados forte, com base na ideia de que os actuais princípios gerais de protecção de dados permanecem válidos numa sociedade sujeita a profundas mutações devido à rapidez dos avanços tecnológicos e da globalização. Para o efeito, há que rever os instrumentos legislativos vigentes.

---

[1] JO L 281, 23.11.1995, p. 31.
[2] JO L 8, 12.1.2001, p. 1.
[3] COM(2010) 609 final.

[4] Ver pág. 5 da Comunicação, n.º 1.
[5] Parecer da Autoridade Europeia para a Protecção de Dados, 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.

6. A Comunicação salienta, com razão, que os desafios são enormes. A EDPS está inteiramente de acordo com esta afirmação e sublinha que, em consequência, as soluções propostas devem ter um nível de ambição correspondente e aumentar a eficácia da protecção.

1.2. *Objectivo do parecer*

7. O presente parecer analisa as soluções propostas na Comunicação com base nos dois critérios seguintes: ambição e eficácia. A sua opinião é, de um modo geral, positiva. A EDPS apoia a Comunicação, mas simultaneamente critica alguns aspectos em que considera que a existência de maior ambição conduziria a um sistema mais eficaz.

8. A EDPS pretende contribuir com o presente parecer para o desenvolvimento do quadro normativo em matéria de protecção de dados. Aguarda com expectativa a proposta da Comissão, que deverá ser apresentada em meados de 2011, e espera que as suas sugestões sejam tidas em conta na formulação dessa proposta. Constata igualmente que a Comunicação parece excluir certos domínios, como o tratamento de dados pelas instituições e organismos da UE, do diploma geral. Caso a Comissão efectivamente decida deixar de fora alguns domínios, nesta fase — facto que a EDPS lamentaria —, solicita-lhe que se comprometa a levar a cabo uma arquitectura verdadeiramente global num prazo curto e especificado.

1.3. *Alicerces do presente parecer*

9. O presente parecer não surge isolado. Baseia-se em posições anteriormente tomadas pela EDPS e pelas autoridades europeias de protecção de dados em diversas ocasiões. Convém salientar, designadamente, que no já referido parecer da EDPS de 25 de Julho de 2007 se identificaram e descreveram alguns dos principais elementos a ter em conta nas futuras alterações. ([6]) Baseia-se igualmente em debates com os outros interessados nos domínios da privacidade e da protecção de dados, cujos contributos foram muito úteis tanto para a Comunicação como para o presente parecer. Pode concluir-se, a este respeito, que existe um certo nível de sinergia quanto à forma de melhorar a eficácia da protecção de dados.

10. Outro importante alicerce do presente parecer é o documento intitulado «The Future of Privacy», contributo conjunto do Grupo de Trabalho do Artigo 29.º para a Protecção de Dados e do Grupo de Trabalho «Polícia e Justiça» para a consulta que a Comissão lançou em 2009 (a seguir denominado «Documento dos grupos de trabalhos sobre o Futuro da Privacidade») ([7]).

11. Mais recentemente, numa conferência de imprensa realizada em 15 de Novembro de 2010, a EDPS comunicou as suas reacções preliminares sobre a Comunicação. O presente parecer aprofunda as opiniões mais genéricas então apresentadas. ([8])

12. Por último, o parecer beneficia do contributo de vários pareceres anteriores da EDPS, bem como de documentos do Grupo de Trabalho do Artigo 29.º para a Protecção de Dados. Ao longo do texto, são feitas referências aos ditos pareceres e documentos, quando necessário.

2. **Contexto**

13. A revisão das normas de protecção de dados surge num momento histórico crucial. A Comunicação descreve o seu contexto de forma aprofundada e convincente. Com base nessa descrição, a EDPS identifica os quatro principais factores que determinam o ambiente em que o processo de revisão se realiza.

14. O primeiro factor é o desenvolvimento tecnológico. A tecnologia actual não é a mesma que existia quando a Directiva 95/46/CE foi concebida e adoptada. Fenómenos tecnológicos como a computação em nuvem, a publicidade comportamental, as redes sociais, a cobrança de portagens nas auto-estradas e os dispositivos de localização geográfica vieram alterar profundamente a forma como os dados são tratados e colocam enormes desafios à protecção de dados. A revisão das normas europeias nesta matéria terá de responder eficazmente a esses desafios.

15. O segundo factor é a globalização. A progressiva eliminação dos obstáculos ao comércio conferiu às empresas uma crescente dimensão mundial. O tratamento de dados transfronteiras e as transferências internacionais de dados

([6]) Nomeadamente (ver ponto 77 do parecer): não há necessidade de alterar os princípios existentes, mas é claramente necessário estabelecer outras disposições administrativas; não deve ser alterado o vasto âmbito de aplicação da lei aplicável a todas as utilizações de dados pessoais; a legislação em matéria de protecção de dados deve permitir uma abordagem equilibrada em casos concretos, devendo igualmente permitir a definição de prioridades por parte das autoridades responsáveis na matéria; o sistema deverá aplicar-se plenamente à utilização de dados pessoais para efeitos de aplicação da lei, embora possam ser necessárias medidas suplementares adequadas para fazer face a problemas especiais neste domínio.

([7]) Documento WP 168 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf). A sua mensagem principal é de que uma alteração legislativa constitui uma boa oportunidade para clarificar algumas normas e princípios fundamentais (por exemplo, o consentimento e a transparência), introduzir princípios novos (por exemplo, a privacidade desde a concepção e a responsabilização), reforçar a eficácia mediante a modernização das disposições (por exemplo, limitando os actuais requisitos de notificação) e incluir todos os domínios num único quadro normativo global (incluindo a cooperação policial e judiciária).

([8]) Os pontos abordados na conferência de imprensa estão disponíveis no sítio *Web* da EDPS, no endereço: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-11-15_Press_conf_speaking_points_PHBG_EN.pdf

aumentaram extraordinariamente nos últimos anos. Além disso, o tratamento de dados tornou-se omnipresente devido às tecnologias da informação e das comunicações: a Internet e a computação em nuvem permitiram o tratamento deslocalizado de grandes quantidades de dados à escala mundial. Na última década, verificou-se também um aumento das actividades policiais e judiciárias de combate ao terrorismo e a outras formas de criminalidade organizada a nível internacional, secundadas por um enorme intercâmbio de informações para efeitos de aplicação da lei. Tudo isto exige que se reflicta seriamente sobre a maneira de garantir eficazmente a protecção de dados pessoais num mundo globalizado, sem dificultar muito as actividades de tratamento internacionais.

16. O terceiro factor é o Tratado de Lisboa. A entrada em vigor do Tratado de Lisboa assinala uma nova era para a protecção de dados. O artigo 16.º do TFUE não só prevê um direito individual da pessoa em causa, como constitui também uma base jurídica directa para uma forte legislação de protecção de dados a nível da UE. Além disso, a supressão da estrutura em pilares obriga o Parlamento Europeu e o Conselho a integrarem a protecção de dados em todos os domínios do direito da UE. Por outras palavras, ela permite um quadro normativo global em matéria de protecção de dados, aplicável ao sector privado, ao sector público dos Estados-Membros e às instituições e organismos da UE. O Programa de Estocolmo ([9]) afirma consistentemente, a este respeito, que a União deve assegurar uma estratégia global de protecção dos dados no seu âmbito e no âmbito das suas relações com países terceiros.

17. O quarto factor é constituído pela evolução concomitante que está a ocorrer no contexto das organizações internacionais. Há vários debates em curso sobre a modernização dos actuais diplomas de protecção de dados. É importante referir, a este respeito, as actuais reflexões sobre a futura revisão da Convenção 108 do Conselho da Europa ([10]) e das directrizes da OCDE em matéria de protecção da vida privada ([11]). Outra evolução importante diz respeito à adopção de normas internacionais em matéria de protecção de dados pessoais e da vida privada, que poderá conduzir a um diploma global vinculativo nessa matéria. Todas estas iniciativas merecem ser plenamente apoiadas. Elas deverão ter como objectivo comum assegurar uma protecção eficaz e coerente, num ambiente baseado na tecnologia e globalizado.

3. **Perspectivas principais**

3.1. *A protecção de dados promove a confiança e deve apoiar outros interesses (públicos)*

18. A importância conferida à protecção de dados no Tratado de Lisboa, nomeadamente no artigo 8.º da Carta dos Direitos Fundamentais da União e no artigo 16.º TFUE, bem como a sua relação indissociável com o artigo 7.º da Carta, conduz necessariamente a um sólido quadro de protecção de dados ([12]).

19. Um tal quadro também serve, todavia, os interesses públicos e privados em geral, numa sociedade da informação em que o tratamento dos dados é omnipresente. A protecção de dados promove a confiança, que é uma componente essencial do bom funcionamento da nossa sociedade. É essencial que as disposições relativas à protecção de dadas sejam interpretadas de modo a — na medida do possível — apoiarem activamente outros direitos e interesses legítimos, em lugar de os dificultarem.

20. São exemplos importantes de outros interesses legítimos uma economia europeia forte, a segurança dos cidadãos e a responsabilização dos governos.

21. O desenvolvimento económico da UE está associado à introdução e à comercialização de novas tecnologias e serviços. Na sociedade da informação, a emergência e a implantação bem-sucedida das tecnologias da informação e das comunicações, bem como dos serviços nesse domínio, dependem da confiança. Se as pessoas não confiarem nas TIC, é provável que estas falhem ([13]). E as pessoas só confiam nas TIC se os seus dados forem eficazmente protegidos. Por conseguinte, a protecção de dados deve ser uma parte integrante das tecnologias e serviços. Um quadro forte em matéria de protecção de dados favorece a economia europeia, desde que esse quadro seja não só forte, mas também adequadamente adaptado. A maior harmonização no interior da UE e a minimização dos encargos administrativos são essenciais, deste ponto de vista (ver Capítulo 5 do parecer).

22. Muito tem sido dito, nos últimos anos, sobre a necessidade de conciliar a privacidade com a segurança, sobretudo em relação aos instrumentos de tratamento e intercâmbio de dados no domínio da cooperação policial e judiciária ([14]). A protecção de dados foi, muitas vezes, erradamente caracterizada como um obstáculo à total protecção da segurança física das pessoas ([15]) ou, pelo menos, como uma condição que as autoridades responsáveis pela aplicação da lei deviam respeitar inevitavelmente. Contudo, esta é uma visão parcelar da realidade. Um quadro forte em matéria de protecção de dados pode melhorar e reforçar a segurança. Com base nos princípios de protecção de dados — quando bem aplicados — os responsáveis pelo tratamento são obrigados a velar por que as informações sejam exactas e actualizadas e os dados pessoais supérfluos, não necessários para efeitos de aplicação da lei, sejam eliminados dos sistemas. De referir também são as obrigações de aplicar medidas tecnológicas e organizativas

([9]) Programa de Estocolmo — Uma Europa aberta e segura que sirva e proteja os cidadãos, JO C 115 de 4.5.2010, p. 1, na p. 10.

([10]) Convenção 108 do Conselho da Europa para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal, ETS n.º 108, 28 Janeiro 1981.

([11]) Directrizes sobre a protecção da privacidade e os fluxos transfronteiras de dados pessoais, publicadas em http://www.oecd.org

([12]) Essa importância da protecção de dados e a sua ligação à vida privada na Carta dos Direitos Fundamentais foram salientadas pelo Tribunal de Justiça no seu Acórdão de 9 de Novembro de 2010, Processos apensos C-92/09 e C-93/09, *Schecke*, ainda não publicados na Colectânea de Jurisprudência.

([13]) Ver Parecer da Autoridade Europeia para a Protecção de Dados, de 18 de Março de 2010, sobre a promoção da confiança na sociedade da informação através do reforço da protecção dos dados e da privacidade, JO C 280 de 16.10.2010, p. 1, ponto 113.

([14]) Ver, por exemplo, o Parecer da EDPS, 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 17.9.2009, p. 8.

([15]) O conceito de segurança ultrapassa a mera segurança física, mas para ilustrar os argumentos em apreço é aqui utilizado na sua acepção mais limitada.

para garantir a segurança dos sistemas, protegendo-os contra a divulgação ou o acesso não autorizados, desenvolvidas no domínio da protecção de dados.

23. O respeito dos princípios de protecção de dados pode funcionar, além do mais, como uma garantia de que as autoridades responsáveis pela aplicação da lei agem em conformidade com o Estado de direito, o que suscita confiança no seu comportamento e promove a confiança, em sentido mais lato, nas nossas sociedades. A jurisprudência desenvolvida ao abrigo do artigo 8.º da Convenção Europeia dos Direitos do Homem vem assegurar que as autoridades policiais e judiciárias possam tratar todos os dados de que necessitam para o seu trabalho, mas que o façam dentro de certos limites. A protecção de dados implica a realização de controlos (ver o Capítulo 9 do parecer sobre a polícia e a justiça).

24. Nas sociedades democráticas, os governos são responsáveis por todas as suas actividades, nomeadamente pela utilização que fazem dos dados pessoais tendo em vista os diversos interesses públicos que servem. Essa utilização pode ir desde a publicação de dados na Internet por motivos de transparência até ao seu uso em apoio de políticas em domínios como a saúde pública, os transportes ou a fiscalidade, ou à vigilância de pessoas para efeitos de aplicação da lei. Um quadro forte em matéria de protecção de dados permite que os governos respeitem as suas responsabilidades e prestem contas, no quadro de uma boa governação.

3.2. *Consequências para o quadro normativo em matéria de protecção de dados*

3.2.1. É necessária uma maior harmonização

25. A Comunicação identificou, justificadamente, que uma das principais lacunas do quadro actual reside no facto de permitir aos Estados-Membros uma margem discricionária excessiva na transposição das disposições europeias para a legislação nacional. A falta de harmonização tem várias consequências negativas numa sociedade da informação em que as fronteiras físicas entre os Estados-Membros são cada vez menos relevantes (ver Capítulo 5 do parecer).

3.2.2. Os princípios gerais de protecção de dados permanecem válidos

26. Uma primeira razão, mais formal, para os princípios gerais de protecção de dados não deverem nem poderem ser alterados é de natureza jurídica. Estes princípios estão consagrados na Convenção 108 do Conselho da Europa, que é vinculativa para todos os Estados-Membros. Esta convenção é a base da protecção de dados na UE. Além disso, alguns dos princípios mais importantes são explicitamente mencionados no artigo 8.º da Carta dos Direitos Fundamentais da União Europeia. A alteração desses princípios exigiria, assim, uma alteração dos Tratados.

27. Porém, este não é o único aspecto. Também há razões substanciais para não se alterarem os princípios gerais. A EDPS está firmemente convencida de que a sociedade da informação não pode nem deve funcionar sem uma protecção adequada da vida privada e dos dados pessoais dos indivíduos. Quanto maiores são as quantidades de informação tratadas, maior é a protecção necessária. Uma sociedade da informação onde se tratam grandes volumes de informação sobre toda a gente deve estar assente no conceito de controlo pelo indivíduo, para que este possa agir e exercer as liberdades a que tem direito numa sociedade democrática, como as liberdades de expressão e de pensamento.

28. Além disso, é difícil imaginar que haja controlo pelo indivíduo se não forem impostas obrigações aos responsáveis pelo tratamento para que limitem o tratamento em conformidade com os princípios da necessidade, da proporcionalidade e da limitação da finalidade. Esse controlo também é difícil de imaginar se não forem reconhecidos os direitos das pessoas em causa, como os direitos de acesso, rectificação, supressão ou bloqueamento de dados.

3.2.3. Perspectiva dos direitos fundamentais

29. A EDPS salienta que a protecção de dados é reconhecida como um direito fundamental. Isto não significa que a protecção de dados deva *prevalecer* sempre sobre outros direitos e interesses importantes numa sociedade democrática, mas tem consequências para a natureza e o âmbito da protecção que deve ser proporcionada por um quadro jurídico da UE, de modo a assegurar que os requisitos de protecção de dados são sempre *adequadamente* tidos em conta.

30. Estas consequências principais podem ser definidas da seguinte forma:

— a protecção deve ser eficaz. Um quadro jurídico deve prever instrumentos que possibilitem que as pessoas exerçam os seus direitos na prática,

— o quadro deve manter-se estável durante um longo período,

— a protecção deve ser assegurada em todas as circunstâncias e não depender das preferências políticas em determinado período,

— podem ser necessárias limitações ao exercício do direito, mas elas devem ser excepcionais, devidamente justificadas e nunca podem afectar os elementos essenciais do próprio direito ([16]).

A EDPS recomenda que a Comissão tenha estas consequências em conta quando propuser soluções legislativas.

3.2.4. São necessários novos instrumentos legislativos

31. A Comunicação concentra-se, a justo título, na necessidade de reforçar os instrumentos legislativos em matéria de protecção de dados. Neste contexto, faz sentido recordar que, no documento do Grupo de Trabalho sobre o Futuro da Privacidade ([17]), as APD realçaram a necessidade

([16]) Ver também o Parecer da EDPS, 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, ponto 17, que se baseia na jurisprudência do Tribunal Europeu dos Direitos do Homem e do Tribunal de Justiça Europeu.

([17]) Ver nota de pé-de-paginá 7.

de reforçar os papéis dos diversos intervenientes no domínio da protecção de dados, nomeadamente as pessoas em causa, os responsáveis pelo tratamento e as próprias autoridades de supervisão.

32. Parece haver um amplo consenso entre as partes interessados quanto à importância fundamental de existirem instrumentos legislativos mais fortes — que tenham em conta os avanços tecnológicos e a globalização — para uma protecção de dados ambiciosa e eficaz no futuro. Como já foi mencionado no ponto 7, estes são os critérios utilizados pela EDPS na avaliação de quaisquer soluções que sejam propostas.

3.2.5. O carácter global como condição sine qua non

33. Tal como se recorda na Comunicação, a Directiva 95/46/CE é aplicável a todas as actividades de tratamento de dados pessoais levadas a cabo nos Estados-Membros, tanto no sector público como no sector privado, à excepção das actividades não sujeitas à aplicação do antigo direito comunitário ([18]). Embora esta excepção fosse necessária ao abrigo do Tratado anterior, deixou de o ser após a entrada em vigor do Tratado de Lisboa. Além disso, a excepção é contrária ao artigo 16.º do TFUE — tanto ao seu teor como, em todo o caso, ao seu espírito.

34. No entender da EDPS, deve considerar-se que um diploma global de protecção de dados que inclua a cooperação policial e judiciária em matéria penal é uma das principais melhorias que um novo quadro jurídico pode trazer. Trata-se de uma condição *sine qua non* para uma protecção dos dados eficaz no futuro.

35. A EDPS salienta os seguintes argumentos em apoio desta afirmação:

— a distinção entre as actividades do sector privado e as do sector de aplicação da lei está cada vez mais indefinida. As entidades do sector privado podem tratar dados que acabem por ser utilizados para efeitos de aplicação da lei [como é o caso dos PNR ([19])], enquanto noutros casos são obrigadas a conservar dados para tais efeitos [por exemplo, a Directiva Conservação de Dados ([20])],

— não há diferenças fundamentais entre as autoridades policiais e judiciárias e outras autoridades responsáveis pela aplicação da lei (fiscais, aduaneiras, anti-fraude, imigração) sujeitas à Directiva 95/46/CE,

— tal como se encontra descrito de forma precisa na Comunicação, o diploma legal de protecção de dados actualmente aplicável às autoridades policiais e judiciárias [Decisão-Quadro 2008/977/JAI ([21])] é inadequado,

— a maioria dos Estados-Membros transpôs a Directiva 95/46 e a Convenção 108 para as suas legislações nacionais, tornando-as também aplicáveis às suas autoridades policiais e judiciais.

36. A inclusão da polícia e da justiça no diploma geral não só ofereceria mais garantias aos cidadãos como facilitaria o trabalho das autoridades policiais. Ter de aplicar vários conjuntos de regras é pesado, desnecessariamente moroso e dificulta a cooperação internacional (ver mais adiante o Capítulo 9 do parecer). Este também é um bom motivo para se incluírem as actividades de tratamento de dados levadas a cabo pelos serviços de segurança nacional, na medida do possível atendendo ao estado actual do direito da União.

3.2.6. Neutralidade tecnológica

37. O período decorrido desde a adopção da Directiva 95/46/CE, em 1995, pode classificar-se como turbulento do ponto de vista tecnológico. São frequentemente introduzidos novos avanços e engenhos tecnológicos, que em muitos casos conduzem a alterações de fundo na forma como os dados pessoais dos indivíduos são tratados. A sociedade da informação já não pode ser considerada como um ambiente paralelo em que as pessoas participam voluntariamente, tendo passado a fazer parte da nossa vida quotidiana. Apenas a título de exemplo, o conceito de Internet das coisas ([22]) estabelece ligações entre os objectos físicos e a informação em linha com eles relacionada.

38. A tecnologia continuará a evoluir, com as respectivas consequências para o novo quadro normativo. Este deve ser eficaz durante um maior número de anos, não entravando, simultaneamente, a ocorrência de novos avanços tecnológicos. Para o efeito, é necessário que as disposições jurídicas sejam tecnologicamente neutras. Contudo, o quadro também deve proporcionar mais segurança jurídica para as empresas e os particulares. Estes devem compreender o que se espera deles e poder exercer os seus direitos. Para esse efeito, é necessário que as disposições jurídicas sejam precisas.

39. No entender da EDPS, um diploma geral para a protecção de dados deve ser formulado, tanto quanto possível, de forma tecnologicamente neutra. Isto implica que os direitos e obrigações dos diversos intervenientes sejam formulados de forma geral e neutra, de modo a permanecerem, em princípio, válidos e aplicáveis independentemente da tecnologia escolhida para tratar os dados pessoais. Não há outra opção, dada a rapidez com que a tecnologia progride actualmente. A EDPS sugere que se introduzam novos direitos «tecnologicamente neutros» para além dos

([18]) O presente parecer concentrar-se-á principalmente no antigo terceiro pilar (cooperação policial e judiciária em matéria penal), uma vez que o antigo segundo pilar é um domínio do direito da UE não só mais complicado (tal como reconhecem o artigo 16.º TFUE e o artigo 39.º TUE), mas também menos pertinente para o tratamento de dados.

([19]) Ver, por exemplo, a Comunicação da Comissão sobre a abordagem global relativa à transferência dos dados do registo de identificação dos passageiros (PNR) para países terceiros, COM(2010) 492 final.

([20]) Directiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de Março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva 2002/58/CE (JO L 105 de 13.4.2006, p. 54).

([21]) Decisão-Quadro 2008/977/JAI do Conselho, de 27 de Novembro de 2008, relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal JO L 350 de 30.12.2008, p. 60.

([22]) Definido em «A Internet das coisas: um plano de acção para a Europa», COM(2009) 278 Final.

actuais princípios de protecção de dados que possam ter uma importância específica no ambiente electrónico em rápida evolução (ver sobretudo Capítulos 6 e 7).

3.2.7. Longo prazo: Segurança jurídica por um período mais longo

40. A Directiva 95/46/CE tem sido o elemento central da protecção de dados na União Europeia, nos últimos quinze anos. Foi transposta para as legislações dos Estados-Membros e aplicada pelos diversos intervenientes. Ao longo dos anos, a aplicação beneficiou da experiência prática e de orientações complementares fornecidas pela Comissão, as autoridades responsáveis pela protecção de dados (a nível nacional e no âmbito do Grupo de Trabalho do Artigo 29.º) e os tribunais nacionais e europeus.

41. Importa salientar que estes desenvolvimentos necessitam de tempo e que — sobretudo tratando-se de um quadro geral que põe em prática um direito fundamental — esse tempo é necessário para gerar segurança jurídica e estabilidade. É necessário elaborar um novo diploma geral com a ambição de que possa criar segurança jurídica e estabilidade por um período mais longo, não esquecendo que é muito difícil prever como a tecnologia e a globalização irão evoluir futuramente. Em todo o caso, a EDPS apoia inteiramente o objectivo de criar segurança jurídica por um período mais longo, comparável à perspectiva da Directiva 95/46/CE. Em suma, quando a tecnologia evolui rapidamente, a lei deve ser estável.

3.2.8. Curto prazo: Utilizar melhor os instrumentos existentes

42. A curto prazo, é essencial assegurar a eficácia dos instrumentos legislativos existentes, a começar pela concentração na sua aplicação a nível nacional e a nível da UE (ver Capítulo 11 do presente parecer).

B. ELEMENTOS DE UM NOVO QUADRO

4. Abordagem global

43. A EDPS apoia inteiramente a abordagem global da protecção de dados, que é não só o título mas também o ponto de partida da Comunicação e que inclui necessariamente a extensão da aplicação das normas gerais de protecção de dados ao domínio da cooperação policial e judiciária em matéria penal ([23]).

44. No entanto, constata também que a Comissão não tenciona incluir todas as actividades de tratamento de dados neste diploma geral. Nomeadamente, o tratamento de dados pelas instituições, organismos, serviços e agências da UE não estará incluído. A Comissão afirma apenas que «irá avaliar a necessidade de adaptar outros diplomas legais ao novo quadro normativo geral de protecção de dados».

45. A EDPS manifesta a sua clara preferência pela inclusão do tratamento a nível da UE no quadro normativo geral. Recorda que era essa a intenção original do antigo artigo 286.º TCE, que mencionou pela primeira vez a protecção de dados a nível do Tratado. O artigo 286.º TCE limitava-se a afirmar que os diplomas relativos à protecção de dados de carácter pessoal também seriam aplicáveis às instituições. Mais importante ainda, um único texto jurídico evita o risco de discrepâncias entre disposições e seria o mais adequado para o intercâmbio de dados entre o nível da UE e as entidades públicas e privadas dos Estados-Membros. Também evitaria o risco de, após a alteração da Directiva 95/46/CE, já não existir interesse político em alterar o Regulamento (CE) n.º 45/2001 ou de não se atribuir a essa alteração a prioridade suficiente para evitar discrepâncias quanto às datas de entrada em vigor.

46. A EDPS insta a Comissão — caso esta conclua que a inclusão do tratamento a nível da UE no diploma geral não seria exequível — a assumir o compromisso de propor uma adaptação do Regulamento (CE) n.º 45/2001 (e não de «avaliar a necessidade» de o fazer) o mais rapidamente possível e, de preferência, até ao final de 2011.

47. É igualmente importante que a Comissão não deixe para trás outros domínios, nomeadamente:

— a protecção de dados no domínio da Política Externa e de Segurança Comum, com base no artigo 39.º TUE ([24]),

— regimes sectoriais de protecção de dados para organismos da UE como a Europol e a Eurojust, e para os sistemas de informação de grande dimensão, na medida em que necessitem de ser adaptados ao novo diploma,

— a Directiva 2002/58/CE, Directiva Privacidade e Comunicações Electrónicas, na medida em que necessite de ser adaptada ao novo diploma.

48. Por último, um diploma geral de protecção de dados pode, e provavelmente deve, ser complementado por regulamentos suplementares sectoriais e específicos, por exemplo para a cooperação policial e judiciária, mas também noutros domínios ([25]). Quando necessário e em conformidade com o princípio de subsidiariedade, esses regulamentos suplementares devem ser adoptados a nível da UE. Os Estados-Membros podem elaborar normas suplementares, em domínios específicos em que tal se justifique (ver 5.2).

([23]) Ver pág. 14 da Comunicação e secção 3.2.5 do presente parecer.

([24]) Ver também Parecer da EDPS, de 24 de Novembro de 2010, sobre a Comunicação da Comissão ao Parlamento Europeu e ao Conselho — «A política de luta contra o terrorismo da UE: principais realizações e desafios futuros», ponto 31,

([25]) Ver também documento do Grupo de Trabalho sobre o Futuro da Privacidade (nota de rodapé 7), n.os 18-21.

5. **Maior harmonização e simplificação**

5.1. *A necessidade de harmonização*

49. A harmonização tem uma importância essencial para a legislação da UE em matéria de protecção de dados. A Comunicação salientou correctamente que a protecção de dados tem uma forte vertente relativa ao mercado interno, visto ter de assegurar o livre fluxo de dados pessoais entre Estados-Membros no mercado interno. Contudo, o nível de harmonização previsto pela presente directiva foi considerado pouco satisfatório. A Comunicação reconhece que esta é uma das preocupações mais frequentes dos interessados. Estes destacam, nomeadamente, a necessidade de aumentar a segurança jurídica, reduzir a sobrecarga administrativa e garantir a igualdade de condições para os operadores económicos. Como a Comissão faz notar, justificadamente, que os responsáveis pelo tratamento de dados estabelecidos em vários Estados-Membros e que devem cumprir as condições (eventualmente divergentes) das legislações nacionais de protecção de dados são especialmente afectados por esta situação ([26]).

50. A harmonização é importante não só para o mercado interno mas também para assegurar uma protecção adequada dos dados. O artigo 16.º TFUE prevê que «todas as pessoas» têm direito à protecção dos dados de carácter pessoal que lhes digam respeito. Para que este direito seja efectivamente respeitado, deve garantir-se um nível de protecção equivalente em toda a União. O documento do Grupo de Trabalho sobre o Futuro da Privacidade salientava que várias disposições relativas às posições das pessoas em causa não foram uniformemente transpostas ou interpretadas em todos os Estados-Membros ([27]). Num mundo globalizado e interligado, estas divergências podem prejudicar ou limitar a protecção das pessoas.

51. A EDPS considera que a maior e melhor harmonização é um dos principais objectivos do processo de revisão. Congratula-se com o compromisso da Comissão de analisar os meios de conseguir maior harmonização da protecção de dados a nível da UE. Constata, todavia, com alguma surpresa, que a Comunicação não propõe, nesta fase, opções concretas. Indica, por isso, alguns domínios em que é mais urgente conseguir uma maior convergência (ver 5.3). A maior harmonização nesses domínios deveria ser obtida não só através da redução da margem de manobra da legislação nacional, mas também através da prevenção de uma transposição incorrecta pelos Estados-Membros (ver também Capítulo 11) e da garantia de uma aplicação mais coerente e coordenada (ver também Capítulo 10).

5.2. *Redução da margem de manobra na aplicação da Directiva*

52. A directiva contém várias disposições formuladas de forma genérica e que, por isso, deixam bastante margem para uma aplicação divergente. O seu considerando 9 confirma explicitamente que é concedida aos Estados-Membros alguma margem de manobra e que, dentro dessa margem, poderão verificar-se disparidades na aplicação da directiva. Várias disposições têm sido aplicadas de forma diferente pelos Estados-Membros, incluindo algumas disposições cruciais ([28]). Esta situação não é satisfatória e deverá procurar-se uma maior convergência.

53. Isto não significa que a diversidade deva ser totalmente excluída. Em determinados domínios, poderá ser necessária flexibilidade para preservar especificidades justificadas, interesses públicos importantes ou a autonomia institucional dos Estados-Membros. No entender da EDPS, a margem para divergências entre os Estados-Membros deve ser limitada, designadamente, às seguintes situações específicas:

— liberdade de expressão: no quadro actual (artigo 9.º), os Estados-Membros podem estabelecer isenções e derrogações em relação ao tratamento de dados efectuado para fins jornalísticos ou de expressão artística ou literária. Esta flexibilidade afigura-se justificada, sob reserva, evidentemente, dos limites previstos na Carta e na CEDH, tendo em conta as diversas tradições e as diferenças culturais que neste domínio possam existir entre os Estados-Membros. Contudo, isto não deve obstar a uma possível actualização do artigo 9.º atendendo à evolução no domínio da Internet,

— interesses públicos específicos: no quadro actual (artigo 13.º), os Estados-Membros podem adoptar medidas legislativas destinadas a restringir o alcance das obrigações e direitos, sempre que tal restrição constitua uma medida necessária à protecção de um interesse público importante, como a segurança do Estado, a defesa, a segurança pública, etc. Esta competência dos Estados-Membros continua a justificar-se. Contudo, sempre que possível, a interpretação das excepções deve ser objecto de maior harmonização (ver secção 9.1). Além disso, o actual âmbito da excepção ao artigo 6.º, n.º 1, afigura-se excessivamente amplo,

— vias de recurso, sanções e procedimentos administrativos: um quadro europeu deve determinar as condições principais, mas no estado actual do direito da União, a determinação das sanções, das vias de recurso, das normas processuais e das modalidades de inspecções aplicáveis a nível nacional devem ser deixadas aos Estados-Membros.

([26]) Comunicação, pág. 10.

([27]) Ver documento do Grupo de Trabalho sobre o Futuro de Privacidade (nota de rodapé 7), ponto 70. O documento refere, em particular, as disposições relativas à responsabilidade e à possibilidade de pedir indemnizações por danos morais.

([28]) Também existem abordagens divergentes no que se refere aos dados tratados manualmente.

5.3. *Domínios que necessitam de maior harmonização*

54. *Definições* (artigo 2.º da Directiva 95/46/CE). As definições são a pedra angular do quadro normativo e devem ser interpretadas de modo uniforme em todos os Estados-Membros, sem margem de aplicação. Têm surgido divergências no âmbito do quadro actual, por exemplo, quanto ao conceito de responsável pelo tratamento dos dados ([29]). A EDPS sugere que se acrescentem outros elementos aos actualmente enunciados no artigo 2.º, a fim de proporcionar uma maior segurança jurídica, como os dados anónimos ou pseudónimos, os dados judiciais, a transferência de dados e o responsável pela protecção de dados.

55. *Licitude do tratamento (artigo 5.º).* O novo instrumento jurídico deve ser tão preciso quanto possível no que diz respeito aos elementos fundamentais que determinam a licitude do tratamento de dados. O artigo 5.º da Directiva (bem como o considerando 9), que mandata os Estados-Membros para especificarem as condições em que é lícito o tratamento de dados, pode deixar de ser, por isso, necessário num futuro quadro.

56. *Motivos para o tratamento de dados* (artigos 7.º e 8.º). A definição das condições para o tratamento de dados é um elemento essencial de qualquer legislação nesta matéria. Os Estados-Membros não devem ser autorizados a introduzir motivos adicionais ou alterados para o tratamento, nem excluir quaisquer motivos. A possibilidade de estabelecer derrogações deve ser excluída ou limitada (sobretudo no que diz respeito aos dados sensíveis ([30])). Num novo diploma, os motivos do tratamento de dados devem ser claramente formulados, reduzindo assim a margem de apreciação na transposição e aplicação. Em especial, o conceito de consentimento poderá necessitar de ser especificado com mais pormenor (ver secção 6.5). Além disso, o motivo baseado no legítimo interesse do responsável pelo tratamento (artigo 7.º, alínea f)) abre caminho a interpretações muito divergentes, devido à sua natureza flexível. É necessário especificá-lo em pormenor. Outra disposição que talvez deva ser especificada é o artigo 8.º, nº 2, alínea b), que permite o tratamento de dados sensíveis que seja necessário para o cumprimento das obrigações e dos direitos do responsável pelo tratamento no domínio da legislação do trabalho ([31]).

57. *Direitos das pessoas em causa* (artigos 10.º-15.º). Este é um dos domínios em que nem todos os elementos da directiva foram coerentemente transpostos e interpretados pelos Estados-Membros. Os direitos das pessoas em causa são fulcrais para uma protecção de dados eficaz. Em consequência, a margem de manobra deve ser substancialmente reduzida. A EDPS recomenda que as informações fornecidas às pessoas em causa pelo responsável pelo tratamento sejam uniformizadas a nível da UE.

58. *Transferências internacionais* (artigos 25.º-26.º). Este é um domínio que suscitou muitas críticas devido à ausência de uma prática uniforme em toda a UE. Os interessados criticaram o facto de as decisões da Comissão sobre a adequação serem interpretadas e aplicadas de formas divergentes pelos Estados-Membros. As normas vinculativas para as empresas são outro elemento em que a EDPS recomenda maior harmonização (ver Capítulo 9).

59. *Autoridades nacionais de protecção de dados* (artigo 28.º). As APD nacionais estão sujeitas a normas muito divergentes nos 27 Estados-Membros, no que respeita ao seu estatuto, recursos e poderes. O artigo 28.º contribuiu parcialmente para esta divergência devido à sua falta de precisão ([32]) e deve ser especificado, em conformidade com o Acórdão do Tribunal de Justiça Europeu no Processo C-518/07 ([33]) (ver ainda Capítulo 10).

5.4. *Simplificação do sistema de notificação*

60. Os requisitos de notificação (artigos 18.º-21.º da Directiva 95/46/CE) são outro domínio em que, até agora, tem sido concedida grande liberdade aos Estados-Membros. A Comunicação reconhece, com razão, que um sistema harmonizado permitiria reduzir os custos e a sobrecarga administrativa dos responsáveis pelo tratamento ([34]).

61. Este é um domínio em que a simplificação deveria ser o objectivo principal. A revisão do quadro de protecção de dados constitui uma oportunidade única para simplificar e/ou reduzir o âmbito dos actuais requisitos de notificação. A Comunicação reconhece que é consensual entre os interessados que o actual sistema de notificações é bastante pesado e não traz, por si só, qualquer valor acrescentado à protecção dos dados pessoais ([35]). A EDPS congratula-se, por conseguinte, com o compromisso da Comissão de explorar as diversas possibilidades de simplificação do actual sistema de notificação.

62. No seu entender, o ponto de partida dessa simplificação seria a substituição de um sistema em que a notificação é a regra, salvo disposição em contrário (isto é, um «sistema de isenção»), por um sistema mais direccionado. O sistema de isenção revelou-se ineficaz, por ser aplicado de forma incoerente entre os Estados-Membros ([36]). A EDPS sugere que se considerem as seguintes alternativas:

([29]) Ver Parecer 1 de 2010 do Grupo de Trabalho do Artigo 29.º sobre os conceitos de «responsável pelo tratamento» e «subcontratante» (WP 169).

([30]) O artigo 8.º, n.ºs 4 e 5, autoriza actualmente, em determinadas condições, que os Estados-Membros prevejam outras derrogações em relação aos dados sensíveis.

([31]) Ver, a este respeito, o Primeiro Relatório da Comissão sobre a implementação da Directiva relativa à protecção de dados, atrás citado, pág. 14.

([32]) Documento do Grupo de Trabalho sobre o Futuro da Privacidade, n.º 87.

([33]) Processo C-518/07, *Comissão das Comunidades Europeias* contra *República Federal da Alemanha*, ainda não publicado na Colectânea de Jurisprudência.

([34]) Ver nota de pé-de-página 26.

([35]) Ver nota de pé-de-página 26.

([36]) Relatório do Grupo de Trabalho do Artigo 29.º sobre a obrigação de notificar as autoridades nacionais de supervisão, a melhor utilização das excepções e simplificações e o papel dos responsáveis pela protecção de dados na União Europeia, WP 106, 2005, p. 7.

— limitar a obrigação de notificação a determinados tipos de operações de tratamento que impliquem riscos específicos (estas notificações poderiam desencadear outras medidas, como o controlo prévio do tratamento),

— uma obrigação de registo simples exigindo que os responsáveis pelo tratamento se registem (em lugar de se registarem todas as operações de tratamento).

Além disso, poderia ser introduzido um formulário normalizado pan-europeu para assegurar uma abordagem harmonizada das informações solicitadas.

63. A revisão do actual sistema de notificação em nada deverá prejudicar a melhoria das obrigações de controlo prévio relativas a determinadas operações de tratamento susceptíveis de apresentar riscos específicos (como os sistemas de informação de grande dimensão). A EDPS seria favorável à inclusão no novo diploma de uma lista não exaustiva de casos em que esse controlo prévio é exigido. O Regulamento (CE) n.º 45/2001 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos da UE fornece um modelo útil para este efeito ([37]).

5.5. *Um regulamento e não uma directiva*

64. Por último, a EDPS considera que o processo de revisão também constitui uma oportunidade para reexaminar o tipo de diploma a utilizar para a protecção de dados. Um regulamento, um instrumento único directamente aplicável nos Estados-Membros, é o meio mais eficaz para proteger o direito fundamental à protecção de dados e para criar um verdadeiro mercado interno onde os dados pessoais possam circular livremente e o nível de protecção seja igual independentemente do país ou do sector onde os dados são tratados.

65. Um regulamento reduziria a margem para interpretações contraditórias e diferenças injustificadas na transposição e aplicação da lei. Reduziria igualmente a importância de determinar a lei aplicável às operações de tratamento no interior da UE, um dos aspectos mais controversos do sistema actual (ver Capítulo 9).

66. No domínio da protecção de dados, um regulamento é ainda mais justificado, porque

— o artigo 16.º TFUE fez ascender o direito à protecção dos dados pessoais ao nível dos tratados e prevê — ou mesmo impõe — um nível uniforme de protecção das pessoas em toda a UE,

— o tratamento de dados tem lugar num ambiente electrónico em que as fronteiras internas entre os Estados-Membros se tornaram menos relevantes.

67. A escolha de um regulamento como diploma geral permite, sempre que necessário, disposições directamente dirigidas aos Estados-Membros, sempre que seja requerida flexibilidade. Também não influencia a competência dos Estados-Membros de adoptarem normas suplementares de protecção de dados, quando necessário, em conformidade como direito da UE.

6. **Reforço dos direitos das pessoas**

6.1. *A necessidade de reforçar os direitos*

68. A EDPS apoia totalmente a Comunicação quando esta propõe que se reforcem os direitos das pessoas, uma vez que os diplomas existentes não proporcionam plenamente a protecção eficaz que é necessária num mundo digitalizado cada vez mais complexo.

69. Por um lado, o desenvolvimento de um mundo digitalizado implica um forte crescimento da recolha, utilização e transferência dos dados pessoais de uma forma extremamente complexa e não transparente. Muitas vezes, as pessoas, não têm conhecimento ou não compreendem como isso acontece, quem recolhe os seus dados, nem como se pode exercer algum controlo. Um exemplo ilustrativo deste fenómeno é o acompanhamento, por parte dos fornecedores de redes de publicidade, das actividades de navegação das pessoas, através de *cookies* ou de dispositivos semelhantes, para efeitos de publicidade direccionada. Quando os utilizadores visitam os sítios Internet, não esperam que terceiros, de que não se apercebem, registem essas visitas e criem registos dos utilizadores com base em informações que revelam o estilo de vida destes, ou aquilo de que gostam ou não gostam.

70. Por outro lado, esta evolução estimula a partilha proactiva de informações pessoais entre os indivíduos, por exemplo nas redes sociais. Cada vez mais, os jovens fazem parte de uma rede social e interagem com os seus pares. É duvidoso que os jovens e outras pessoas estejam cientes da amplitude da difusão dos seus dados e dos efeitos a longo prazo das suas acções.

6.2. *Aumentar a transparência*

71. A transparência tem enorme importância em qualquer regime de protecção de dados, não só devido ao seu valor intrínseco, mas também porque permite o exercício de outros princípios de protecção de dados. As pessoas só poderão exercer os seus direitos se tiverem conhecimento do tratamento de dados.

72. A Directiva 95/46/CE contém várias disposições relativas à transparência. Os artigos 10.º e 11.º prevêem a obrigação de fornecer informações às pessoas sobre a recolha dos seus dados pessoais. Além disso, o artigo 12.º reconhece às pessoas em causa o direito de obterem uma cópia dos seus dados pessoais sob forma inteligível (direito de acesso). O artigo 15.º reconhece o direito de conhecer a lógica subjacente às decisões automatizadas que produzem efeitos na sua esfera jurídica. Em último lugar, mas não menos importante, o artigo 6.º, n.º 1, alínea a), que exige que o tratamento seja leal, também implica um requisito de transparência. Os dados pessoais não podem ser tratados por razões ocultas ou secretas.

([37]) Ver artigo 27.º do Regulamento, JO L 8 de 12.1.2001, p. 1.

73. A Comunicação sugere que se acrescente um princípio geral de transparência. Em reacção a esta sugestão, a EDPS salienta que o conceito de transparência já faz parte do actual quadro normativo em matéria de protecção de dados, ainda que de forma implícita. Isto pode ser deduzido das diversas disposições respeitantes à transparência, mencionadas no número anterior. No entender da EDPS, a inclusão de um princípio de transparência *explícito*, ligado ou não à disposição existente de tratamento leal, poderia ter valor acrescentado. Ele aumentaria a segurança jurídica, além de confirmar que um responsável pelo tratamento deve tratar os dados pessoais de forma transparente em todas as circunstâncias e não apenas quando isso lhe é pedido, ou quando uma disposição jurídica específica lho exija.

74. Contudo, talvez seja mais importante reforçar as actuais disposições em matéria de transparência, como os actuais artigos 10.º e 11.º da Directiva 95/46/CE. Essas disposições especificam os elementos de informação que devem ser fornecidos, mas não indicam de forma precisa as modalidades desse fornecimento. Mais concretamente, a EDPS sugere que as disposições actuais sejam reforçadas por meio de:

— um requisito para que os responsáveis pelo tratamento forneçam informações sobre o tratamento de dados de maneira acessível e fácil de compreender, numa linguagem clara e simples ([38]). As informações devem ser claras, conspícuas e visíveis. A disposição também poderia incluir a obrigação de garantir uma compreensão fácil das informações, que ilegalizaria os regimes de privacidade opacos ou difíceis de entender,

— um requisito para que as informações sejam facultadas às pessoas em causa de forma fácil e directa. As informações também devem estar permanentemente acessíveis e não desaparecer ao fim de muito pouco tempo de um suporte electrónico. Isto ajudaria os utilizadores a armazenarem e reproduzirem as informações futuramente, permitindo um acesso ulterior.

6.3. *Apoio a uma obrigação de comunicar as violações da segurança*

75. A EDPS apoia a introdução no diploma geral de uma disposição sobre a notificação das violações dos dados pessoais que alargue a todos os responsáveis pelo tratamento a obrigação aplicável a alguns prestadores que foi incluída na Directiva Privacidade e Comunicações Electrónicas revista, tal como é proposto na Comunicação. Nos termos da Directiva Privacidade e Comunicações Electrónicas revista, a obrigação só é aplicável aos prestadores de serviços de comunicações electrónicas (serviços de telefonia (incluindo VoIP) e acesso à Internet). Os outros responsáveis pelo tratamento de dados não estão abrangidos por essa obrigação, mas os motivos que a justificam são inteiramente aplicáveis a outros responsáveis pelo tratamento para além dos prestadores de serviços de comunicações electrónicas.

76. A notificação das violações da segurança tem diversos fins e objectivos. O mais evidente, que a Comunicação destaca, é servir de instrumento de informação para sensibilizar as pessoas em relação aos riscos que enfrentam quando os seus dados pessoais são comprometidos. Isso poderá contribuir para que tomem as medidas necessárias para reduzirem esses riscos. Por exemplo, quando alertadas para violações que afectem as suas informações financeiras, as pessoas poderão, nomeadamente, alterar as palavras-passe ou cancelar as suas contas. Além disso, a notificação das violações da segurança contribui para a aplicação eficaz de outros princípios e obrigações contidos na directiva. Por exemplo, os requisitos de notificação das violações da segurança incentivam os responsáveis pelo tratamento a aplicar medidas de segurança mais fortes para prevenirem tais violações. A notificação das violações da segurança também é um instrumento para reforçar a responsabilidade dos responsáveis pelo tratamento e, muito em especial, para aumentar a sua responsabilização (ver Capítulo 7). Por último, é um instrumento que auxilia a aplicação da lei pelas APD. A notificação de uma violação a essas autoridades pode levar à investigação das práticas globais de um responsável pelo tratamento.

77. As normas específicas sobre a violação da segurança previstas na Directiva Privacidade e Comunicações Electrónicas alterada foram amplamente debatidas durante a fase parlamentar do quadro legislativo que antecedeu a adopção dessa directiva. Nesse debate, os pareceres do Grupo de Trabalho do Artigo 29.º e da EDPS foram tomados em consideração, juntamente com as opiniões de outras partes interessadas, pelo que as normas reflectem as ideias das diversas partes. Representam, assim, um equilíbrio de interesses: embora os critérios que desencadeiam a obrigação de notificar sejam, em princípio, adequados para proteger as pessoas, fazem-no sem impor requisitos excessivamente pesados e inúteis.

6.4. *Reforçar o consentimento*

78. O artigo 7.º da Directiva relativa à protecção de dados enumera seis bases jurídicas para o tratamento de dados pessoais. O consentimento da pessoa em causa é uma delas. Um responsável pelo tratamento pode tratar dados pessoais desde que as pessoas tenham dado o seu consentimento informado para que os seus dados sejam recolhidos e tratados.

79. Na prática, os utilizadores têm, muitas vezes, um controlo limitado em relação aos seus dados, sobretudo em ambientes tecnológicos. Um dos métodos por vezes utilizado é o consentimento tácito, ou seja um consentimento que tenha sido inferido. Pode ser inferido da acção da pessoa em causa (por exemplo, considera-se que a acção de utilizar um sítio Internet consente que os dados do utilizador

([38]) Ver Comunicação, pág. 6.

sejam registados para efeitos de *marketing*). Também pode ser inferido do silêncio ou da inacção (não eliminar o sinal de um campo assinalado é entendido como um consentimento).

80. Nos termos da directiva, o consentimento, para ser válido, deve ser informado, livre e específico. Deve ser uma manifestação de vontade informada pela qual as pessoas aceitam que dados pessoais que lhes dizem respeito sejam objecto de tratamento. A forma como o consentimento é dado deve ser inequívoca.

81. O consentimento inferido a partir de uma acção e, muito em especial, do silêncio ou da inacção não é, frequentemente, um consentimento inequívoco. Contudo, aquilo que constitui um consentimento verdadeiro e inequívoco nem sempre é claro. Alguns responsáveis pelo tratamento exploram esta incerteza recorrendo a métodos que não são adequados para se obter um consentimento verdadeiro e inequívoco.

82. Tendo em conta o que precede, a EDPS apoia a Comissão no que diz respeito à necessidade de clarificar os limites do consentimento e de velar por que só o consentimento manifestado de forma sólida seja assim considerado. Neste contexto, a EDPS sugere o seguinte ([39]):

— poderá ponderar-se a possibilidade de prever um maior número de situações em que o consentimento explícito seja exigido, e que actualmente estão limitadas aos dados sensíveis,

— que se adoptem normas suplementares relativas ao consentimento no ambiente em linha,

— que se adoptem normas suplementares relativas ao consentimento para que os dados sejam tratados para fins secundários (isto é, um tratamento secundário em relação ao tratamento principal ou um tratamento que não é óbvio),

— que se determine, num diploma legislativo suplementar, adoptado ou não pela Comissão ao abrigo do artigo 290.º TFUE, o tipo de consentimento necessário, por exemplo, para autorizar o tratamento de dados provenientes de etiquetas RFID apostas a produtos de consumo ou outras técnicas específicas.

6.5. *Portabilidade dos dados e direito a ser esquecido*

83. A portabilidade dos dados e o direito a ser esquecido são dois conceitos conexos que a Comunicação propõe para reforçar os direitos das pessoas em causa. São complementares aos princípios já mencionados na directiva, prevendo o direito de a pessoa em causa se opor ao tratamento dos seus dados pessoais e a obrigação do responsável pelo tratamento de apagar a informação assim que esta deixe de ser necessária para a finalidade do tratamento.

84. O valor acrescentado destes dois conceitos verifica-se sobretudo no contexto de uma sociedade da informação, em que cada vez mais dados são automaticamente armazenados e conservados por períodos indefinidos. A prática mostra que, mesmo que os dados sejam carregados pela pessoa em causa, o grau de controlo que esta efectivamente tem sobre os seus dados pessoais é, na realidade, muito limitado. Isto ainda é mais verdadeiro face à memória gigantesca que a Internet actualmente representa. Além disso, de um ponto de vista económico, fica mais caro a um responsável pelo tratamento apagar os dados do que conservá-los armazenados. O exercício dos direitos das pessoas em causa contraria, assim, a tendência económica natural.

85. Tanto a portabilidade dos dados como o direito a ser esquecido podem contribuir para alterar o equilíbrio a favor da pessoa em causa. O objectivo da portabilidade dos dados seria dar às pessoas um maior controlo sobre as informações que lhes dizem respeito, enquanto o direito a ser esquecido garantiria o desaparecimento automático das informações ao fim de um certo período, mesmo que a pessoa em causa nada faça para isso, nem esteja sequer ciente de que os dados chegaram a ser armazenados.

86. Mais especificamente, entende-se por portabilidade dos dados a capacidade dos utilizadores de alterarem as suas preferências quanto ao tratamento dos dados que lhes dizem respeito, em particular no âmbito dos novos serviços tecnológicos. Isto aplica-se, cada vez mais, aos serviços que implicam o armazenamento de informações, incluindo dados pessoais, como a telefonia móvel, e aos que armazenam imagens, mensagens de correio electrónico e outras informações, por vezes utilizando serviços de «computação em nuvem».

87. As pessoas devem poder mudar de prestador de serviços e transferir os seus dados pessoais para outro prestador com toda a liberdade e facilidade. A EDPS considera que os actuais direitos previstos na Directiva 95/46/CE poderiam ser reforçados pela inclusão de um direito de portabilidade, nomeadamente no contexto dos serviços da sociedade da informação, para que as pessoas possam estar seguras de que os prestadores de serviços e outros responsáveis pelo tratamento em causa lhes facultam o acesso às suas informações pessoais e, simultaneamente, os antigos prestadores ou outros responsáveis pelo tratamento apagam essas informações, mesmo que desejassem conservá-las para os seus próprios fins legítimos.

88. A codificação de um novo «direito a ser esquecido» permitiria garantir o apagamento dos dados pessoais ou a proibição de serem posteriormente utilizados, sem que

([39]) O Grupo de Trabalho do Artigo 29.º está a trabalhar num parecer sobre o «consentimento». Esse parecer poderá dar lugar a sugestões suplementares.

a pessoa em causa tivesse de actuar nesse sentido, mas na condição de esses dados já estarem armazenados há algum tempo. Por outras palavras, atribuir-se-ia aos dados uma espécie de prazo de validade. Este princípio já é afirmado em processos dos tribunais nacionais ou aplicado em sectores específicos, por exemplo, em relação aos ficheiros policiais, registos criminais ou processos disciplinares: algumas legislações nacionais prevêem que as informações sobre pessoas singulares sejam automaticamente apagadas, ou não possam ser posteriormente utilizadas e divulgadas, sobretudo após um prazo estabelecido, sem que seja necessário analisar previamente os casos concretos.

89. Neste sentido, deveria associar-se um novo «direito a ser esquecido» à portabilidade dos dados. O valor acrescentado desta medida residiria no facto de a pessoa em causa não necessitar de realizar qualquer esforço ou insistência para os seus dados serem apagados, uma vez que isso seria feito de forma objectiva e automática. Só em circunstâncias muito específicas, em que fosse possível determinar uma especial necessidade de conservar os dados por mais tempo, o responsável pelo tratamento teria direito a fazê-lo. Esse «direito a ser esquecido» inverteria, assim, o ónus da prova, transferindo-o da pessoa em causa para o responsável pelo tratamento, e criaria um ambiente de «privacidade por defeito» para o tratamento de dados pessoais.

90. A EDPS considera que o direito a ser esquecido se poderia revelar particularmente útil no contexto dos serviços da sociedade da informação. Uma obrigação de apagar ou de não continuar a divulgar as informações após um prazo estabelecido faz particular sentido nos meios de comunicação social ou na Internet e, nomeadamente, nas redes sociais. Também seria útil no que diz respeito aos equipamentos terminais: os dados armazenados em dispositivos móveis e computadores seriam automaticamente apagados ou bloqueados no fim de um determinado período, quando já não estivessem na posse das pessoas. Nesse sentido, o direito a ser esquecido pode traduzir-se numa obrigação de «privacidade desde a concepção».

91. Em suma, a EDPS considera que a portabilidade dos dados e o direito a ser esquecido são conceitos úteis. Valeria a pena incluí-los no diploma, mas limitando-os, provavelmente, ao ambiente electrónico.

6.6. Tratamento de dados pessoais relativos a crianças

92. A Directiva 95/46/CE não prevê normas específicas em relação ao tratamento dos dados pessoais de crianças. Não se reconhece, assim, a necessidade de uma protecção específica das crianças em determinadas circunstâncias, devido à sua vulnerabilidade e à insegurança jurídica que suscita, designadamente nos seguintes domínios:

— a recolha de dados de crianças e a forma como estas devem ser informadas sobre essa recolha,

— a forma como o consentimento das crianças é obtido. Devido à inexistência de normas específicas sobre a forma de obter o consentimento das crianças e a idade em que estas devem ser como tal consideradas, este assunto é tratado no âmbito do direito nacional, que difere consoante os Estados-Membros ([40]),

— a forma e as condições em que as crianças, ou os seus representantes legais, podem exercer os direitos que lhes são outorgados pela directiva.

93. A EDPS considera que os interesses específicos das crianças ficariam mais protegidos se o novo diploma contivesse disposições adicionais que focassem especificamente a recolha e o tratamento dos dados de crianças. Essas disposições específicas também forneceriam segurança jurídica neste domínio e beneficiariam os responsáveis pelo tratamento, que actualmente estão expostos a requisitos jurídicos diferentes.

94. A EDPS sugere que no diploma se incluam as seguintes disposições:

— um requisito para que a informação sobre a recolha de dados seja adaptada às crianças, de modo a que estas entendam facilmente o que significa os seus dados serem recolhidos,

— outros requisitos de informação adaptados às crianças, sobre a maneira como as informações devem ser transmitidas e talvez também sobre o seu conteúdo,

— uma disposição específica que proteja as crianças contra a publicidade comportamental,

— o princípio de limitação da finalidade deve ser reforçado no caso dos dados de crianças,

— algumas categorias de dados nunca devem ser recolhidas junto de crianças,

— um limite de idade. Abaixo desse limite, em regra, só se poderiam recolher informações junto de crianças com o consentimento explícito e verificável dos pais,

— se o consentimento parental for necessário, haverá que estabelecer normas sobre o modo de verificar a

([40]) O consentimento está normalmente ligado à idade em que as crianças podem assumir obrigações contratuais, partindo-se do pressuposto de que as crianças já atingiram um certo nível de maturidade. Por exemplo, a legislação espanhola exige uma autorização parental para recolher os dados de crianças de idade inferior a 14 anos. Acima desta idade, considera-se que as crianças podem dar o seu consentimento. No Reino Unido, a Lei da protecção de dados não refere idades ou limites de idade específicos. Contudo, a autoridade de protecção de dados do Reino Unido interpreta-a no sentido de que as crianças com mais de 12 anos já possam dar o seu consentimento. Em contrapartida, as crianças com menos de 12 anos não o podem fazer e para obter os seus dados pessoais é necessário obter a autorização prévia dos pais ou de um tutor.

idade da criança, ou seja, saber se ela é menor, e a maneira de verificar o consentimento dos pais. Este é um domínio em que a UE se pode inspirar noutros países, por exemplo nos Estados Unidos ([41]).

6.7. *Mecanismos colectivos de recurso*

95. De nada servirá reforçar a substância dos direitos das pessoas se não existirem mecanismos processuais eficazes para aplicar esses direitos. A EDPS recomenda, assim, que se introduzam na legislação da UE mecanismos colectivos de recurso para as violações das normas de protecção de dados. Os mecanismos colectivos de recurso, em especial, ao permitirem que grupos de cidadãos combinem as suas reclamações numa única acção, poderiam constituir um instrumento muito poderoso para facilitar a aplicação das normas de protecção de dados ([42]). Esta inovação também é apoiada pelas autoridades responsáveis pela protecção de dados no documento do Grupo de Trabalho sobre o Futuro da Privacidade.

96. Em casos com menos impacto, é pouco provável que as vítimas de uma violação das normas de protecção de dados intentem acções individuais contra os responsáveis pelo tratamento, devido aos custos, atrasos, incertezas, riscos e dificuldades a que ficariam expostos. Estas dificuldades poderiam ser superadas ou substancialmente reduzidas se existisse um sistema colectivo de recurso que permitisse agregar as acções individuais das vítimas de tais violações numa acção única. A EDPS também seria favorável à concessão de poderes a entidades qualificadas, como associações de consumidores ou organismos públicos, para intentarem acções por perdas e danos em nome das vítimas de violação das normas de protecção de dados. Essas acções em nada prejudicariam o direito das pessoas em causa a intentarem acções individuais.

97. As acções colectivas não só são importantes para garantir a indemnização ou outra acção de reparação como exercem, indirectamente, uma função dissuasória. O risco de incorrer no pagamento de onerosas indemnizações colectivas em tais acções constituiria um incentivo acrescido para os responsáveis pelo tratamento se empenharem em garantir o cumprimento das normas. Neste aspecto, o reforço da aplicação da lei pelos particulares graças aos mecanismos colectivos de recurso complementaria a sua aplicação pelas autoridades públicas.

98. A Comunicação não se pronuncia sobre este tema. A EDPS está ciente do actual debate a nível europeu sobre a introdução da tutela colectiva dos consumidores. Está igualmente ciente do risco de excessos que esses mecanismos podem ocasionar, com base na experiência de outros sistemas jurídicos. Contudo, estes factores não constituem, no seu entender, argumentos suficientes para rejeitar ou adiar a introdução desses mecanismos na legislação de protecção de dados, tendo em conta os benefícios que implicariam ([43]).

7. **Reforço do papel das organizações/responsáveis pelo tratamento**

7.1. *Generalidades*

99. A EDPS considera que, para além de reforçar os direitos das pessoas, um diploma moderno em matéria de protecção de dados deve conter os instrumentos necessários para aumentar a responsabilização dos responsáveis pelo tratamento. Especificamente, o quadro normativo deve conter incentivos para que estes responsáveis, tanto do sector privado como do sector público, tomem a iniciativa de incluir medidas de protecção de dados nos seus processos operacionais. Em primeiro lugar, esses instrumentos seriam úteis porque, como já foi dito, os avanços tecnológicos provocaram um forte crescimento da recolha, utilização e transferência dos dados pessoais, aumentando os riscos para a privacidade e a protecção desses dados, os quais devem ser eficazmente compensados. Em segundo lugar, o quadro actual não possui tais instrumentos, excepto em algumas disposições bem definidas (ver *infra*), e os responsáveis pelo tratamento podem adoptar uma abordagem *reactiva* em matéria de protecção de dados e privacidade, só agindo depois de ocorrer um problema. Esta abordagem reflecte-se nas estatísticas, reveladoras de que as más práticas de aplicação da lei e as perdas de dados são problemas recorrentes.

100. No entender da EDPS, o quadro actual não é suficiente para proteger os dados pessoais eficazmente, nas condições presentes e futuras. Quanto maiores são os riscos, maior a necessidade de aplicar medidas concretas que protejam a informação a nível prático e assegurem uma protecção eficaz. Se essas medidas proactivas não forem *de facto* aplicadas, é provável que continuem a verificar-se erros, contratempos e negligências, pondo em risco a privacidade das pessoas nesta sociedade cada vez mais digital. Para o efeito, a EDPS propõe as medidas seguintes.

7.2. *Reforço da responsabilização dos responsáveis pelo tratamento*

101. A EDPS recomenda que no diploma se insira uma nova disposição exigindo que os responsáveis pelo tratamento apliquem medidas adequadas e eficazes para pôr em prática os princípios e as obrigações nele contidas e que o demonstrem a pedido.

([41]) Nos EUA, a COPPA (Children's Online Privacy Protection Act Rule) requer que os operadores de sítios Internet ou de serviços em linha comerciais dirigidos a crianças com menos de 13 anos de idade obtenham o consentimento dos pais antes de recolherem informações pessoais e que os operadores de sítios Internet comerciais com um público generalista tenham um conhecimento efectivo de que determinados visitantes são crianças.

([42]) Ver também o Parecer da EDPS, 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. 10.

([43]) Algumas legislações nacionais já prevêem mecanismos semelhantes.

102. Este tipo de disposição não é inteiramente novo. O artigo 6.º, n.º 2, da Directiva 95/46/CE alude aos princípios relativos à qualidade dos dados e refere que «incumbe ao responsável pelo tratamento assegurar a observância do disposto no n.º 1». Do mesmo modo, o artigo 17.º, n.º 1, exige que os responsáveis pelo tratamento ponham em prática medidas de carácter técnico e organizativo. No entanto, essas disposições têm um âmbito limitado. A inserção de uma disposição geral relativa à responsabilização incitaria os responsáveis pelo tratamento a adoptarem medidas proactivas que lhes permitissem cumprir todos os elementos da legislação de protecção de dados.

103. Em consequência da disposição relativa à responsabilização, os responsáveis pelo tratamento teriam de adoptar mecanismos e sistemas de controlo internos capazes de garantir o cumprimento dos princípios e obrigações do quadro normativo. Isso exigiria, por exemplo, que os níveis superiores de gestão se envolvessem nos regimes de protecção de dados, que se adoptassem métodos de mapeamento para assegurar a correcta identificação de todas as operações de tratamento de dados, que existissem regimes de protecção de dados vinculativos, constantemente revistos e actualizados de modo a abrangerem novas operações de tratamento de dados, e que se cumprissem os princípios de qualidade, notificação, segurança, acesso, etc., aplicáveis aos dados. Exigiria igualmente que os responsáveis pelo tratamento conservassem elementos comprovativos do cumprimento das normas que pudessem apresentar às autoridades, a pedido destas. A demonstração do cumprimento perante o público em geral também se tornaria, em alguns casos, obrigatória. Para o efeito poder-se-ia, por exemplo, solicitar aos responsáveis pelo tratamento que incluíssem a protecção de dados nos relatórios públicos (anuais) que sejam eventualmente exigidos para outros fins.

104. Evidentemente que os tipos de medidas internas e externas a aplicar devem ser adequados e depender dos factos e circunstâncias de cada caso concreto. É diferente ser responsável pelo tratamento de algumas centenas de registos de clientes que apenas contêm os seus nomes e endereços, ou tratar milhões de registos de doentes, incluindo a respectiva história clínica. O mesmo se aplica às maneiras específicas de avaliar a eficácia das medidas. É necessário haver capacidade de adaptação em termos de escala.

105. O diploma legal geral e completo em matéria de protecção de dados não deve definir os requisitos de responsabilização específicos, mas apenas os elementos essenciais desses requisitos. A Comunicação prevê alguns elementos destinados a reforçar a responsabilidade dos responsáveis pelo tratamento, os quais são muito bem-vindos. Muito em particular, a EDPS apoia inteiramente a proposta de tornar obrigatórias a nomeação de responsáveis pela protecção de dados e as avaliações do impacto na privacidade, sujeitas a certos limiares.

106. Além disso, a EDPS recomenda que se deleguem poderes na Comissão, nos termos do artigo 290.º do TFUE, para complementar os requisitos básicos necessários para dar cumprimento à norma relativa à responsabilização. A utilização desses poderes aumentaria a segurança jurídica dos responsáveis pelo tratamento e harmonizaria o cumprimento das normas em toda a UE. O Grupo de Trabalho do Artigo 29.º e a EDPS deverão ser consultados aquando da elaboração desses instrumentos específicos.

107. Por último, as medidas de responsabilização concretas a aplicar pelos responsáveis pelo tratamento também poderiam ser impostas pelas autoridades responsáveis pela protecção de dados no contexto dos seus poderes de execução. Para o efeito, devem ser outorgados novos poderes a essas autoridades, que lhes permitam impor medidas correctivas ou sanções. Entre os exemplos devem figurar a criação de programas internos de verificação da conformidade, a aplicação da privacidade desde a concepção em produtos e serviços específicos, etc. As medidas correctivas só devem ser impostas se forem adequadas, proporcionadas e eficazes para garantir o cumprimento das normas jurídicas aplicáveis e executáveis.

7.3. Privacidade desde a concepção

108. Entende-se por privacidade desde a concepção a integração da protecção de dados e da privacidade desde o início dos novos produtos, serviços e procedimentos que impliquem o tratamento de dados pessoais. No entender da EDPS, a privacidade desde a concepção é um dos elementos da responsabilização. Consequentemente, os responsáveis pelo tratamento também seriam obrigados a demonstrar que tinham aplicado a privacidade desde a concepção, sempre que necessário. Recentemente, a 32.ª Conferência Internacional dos Comissários para a Protecção dos Dados e da Vida Privada adoptou uma resolução onde reconhece a privacidade desde a concepção como uma componente essencial da protecção do direito fundamental à privacidade ([44]).

109. A Directiva 95/46/CE contém algumas disposições que encorajam a privacidade desde a concepção ([45]), mas não reconhece essa obrigação explicitamente. A EDPS congratula-se com o apoio dado na Comunicação à privacidade desde a concepção como instrumento para garantir o cumprimento das normas de protecção de dados. Sugere

([44]) Resolução sobre a Privacidade desde a Concepção, aprovada pela 32.ª Conferência Internacional dos Comissários para a Protecção dos Dados e da Vida Privada, Jerusalém, 27-29 de Outubro de 2010.

([45]) A Directiva inclui disposições que exigem indirectamente a aplicação da privacidade desde a concepção, em diversas situações. Em especial, o artigo 17.º exige que os responsáveis pelo tratamento ponham em prática medidas técnicas e organizativas para impedir o tratamento ilícito de dados. A Directiva Privacidade e Comunicações Electrónicas é mais explícita. No artigo 14.º, n.º 3, prevê 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».

que se inclua uma disposição vinculativa que estabeleça uma obrigação de «privacidade desde a concepção», possivelmente baseada no texto do considerando 46 da Directiva 95/46/CE. Mais especificamente, a disposição exigiria explicitamente que os responsáveis pelo tratamento tomassem medidas de carácter técnico e organizativo, tanto aquando da concepção do sistema de tratamento como da realização do próprio tratamento, a fim de assegurar, em especial, a protecção dos dados pessoais e impedir qualquer tratamento não autorizado ([46]).

110. Com base nessa disposição, os responsáveis pelo tratamento seriam obrigados, nomeadamente, a garantir que os sistemas de tratamento de dados são concebidos para tratar a menor quantidade possível de dados pessoais, aplicar ambientes de privacidade por defeito, por exemplo nas redes sociais, manter a privacidade dos perfis de umas pessoas em relação a outras por defeito e utilizar instrumentos que permitam que os utilizadores protejam melhor os seus dados pessoais (por exemplo, controlos de acesso e cifragem).

111. As vantagens de fazer uma referência mais explícita à privacidade desde a concepção podem resumir-se da seguinte forma:

— ela realçaria a importância do princípio em si mesmo, como um instrumento para garantir que os processos, produtos e serviços são concebidos desde o início tendo a privacidade em atenção,

— reduziria os ataques à privacidade e minimizaria a recolha desnecessária de dados, além de permitir que as pessoas fizessem escolhas efectivas a respeito dos seus dados pessoais,

— evitaria que se tivesse de recorrer a soluções de recurso para resolver problemas cuja correcção poderá ser difícil, se não impossível,

— também facilitaria a aplicação e a execução eficazes deste princípio pelas autoridades responsáveis pela protecção de dados.

112. O efeito combinado desta obrigação suscitaria uma maior procura de produtos e serviços que incluam a privacidade desde a concepção, dando mais incentivos à indústria para responder a essa procura. Além disso, deveria ponderar-se a criação de uma obrigação distinta dirigida aos conceptores e fabricantes de novos produtos e serviços susceptíveis de afectar a protecção de dados e a privacidade. A EDPS sugere a inclusão dessa obrigação distinta, que também criaria melhores condições para os responsáveis pelo tratamento cumprirem a sua própria obrigação.

113. A codificação da privacidade desde a concepção poderia ser complementada por uma disposição que estabelecesse requisitos gerais de privacidade desde a concepção aplicáveis a diversos sectores, produtos e serviços, garantindo, por exemplo, a adopção de medidas para reforçar a capacidade dos utilizadores em aplicação desse princípio.

114. A EDPS recomenda ainda que se deleguem poderes na Comissão, nos termos do artigo 290.º do TFUE, para complementar, quando necessário, os requisitos básicos de privacidade desde a concepção aplicáveis a determinados produtos e serviços. A utilização desses poderes aumentaria a segurança jurídica dos responsáveis pelo tratamento e harmonizaria o cumprimento das normas em toda a UE. O Grupo de Trabalho do Artigo 29.º e a EDPS deveriam ser consultados aquando do desenvolvimento desses instrumentos específicos (ver, no mesmo sentido, o ponto 106 relativo à responsabilidade).

115. Por último, deveria outorgar-se às autoridades responsáveis pela protecção de dados o poder de impor medidas correctivas ou sanções, em condições restritivas semelhantes às já mencionadas no ponto 107, quando for claro que os responsáveis pelo tratamento não tomaram medidas concretas nos casos em que elas seriam necessárias.

7.4. *Serviços de certificação*

116. A Comunicação reconhece a necessidade de explorar a criação de regimes de certificação da UE para produtos e serviços que respeitem a privacidade. A EDPS subscreve inteiramente este objectivo e sugere que se inclua uma disposição que preveja a criação desses regimes e os seus possíveis efeitos em toda a UE, a qual poderá ser posteriormente desenvolvida para dar lugar a legislação adicional. Essa disposição complementaria as disposições relativas à responsabilização e à privacidade desde a concepção.

117. Os regimes de certificação voluntária permitiriam verificar se um responsável pelo tratamento adoptou medidas para dar cumprimento ao diploma. Além disso, os responsáveis pelo tratamento — ou mesmo os produtos e serviços — que usufruam do benefício de um rótulo de certificação obterão, provavelmente, uma vantagem competitiva sobre os restantes. Esses regimes também auxiliariam as autoridades responsáveis pela protecção de dados na sua função de supervisão e execução.

8. **Globalização e lei aplicável**

8.1. *Clara necessidade de uma protecção mais coerente*

118. Como já foi referido no Capítulo 2, a transferência de dados pessoais para além das fronteiras da UE cresceu exponencialmente em consequência do desenvolvimento de novas tecnologias, do papel das empresas multinacionais e da maior influência dos governos no tratamento e na partilha de dados pessoais a nível internacional. Esta é uma das principais razões que justificam a revisão do actual quadro normativo. Consequentemente, é um dos domínios em que a EDPS pede ambição e eficácia, uma vez que há clara necessidade de uma protecção mais coerente quando os dados são tratados fora da UE.

([46]) No quadro actual, o considerando 46 incentiva os responsáveis pelo tratamento a aplicarem tais medidas, mas é claro que um considerando não é vinculativo.

8.2. *Investir em normas internacionais*

119. No entender da EDPS é necessário investir mais na elaboração de normas internacionais. A maior harmonização do nível de protecção dos dados pessoais em todo o mundo clarificaria consideravelmente a substância dos princípios que devem ser respeitados e das condições para a transferência de dados. Essas normas globais teriam de conciliar a necessidade de um elevado nível de protecção dos dados — incluindo os elementos fundamentais da protecção de dados da UE — com as especificidades regionais.

120. A EDPS apoia o ambicioso trabalho realizado até à data no âmbito da Conferência Internacional dos Comissários para a Protecção dos Dados e da Vida Privada com o intuito desenvolver e difundir as denominadas «normas de Madrid», tendo em vista a sua integração num instrumento vinculativo e o possível lançamento de uma conferência intergovernamental ([47]). Solicita, assim, à Comissão que promova as iniciativas necessárias para facilitar a realização deste objectivo.

121. No entender da EDPS, é igualmente importante garantir a coerência entre esta iniciativa relativa à adopção de normas internacionais, a actual revisão do quadro de protecção de dados da UE e outros acontecimentos, como a actual revisão das directrizes da OCDE em matéria de protecção da vida privada e da Convenção 108 do Conselho da Europa, que está aberta à assinatura de países terceiros (ver também ponto 17). A EDPS considera que a Comissão tem um papel específico a desempenhar nesta matéria, especificando de que modo irá promover essa coerência nas negociações em curso na OCDE e no Conselho da Europa.

8.3. *Clarificar os critérios da lei aplicável*

122. Uma vez que não é fácil obter uma coerência total, continuará a existir — pelo menos num futuro próximo — alguma diversidade entre as leis existentes no interior da UE e *a fortiori* fora das fronteiras da União. A EDPS considera que um novo diploma legal terá de clarificar os critérios que determinam a lei aplicável e de assegurar mecanismos racionalizados para os fluxos de dados, bem como a responsabilização dos intervenientes nesses fluxos.

123. Em primeiro lugar, o diploma deve estipular que a legislação da UE é aplicável quando os dados pessoais são tratados fora das fronteiras da União, mas nos casos em que isso se justifique. O exemplo dos serviços não europeus de computação em nuvem destinados a pessoas residentes na União Europeia ilustra bem essa necessidade. Num ambiente em que os dados não são fisicamente armazenados e tratados num local fixo, em que prestadores de serviços e utilizadores localizados em diferentes países têm uma influência que interfere com os dados, é muito difícil identificar quem é responsável pelo cumprimento dos diversos princípios de protecção de dados. Têm sido dadas orientações, nomeadamente pelas autoridades responsáveis pela protecção de dados, sobre o modo de interpretar e aplicar a Directiva 95/46/CE nesses casos, mas as orientações não são, só por si, suficientes para garantir a segurança jurídica neste novo ambiente.

124. No território da UE, a necessidade de maior precisão no quadro normativo e de um critério simplificado para determinar a lei aplicável foi salientada pelo Grupo de Trabalho do Artigo 29.º num parecer recente ([48]).

125. No entender da EDPS, seria preferível que o diploma assumisse a forma de um regulamento, o que levaria à aplicação de normas idênticas em todos os Estados-Membros. Um regulamento reduziria a importância de determinar a lei aplicável, sendo essa uma das razões por que a EDPS é fortemente favorável à adopção de um regulamento. No entanto, um regulamento também poderia deixar alguma margem de manobra aos Estados-Membros. Caso se mantenha uma margem de manobra significativa no novo diploma, a EDPS apoiaria a sugestão do Grupo de Trabalho para que se substitua uma aplicação distributiva das diversas leis nacionais pela aplicação centralizada de uma legislação única em todos os Estados-Membros onde um responsável pelo tratamento de dados tenha estabelecimentos. Preconiza igualmente uma maior cooperação e coordenação entre as autoridades responsáveis pela protecção de dados nos casos e queixas transnacionais (ver Capítulo 10).

8.4. *Racionalizar os mecanismos de fluxo de dados*

126. A necessidade de coerência e de um parâmetro de referência de alto nível deve ser tida em conta não só com vista aos princípios globais de protecção de dados, mas também no tocante às transferências internacionais. A EDPS apoia inteiramente o objectivo da Comissão de racionalizar os procedimentos em vigor para as transferências internacionais de dados e de garantir uma abordagem mais uniforme e coerente face a países terceiros e a organizações internacionais.

127. O mecanismo dos fluxos de dados inclui transferências do sector privado, em especial através de cláusulas contratuais ou de normas vinculativas para as empresas, e transferências entre autoridades públicas. As normas vinculativas para as empresas são um dos aspectos em que seria desejável uma abordagem mais coerente e racionalizada. A EDPS recomenda que no novo diploma se abordem explicitamente as condições aplicáveis a essas normas ([49]):

— reconhecendo explicitamente as normas vinculativas para as empresas como instrumentos que fornecem garantias adequadas,

— prevendo os principais elementos e condições para a adopção dessas normas,

([47]) Tal como é sugerido na Resolução sobre as normas internacionais, aprovada pela 32.ª Conferência dos Comissários para a Protecção de Dados e da Vida Privada, Jerusalém 27-29 de Outubro de 2010.

([48]) Parecer 8/2010 do Grupo de Trabalho do Artigo 29.º sobre a lei aplicável, WP 179.

([49]) Relativamente às transferências internacionais, ver também o Capítulo 8 do parecer.

— estabelecendo procedimentos de cooperação para a adopção de normas vinculativas para as empresas, incluindo critérios para a selecção de uma autoridade de supervisão principal (balcão único).

9. **O domínio da polícia e da justiça**

9.1. *Quadro geral*

128. A Comissão tem salientado repetidamente a importância de reforçar a protecção de dados no contexto da aplicação da lei e da prevenção da criminalidade, domínios em que o intercâmbio e a utilização de informações pessoais se intensificaram significativamente. O Programa de Estocolmo, aprovado pelo Conselho Europeu, também refere um sólido regime de protecção de dados como principal requisito para a Estratégia de Gestão da Informação da UE neste domínio ([50]).

129. A revisão do quadro geral de protecção de dados constitui a oportunidade perfeita para fazer progressos nesta matéria, sobretudo tendo em conta que a Comunicação afirma, justificadamente, que a Decisão-Quadro 2008/977 é inadequada ([51]).

130. A EDPS apresentou na secção 3.2.5 do presente parecer os motivos por que o domínio da cooperação policial e judiciário deve ser incluído no quadro geral. A inclusão da polícia e da justiça tem várias vantagens adicionais, levando a que as normas deixem de ser apenas aplicáveis ao intercâmbio de dados ([52]) transfronteiras e passem a sê-lo também ao tratamento de dados a nível nacional. Também será garantida uma protecção mais adequada no intercâmbio de dados pessoais com países terceiros, incluindo no que diz respeito aos acordos internacionais. Além disso, as APD terão os mesmos poderes amplos e harmonizados face às autoridades policiais e judiciárias de que dispõem em relação a outros responsáveis pelo tratamento. Por último, o actual artigo 13.º, que prevê que os Estados-Membros podem adoptar legislação específica destinada a restringir as obrigações e os direitos previstos no diploma geral por motivos específicos de interesse público, terá de ser aplicado da mesma forma restritiva em que é aplicado noutros domínios. Em especial, as garantias específicas previstas no diploma geral neste domínio terão de ser igualmente respeitadas na legislação nacional adoptada no domínio da cooperação policial e judiciária.

9.2. *Normas suplementares específicas para a polícia e a justiça*

131. Contudo, essa inclusão não exclui a existência de regras e derrogações especiais, que tenham devidamente em conta as especificidades deste sector, em conformidade com a Declaração 21 anexada ao Tratado de Lisboa. Podem prever-se limitações aos direitos das pessoas em causa, mas elas têm de ser necessárias e proporcionadas e não alterar os elementos essenciais do próprio direito. Convém salientar, neste contexto, que a Directiva 95/46/CE, nomeadamente o seu artigo 13.º, é actualmente aplicável à aplicação da lei em diversos domínios (por exemplo, fiscal, aduaneiro e de luta contra a fraude) que não são fundamentalmente diferentes de muitas actividades no domínio da polícia e da justiça.

132. Além disso, há que adoptar igualmente garantias específicas para compensar a pessoa em causa, dando-lhe uma protecção adicional no domínio em que o tratamento de dados pessoais pode ser mais invasivo.

133. Atendendo ao que precede, a EDPS considera que o novo quadro deve incluir, no mínimo, os seguintes elementos, em conformidade com a Convenção 108 e a Recomendação n.º R (87) 15:

— uma distinção entre as diferentes categorias de dados e ficheiros, em função da sua precisão e fiabilidade, segundo o princípio de que os dados baseados em factos devem ser distinguidos dos dados baseados em opiniões ou juízos pessoais,

— uma distinção entre as várias categorias de pessoas a que os dados se referem (criminosos, suspeitos, vítimas, testemunhas, etc.) e de ficheiros (temporários, permanentes e ficheiros de recolha de informações). É necessário prever condições e garantias específicas para o tratamento de dados de pessoas que não são suspeitas,

— mecanismos para garantir a verificação e a rectificação periódicas dos dados tratados, a fim de garantir a qualidade dos mesmos,

— disposições e/ou garantias específicas que podem ser formuladas em relação ao tratamento (cada vez mais relevante) de dados biométricos e genéticos no domínio da aplicação da lei. A sua utilização deve estar exclusivamente limitada aos casos em que não estão disponíveis meios menos invasivos que possam assegurar o mesmo efeito ([53]),

— as condições aplicáveis às transferências de dados pessoais para autoridades não competentes e particulares, bem como ao acesso e posterior utilização pelas autoridades de aplicação da lei dos dados pessoais recolhidos por particulares.

([50]) Ver a este respeito o Parecer da EDPS, de 30 de Setembro de 2010, sobre a Comunicação da Comissão ao Parlamento Europeu e ao Conselho — «Apresentação geral da gestão da informação no domínio da liberdade, segurança e justiça», pontos 9-19.

([51]) Ver secção 3.2.5 *supra*.

([52]) Este é, actualmente, o âmbito limitado da Decisão-Quadro 2008/977/JAI.

([53]) Neste sentido, ver documento do Grupo de Trabalho sobre o Futuro da Privacidade, n.º 112.

9.3. *Regimes sectoriais de protecção de dados*

134. A Comunicação afirma que «a decisão-quadro não substitui os vários diplomas legislativos aplicáveis a sectores específicos da cooperação policial e judiciária em matéria penal adoptados a nível da UE, em especial os que regulam o funcionamento da Europol, da Eurojust, do Sistema de Informação Schengen (SIS) e do Sistema de Informações Aduaneiras (SIA), que prevêem regimes especiais de protecção de dados e/ou que remetem habitualmente para os instrumentos de protecção de dados do Conselho da Europa».

135. No entender da EDPS, um novo quadro normativo deveria ser, na medida do possível, claro, simples e coerente. Quando há uma proliferação de regimes diferentes aplicáveis, por exemplo, à Europol, à Eurojust, ao SIS e à Decisão Prüm, a conformidade com as normas continua a ser complicada, ou complica-se ainda mais. Este é um dos motivos que levam a EDPS a preferir um diploma global para todos os sectores.

136. Contudo, a EDPS compreende que a harmonização das normas dos diversos sistemas exigirá um trabalho considerável, que deverá ser realizado cuidadosamente. A EDPS considera que uma abordagem gradual, tal como a Comunicação refere, faz sentido desde que o compromisso de garantir um nível elevado de protecção de dados de forma coerente e efectiva permaneça claro e visível. Mais concretamente:

— numa primeira fase, o diploma geral de protecção de dados deve ser aplicável a todo o tratamento de dados no domínio da cooperação policial e judiciária, incluindo as adaptações para a polícia e a justiça (como é referido no n.º 9.2),

— numa segunda fase, os regimes sectoriais de protecção de dados devem ser harmonizados com este diploma geral, devendo a Comissão comprometer-se a adoptar propostas para esta segunda fase, num prazo curto e especificado.

10. **Autoridades responsáveis pela protecção de dados (APD) e cooperação entre APD**

10.1. *Reforço do papel das APD*

137. A EDPS apoia inteiramente o objectivo da Comissão de abordar a questão do estatuto das APD e, mais explicitamente, de reforçar a sua independência, recursos e poderes de execução.

138. A EDPS também insiste na necessidade de clarificar no novo diploma o conceito essencial de independência das APD. O Tribunal de Justiça Europeu tomou recentemente uma decisão sobre este assunto no Processo C-518/07 ([54]), onde salientou que a independência implica a inexistência de quaisquer influências externas. Uma APD não pode pedir nem receber instruções seja de quem for. A EDPS sugere que estes elementos de independência sejam explicitamente codificados na legislação.

139. As APD devem ser dotadas dos recursos humanos e financeiros suficientes para exercerem as suas funções. A EDPS sugere que este requisito seja incluído na legislação ([55]). Destaca, por último, a necessidade de velar por que as autoridades disponham de competências totalmente harmonizadas em termos de investigação e de imposição de medidas correctivas e sanções suficientemente dissuasoras. Reforçar-se-ia, assim, a segurança jurídica para as pessoas em causa e para os responsáveis pelo tratamento.

140. O reforço da independência, dos recursos e dos poderes das APD deve ser acompanhado do reforço da cooperação a nível multilateral, sobretudo tendo em conta o número crescente de questões de protecção de dados que se colocam à escala europeia. A principal infra-estrutura a utilizar para esta cooperação é, evidentemente, o Grupo de Trabalho do Artigo 29.º.

10.2. *Reforço do papel do Grupo de Trabalho*

141. A história mostra que, desde o seu início, em 1997, até ao presente, o funcionamento do grupo evoluiu. Tornou-se mais independente e já não pode ser qualificado, na prática, como um simples grupo de trabalho consultivo ao serviço da Comissão. A EDPS sugere que sejam introduzidas novas melhorias no funcionamento do Grupo de Trabalho, nomeadamente no que se refere à sua infra-estrutura e independência.

142. A EDPS considera que a solidez do grupo está intrinsecamente ligada à independência e às competências dos seus membros. A autonomia do Grupo de Trabalho deve ser assegurada no novo quadro normativo, em conformidade com os critérios desenvolvidos em relação à total independência das APD pelo Tribunal de Justiça Europeu no Processo C-518/07. A EDPS considera que o Grupo de Trabalho também deve ser dotado dos recursos e do orçamento suficientes, bem como de um secretariado reforçado, para apoiar os seus contributos.

143. Quanto ao secretariado do Grupo de Trabalho, a EDPS valoriza o facto de ele estar integrado na Unidade Protecção de Dados da DG Justiça, com a vantagem de o próprio Grupo de Trabalho poder beneficiar de contactos eficientes e flexíveis e de informações actualizadas sobre a evolução no domínio da protecção de dados. Em contrapartida, questiona o facto de a Comissão (e mais especificamente a Unidade) ser simultaneamente membro, secretariado e destinatário dos pareceres do Grupo de Trabalho, o que justificaria uma maior independência do secretariado. A EDPS exorta a Comissão a avaliar — em concertação com os interessados — a melhor forma de assegurar essa independência.

([54]) Processo C-518/07, *Comissão* contra *República Federal da Alemanha*, ainda não publicado na Colectânea de Jurisprudência.

([55]) Ver, por exemplo, o artigo 43.º, n.º 2, do Regulamento (CE) n.º 45/2001, que contém esse requisito em relação à EDPS.

144. Por último, o reforço dos poderes das APD também implica que os poderes do Grupo de Trabalho sejam maiores, com uma estrutura dotada de melhores normas e garantias, bem como de maior transparência. Esta estrutura será desenvolvida tanto para a função consultiva como para a função executiva do Grupo de Trabalho.

10.3. *Função consultiva do Grupo de Trabalho*

145. As posições do Grupo de Trabalho devem ser efectivamente aplicadas, no caso da função consultiva que desempenha junto da Comissão, nomeadamente no que diz respeito à interpretação e aplicação dos princípios da directiva e de outros instrumentos de protecção de dados, ou seja, há que conferir autoridade às posições do Grupo de Trabalho. É necessário um debate mais aprofundado entre as APD para identificar a forma de incluir este aspecto no diploma.

146. A EDPS recomenda que se adoptem soluções que confiram mais autoridade aos pareceres do Grupo de Trabalho sem alterarem substancialmente a sua forma de funcionar. A EDPS sugere que se inclua uma obrigação de que as APD e a Comissão tenham na melhor conta os pareceres e as posições comuns emitidos pelo Grupo de Trabalho, com base no modelo adoptado para as posições do Organismo dos Reguladores Europeus das Comunicações Electrónicas (ORECE) ([56]). Além disso, o novo diploma poderia atribuir ao Grupo de Trabalho a tarefa explícita de emitir «recomendações interpretativas». Estas soluções alternativas confeririam maior força às posições do Grupo de Trabalho, nomeadamente perante os Tribunais.

10.4. *Execução coordenada pelo Grupo de Trabalho*

147. No quadro normativo actual, a aplicação da legislação de protecção de dados nos Estados-Membros é deixada às 27 autoridades responsáveis pela protecção de dados, com pouca coordenação no que se refere à gestão de casos específicas. Quando os casos envolvem mais do que um Estado-Membro ou têm claramente uma dimensão mundial, multiplicam-se os custos para as empresas, que são obrigadas a tratar com diversas autoridades públicas em relação à mesma actividade, para além de esta situação aumentar o risco de incoerência na aplicação da lei: em casos excepcionais, as mesmas actividades de tratamento podem ser consideradas lícitas por uma autoridade e proibidas por outra.

148. Alguns casos têm uma dimensão estratégica, que deve ser abordada de forma centralizada. O Grupo de Trabalho do Artigo 29.º facilita as acções de coordenação e execução entre as APD ([57]) relativamente a importantes questões de protecção de dados com implicações internacionais. Foi o caso das redes sociais e dos motores de busca ([58]), bem como das inspecções coordenadas realizadas em diversos Estados-Membros nos sectores das telecomunicações e dos seguros de saúde.

149. Contudo, há limites para as acções de execução que o Grupo de Trabalho pode realizar ao abrigo do quadro actual. O Grupo de Trabalho pode tomar posições comuns, mas não há instrumentos para garantir que essas posições são efectivamente aplicadas na prática.

150. A EDPS sugere que se incluam no diploma disposições adicionais em apoio da aplicação coordenada, nomeadamente:

— uma obrigação de garantir que as APD e a Comissão têm na melhor conta os pareceres e as posições comuns emitidos pelo Grupo de Trabalho do Artigo 29.º ([59]),

— uma obrigação de que as APD cooperem lealmente entre si, com a Comissão e o Grupo de Trabalho do Artigo 29.º ([60]). Como exemplo ilustrativo de uma cooperação leal na prática, poderia estabelecer-se um procedimento para as APD informarem a Comissão ou o Grupo de Trabalho caso sejam adoptadas medidas coercivas nacionais com um elemento transfronteiriço, em analogia com o procedimento aplicável no quadro actual em relação às decisões nacionais sobre a adequação,

— a especificação das regras de votação para aumentar o empenhamento das APD na aplicação das decisões do Grupo de Trabalho. Poderia definir-se que o Grupo de Trabalho deverá decidir com base no consenso e que quando este não possa ser alcançado, as suas decisões

([56]) Regulamento (CE) n.º 1211/2009 do Parlamento Europeu e do Conselho, de 25 de Novembro de 2009, que cria o Organismo de Reguladores Europeus das Comunicações Electrónicas (ORECE) e o Gabinete, JO L 337 de 18.12.2009, p. 1.

([57]) Para além do Grupo de Trabalho do Artigo 29.º, a Conferência Europeia dos Comissários para a Protecção dos Dados e da Vida Privada criou, há cerca de dez anos, um *workshop* permanente destinado a abordar as queixas transfronteiriças de forma coordenada. Embora este *workshop* represente um valor acrescentado indiscutível em termos de intercâmbio entre o pessoal das APD e ofereça uma rede fiável de pontos de contacto, não pode ser considerado como um mecanismo de coordenação para a tomada de decisões.

([58]) Ver as cartas do Grupo de Trabalho do Artigo 29.º de 12 de Maio de 2010 e 26 de Maio de 2010, publicadas no sítio Internet do Grupo (http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010-others_en.htm).

([59]) Como já foi mencionado, está prevista uma obrigação semelhante no Regulamento (CE) n.º 1211/2009 que especifica as funções do Organismo de Reguladores Europeus das Comunicações Electrónicas (ORECE).

([60]) Ver, a este respeito, o artigo 3.º do Regulamento (CE) n.º 1211/2009, atrás citado.

só podem ser aplicadas por maioria qualificada. Complementarmente, poderia prever-se, num considerando, que as APD que votem a favor de um documento têm a obrigação ou o compromisso político de o aplicarem a nível nacional.

151. A EDPS colocaria uma restrição à introdução de medidas mais fortes, como a de tornar as posições do Grupo de Trabalho do Artigo 29.º vinculativas. Isso prejudicaria o estatuto de independência de cada uma das DPA, o qual deve ser garantido pelos Estados-Membros nos termos da legislação nacional. Se as decisões do Grupo de Trabalho tivessem um impacto directo em terceiros como os responsáveis pelo tratamento, deveriam prever-se novos procedimentos que incluíssem garantias como a transparência e o recurso, incluindo o eventual recurso perante o Tribunal de Justiça Europeu.

10.5. *Cooperação entre a EDPS e o Grupo de Trabalho*

152. A forma como a EDPS e o Grupo de Trabalho cooperam também poderá ser melhorada. A EDPS é membro do Grupo de Trabalho e contribui no seu seio para as posições relativas aos principais avanços estratégicos da UE, ao mesmo tempo que garante a coerência com as suas próprias posições. A EDPS observa o número crescente de questões de privacidade, tanto no sector privado como no sector público, que têm implicações a nível nacional em muitos Estados-Membros e em que o Grupo de Trabalho tem um papel específico a desempenhar.

153. A EDPS desempenha a função complementar de emitir pareceres sobre a evolução no contexto da UE, a qual deve ser mantida. Como organismo europeu, exerce a sua competência consultiva junto das Instituições da UE da mesma forma que as APD aconselham os respectivos governos.

154. A EDPS e o Grupo de Trabalho actuam de uma perspectiva diferente, mas complementar. É, por isso, necessário preservar e talvez melhorar a coordenação entre o Grupo de Trabalho e a EDPS, a fim de assegurar que colaboram nas principais questões de protecção de dados, por exemplo coordenando as suas agendas regularmente ([61]) e garantindo a transparências nas questões que têm um aspecto mais nacional ou mais especificamente da UE.

155. A coordenação não é mencionada na actual directiva pela simples razão de que a EDPS não existia na altura em que ela foi adoptada, mas ao fim de seis anos de existência, as complementaridades da EDPS e do Grupo de Trabalho são visíveis e poderiam ser formalmente reconhecidas. A EDPS recorda que, nos termos do Regulamento (CE) n.º 45/2001, tem o dever de cooperar com as APD nacionais e de participar nas actividades do Grupo de Trabalho. Recomenda, assim, que se mencione explicitamente a cooperação no novo diploma e que ela seja estruturada na medida do necessário, por exemplo, prevendo um procedimento de cooperação.

10.6. *Cooperação entre a EDPS e as APD na supervisão dos sistemas da UE*

156. Estas considerações são igualmente aplicáveis a domínios em que a supervisão deve ser coordenada entre o nível europeu e o nível nacional. É o caso dos organismos da UE que tratam significativas quantidades de dados entregues pelas autoridades nacionais ou dos sistemas de informação de grande dimensão com uma componente europeia ou nacional.

157. O actual sistema de alguns organismos da UE e sistemas de informação de grande dimensão — por exemplo, a Europol, a Eurojust e a primeira geração do Sistema de Informação Schengen (SIS) têm instâncias comuns de controlo com representantes das APD nacionais — é uma reminiscência da cooperação intergovernamental da era anterior ao Tratado de Lisboa e não respeita a estrutura institucional da UE, de que a Europol e a Eurojust são agora uma parte integrante e na qual o «acervo de Schengen» também já foi integrado ([62]).

158. A Comunicação anuncia que a Comissão irá lançar em 2011 uma consulta das partes interessadas sobre a revisão destes sistemas de supervisão. A EDPS insta a Comissão a tomar posição, o mais rapidamente possível (num prazo curto e especificado, ver supra), no actual debate sobre a supervisão. Nesse debate, a EDPS assumirá o seguinte ponto de vista.

159. Como ponto de partida, deve garantir-se que todos os organismos de supervisão preenchem os indispensáveis critérios de independência, recursos e poderes de execução. Além disso, deve assegurar-se que as perspectivas e os conhecimentos especializados existentes a nível da UE são tidos em conta. Isto significa que a cooperação se deve verificar não só entre as autoridades nacionais, mas também com a APD europeia (actual EDPS). A EDPS considera necessário seguir um modelo que preencha estes requisitos ([63]).

160. Nos últimos anos, foi desenvolvido o modelo de «supervisão coordenada». Este modelo de supervisão, presentemente em vigor no Eurodac e em partes do Sistema de Informações Aduaneiras, em breve será alargado ao Sistema de Informação sobre Vistos (SIV) e à segunda geração do Sistema de Informação Schengen (SIS II). Este modelo tem três níveis: (1) a supervisão a nível nacional é assegurada pelas APD; (2) a supervisão a nível da UE é assegurada pela EDPS; (3) a coordenação é assegurada

([61]) Por exemplo, com base no Inventário dos actos regulamentares, publicado anualmente e regularmente actualizado, que está disponível no sítio Internet da EDPS.

([62]) Nos termos do Regulamento (CE) n.º 45/2001, a EDPS tem o dever de cooperar com estes organismos.

([63]) No caso da Eurojust, o modelo também deve prever que a supervisão da protecção de dados respeite a independência do sistema judiciário, na medida em que a Eurojust trata dados no contexto dos processos penais.

através de reuniões regulares organizadas pela EDPS, actuando como secretariado deste mecanismo de coordenação. Este modelo já provou ser bem-sucedido e eficaz, devendo ser futuramente considerado para outros sistemas de informação.

C. **COMO MELHORAR A APLICAÇÃO DO QUADRO ACTUAL?**

11. **A curto prazo**

161. Embora o processo de revisão esteja em curso, há que envidar esforços para aplicar as normas actuais de forma plena e efectiva. Estas normas continuarão a ser aplicáveis até o futuro quadro ser adoptado e transposto para as legislações nacionais dos Estados-Membros. Neste sentido, é possível identificar várias linhas de acção.

162. Em primeiro lugar, a Comissão deverá continuar a acompanhar o cumprimento da Directiva 95/46/CE pelos Estados-Membros e, quando necessário, a utilizar os poderes que lhe são conferidos pelo artigo 258.º TFUE. Recentemente, foram instaurados processos por infracção devido à incorrecta aplicação do artigo 28.º da Directiva no que respeita ao requisito de independência das APD ([64]), mas é necessário fiscalizar e assegurar o pleno cumprimento também noutros domínios. ([65]) A EDPS acolhe, assim, favoravelmente e apoia inteiramente o compromisso formulado na Comunicação da Comissão de prosseguir uma política de repressão das infracções. A Comissão também deverá prosseguir o diálogo estrutural com os Estados-Membros sobre a implementação da directiva ([66]).

163. Em segundo lugar, a aplicação a nível nacional deve ser incentivada de modo a garantir a aplicação na prática das normas de protecção de dados, nomeadamente no que diz respeito aos novos fenómenos tecnológicos e aos intervenientes a nível mundial. As APD devem utilizar plenamente os seus poderes de investigação e sanção. É igualmente importante que os actuais direitos das pessoas em causa, em especial os direitos de acesso, sejam cabalmente postos em prática.

164. Em terceiro lugar, afigura-se necessário assegurar uma maior coordenação da aplicação a curto prazo. O papel do G29 e dos seus documentos interpretativos nesta matéria é crucial, mas as APD também devem esforçar-se ao máximo para os pôr em prática. É necessário evitar resultados divergentes nos casos a nível da UE ou a nível mundial, sendo possível e desejável que se consiga chegar a posições comuns no âmbito do Grupo de Trabalho. As investigações coordenadas a nível da UE sob a égide do Grupo de Trabalho também podem trazer um valor acrescentado significativo.

165. Em quarto lugar, os princípios de protecção de dados devem ser «incorporados» de forma proactiva nas novas regulamentações que possam ter um impacto directo ou indirecto na protecção de dados. A nível da UE, a EDPS realiza esforços consideráveis no sentido de contribuir para melhorar a legislação da UE, e esses esforços devem ser desenvolvidos também a nível nacional. As autoridades responsáveis pela protecção de dados devem, pois, utilizar plenamente as suas competências consultivas para garantirem essa abordagem proactiva. As autoridades responsáveis pela protecção de dados, incluindo a EDPS, também podem desempenhar um papel proactivo no acompanhamento dos avanços tecnológicos. Esse acompanhamento é importante para identificar precocemente as tendências emergentes, revelando as suas eventuais implicações para a protecção de dados, apoiando soluções favoráveis a essa protecção e sensibilizando para ela as partes interessadas.

166. Por último, é necessário promover activamente uma cooperação aprofundada entre os diversos intervenientes a nível internacional, sendo, por isso, importante reforçar os instrumentos de cooperação internacionais. Iniciativas como as normas de Madrid e o trabalho em curso no âmbito do Conselho da Europa e da OCDE merecem todo o apoio. Neste contexto, é muito positivo que a Comissão Federal do Comércio dos EUA também tenha aderido agora à «família» dos Comissários para a Protecção dos Dados e da Vida Privada no âmbito da sua Conferência Internacional.

D. **CONCLUSÕES**

OBSERVAÇÕES GERAIS

167. A EDPS congratula-se com a Comunicação da Comissão em geral, pois considerar que a revisão do actual quadro normativo em matéria de protecção de dados é necessária para assegurar uma protecção eficaz numa sociedade da informação cada vez mais desenvolvida e globalizada.

168. A Comunicação identifica as questões e os desafios principais. A EDPS concorda com a opinião da Comissão de que, no futuro, continuará a ser necessário um sistema de protecção de dados forte, com base na ideia de que os actuais princípios gerais de protecção de dados permanecem válidos numa sociedade sujeita a profundas mutações. A EDPS subscreve a afirmação da Comunicação de que os desafios são enormes e sublinha que, em consequência, as soluções propostas devem ter um nível de ambição correspondente e aumentar a eficácia da protecção. Por conseguinte, solicita uma abordagem mais ambiciosa em vários aspectos.

169. A EDPS apoia totalmente a abordagem global da protecção de dados. No entanto, lamenta que a Comunicação exclua certos domínios do diploma geral, designadamente o tratamento de dados pelas instituições e os organismos da UE. Caso a Comissão efectivamente decida deixar de

([64]) Ver Processo C-518/07, atrás citado e o Comunicado de Imprensa da Comissão de 28 de Outubro de 2010 (IP/10/1430).

([65]) A Comissão instaurou um processo por infracção contra o Reino Unido devido à alegada violação de várias disposições de protecção de dados, incluindo o requisito de confidencialidade das comunicações electrónicas no que diz respeito à publicidade comportamental. Ver Comunicado de Imprensa da Comissão de 9 de Abril de 2009 (IP/09/570).

([66]) Ver, a este respeito, o Primeiro Relatório da Comissão sobre a implementação da Directiva relativa à protecção de dados, atrás citado, pp. 22 *et seq*.

fora alguns domínios, a EDPS exorta-a a adoptar uma proposta para o nível da UE no mais curto prazo possível, mas de preferência até finais de 2011.

PERSPECTIVAS PRINCIPAIS

170. Para a EDPS os pontos de partida do processo de revisão são os seguintes:

— as disposições relativas à protecção de dados devem, tanto quanto possível, apoiar activamente outros interesses legítimos e não dificultá-los (como é o caso da economia europeia, da segurança das pessoas e da responsabilização dos governos),

— os princípios gerais de protecção de dados não devem nem podem ser alterados,

— a maior harmonização deve ser um dos principais objectivos da revisão,

— a perspectiva dos direitos fundamentais deve estar no centro do processo de revisão. Um direito fundamental visa proteger os cidadãos em todas as circunstâncias,

— o novo diploma deve incluir o sector policial e judiciário,

— o novo diploma deve ser, tanto quanto possível, formulado de forma tecnologicamente neutra e procurar gerar segurança jurídica a longo prazo.

ELEMENTOS DE UM NOVO QUADRO

Harmonização e simplificação

171. A EDPS congratula-se com o compromisso da Comissão de analisar os meios de conseguir maior harmonização das normas de protecção de dados a nível da UE. A EDPS aponta os domínios em que é urgente uma maior e melhor harmonização: definições, motivos para o tratamento de dados, direitos das pessoas em causa, transferências internacionais e autoridades responsáveis pela aplicação dos dados.

172. A EDPS sugere que se ponderem as seguintes alternativas para simplificar e/ou reduzir o âmbito dos requisitos de notificação:

— limitar a obrigação de notificação a alguns tipos de operações de tratamento que impliquem riscos específicos,

— uma obrigação de registo simples exigindo que os responsáveis pelo tratamento se registem (em lugar de se registarem todas as operações de tratamento de dados),

— a introdução de um formulário de notificação normalizado a nível pan-europeu.

173. No entender da EDPS, um regulamento, instrumento único directamente aplicável nos Estados-Membros, é o meio mais eficaz para proteger o direito fundamental à protecção de dados e alcançar uma maior convergência no mercado interno.

Reforço dos direitos das pessoas

174. A EDPS subscreve a Comunicação quando propõe que se reforcem os direitos das pessoas e apresenta as seguintes sugestões:

— pode introduzir-se na lei um princípio de transparência. Contudo, é mais importante reforçar as actuais disposições relativas à transparência (como os actuais artigos 10.º e 11.º da Directiva 95/46/CE),

— deve introduzir-se no diploma geral uma disposição sobre a notificação da violação dos dados pessoais, que alargue a todos os responsáveis pelo tratamento a obrigação aplicável a alguns prestadores que foi incluída na Directiva Privacidade e Comunicações Electrónicas revista,

— os limites do consentimento devem ser clarificados. Deve ponderar-se a possibilidade de prever um maior número de situações em que o consentimento explícito seja exigido, bem como a adopção de normas adicionais para o ambiente em linha,

— devem ser introduzidos direitos adicionais, como a portabilidade dos dados e o direito a ser esquecido, sobretudo para os serviços da sociedade da informação na Internet,

— os interesses das crianças devem ser mais eficazmente protegidos com várias disposições suplementares, especificamente direccionadas para a recolha e o tratamento de dados relativos a crianças,

— devem introduzir-se na legislação da UE mecanismos colectivos de recurso para a violação das normas de protecção de dados, a fim de outorgar poderes a entidades qualificadas para intentarem acções em nome de grupos de pessoas.

Reforço das obrigações das organizações/responsáveis pelo tratamento

175. O novo quadro deve conter incentivos para que os responsáveis pelo tratamento tomem a iniciativa de incluir medidas de protecção de dados nos seus processos operacionais. A EDPS propõe que se introduzam disposições gerais em matéria de responsabilização e de «privacidade desde a concepção». Também deve ser introduzida uma disposição relativa aos regimes de certificação da privacidade.

Globalização e lei aplicável

176. A EDPS apoia o ambicioso trabalho realizado no âmbito da Conferência Internacional dos Comissários para a Protecção dos Dados e da Vida Privada com o intuito de desenvolver as denominadas «normas de Madrid», tendo em vista a sua integração num instrumento vinculativo e o possível lançamento de uma conferência intergovernamental. A EDPS solicita à Comissão que tome medidas concretas nesse sentido, em estreita cooperação com a OCDE e o Conselho da Europa.

177. Um novo diploma deve clarificar os critérios que determinam a lei aplicável. Deve garantir-se que os dados tratados fora das fronteiras da UE não escapam à jurisdição da União quando a aplicação da sua legislação se justificar. Se o quadro normativo assumir a forma de um regulamento, existirão normas idênticas em todos os Estados-Membros e tornar-se-á menos relevante determinar a lei aplicável (na UE).

178. A EDPS apoia totalmente o objectivo de garantir uma abordagem mais uniforme e coerente face a países terceiros e a organizações internacionais. No diploma devem incluir-se normas vinculativas para as empresas.

O domínio da polícia e da justiça

179. Um instrumento global que inclua a polícia e a justiça pode prever normas especiais que tenham devidamente em conta as especificidades deste sector, em conformidade com a Declaração 21 anexada ao Tratado de Lisboa. É necessário adoptar garantias específicas, para compensar as pessoas em causa dando-lhes uma protecção adicional num domínio em que o tratamento de dados pessoais é, por natureza, mais invasivo.

180. O novo quadro normativo deve, na medida do possível, ser claro, simples e coerente. Há que evitar a proliferação de diferentes regimes aplicáveis, por exemplo, à Europol, à Eurojust, ao SIS e à Decisão Prüm. A EDPS compreende que a harmonização das normas dos diversos sistemas terá de ser realizada de forma cuidadosa e gradual.

As APD e a cooperação entre APD

181. A EDPS apoia inteiramente o objectivo da Comissão de abordar a questão do estatuto das autoridades responsáveis pela protecção de dados (APD) e de reforçar a sua independência, os seus recursos e os seus poderes de execução. Recomenda:

— que se codifique no novo diploma o conceito essencial de independência das APD, tal como é especificado pelo Tribunal de Justiça Europeu,

— que se consagre na legislação que as APD devem ser dotadas de recursos suficientes,

— que se outorguem às autoridades poderes harmonizados de investigação e sanção.

182. A EDPS sugere que se introduzam novas melhorias no funcionamento do Grupo de Trabalho do artigo 29.º, nomeadamente quanto à sua independência e infra-estrutura. O Grupo de Trabalho também deve ser dotado de recursos suficientes e de um secretariado reforçado.

183. A EDPS sugere que se reforce o papel consultivo do Grupo de Trabalho mediante a introdução de uma obrigação para que as APD e a Comissão *tenham na melhor conta os pareceres e as posições comuns* emitidos pelo Grupo de Trabalho. A EDPS não é favorável a que as posições do Grupo de Trabalho se tornem vinculativas, sobretudo devido ao estatuto independente das diversas APD. A EDPS recomenda que a Comissão introduza disposições específicas para aumentar a cooperação com a EDPS no novo diploma.

184. A EDPS insta a Comissão a tomar posição, o mais rapidamente possível, sobre a questão da supervisão dos organismos da UE e dos sistemas de informação de grande dimensão, tomando em consideração que todos os organismos de supervisão devem satisfazer os indispensáveis critérios de independência, recursos suficientes e poderes de execução, e que se deve garantir que a perspectiva da UE está devidamente representada. A EDPS apoia o modelo de «supervisão coordenada».

Melhorias no âmbito do actual sistema:

185. A EDPS incentiva a Comissão a:

— continuar a acompanhar o cumprimento da Directiva 95/46/CE pelos Estados-Membros e, sempre que necessário, a utilizar os poderes de execução que lhe são conferidos pelo artigo 258.º TFUE,

— incentivar a aplicação a nível nacional e a coordenação da aplicação,

— incorporar de forma proactiva os princípios de protecção de dados nas novas regulamentações que possam ter impacto, directa ou indirectamente, na protecção de dados,

— prosseguir e aprofundar a cooperação entre os vários intervenientes a nível internacional.

Feito em Bruxelas, em 14 de Janeiro de 2011.

Peter HUSTINX

Supervisor Europeu para a Protecção de Dados