AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS

Parecer da Autoridade Europeia para a Protecção de Dados sobre a proposta de decisão-quadro do Conselho relativa ao intercâmbio de informações com base no princípio da disponibilidade (COM(2005) 490 final)

(2006/C 116/04)

A AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS

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

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

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

Tendo em conta o pedido de parecer nos termos do n.º 2 do artigo 28.º do 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,

ADOPTOU O SEGUINTE PARECER:

I. OBSERVAÇÕES PRELIMINARES

1. A proposta de decisão-quadro do Conselho relativa ao intercâmbio de informações com base no princípio da disponibilidade foi transmitida pela Comissão à AEPD por carta de 12 de Outubro de 2005. A AEPD interpreta essa carta como um pedido de aconselhamento das instituições e órgãos comunitários, como prevê o n.º 2 do artigo 28.º do Regulamento (CE) n.º 45/2001/CE. No entender da AEPD, o presente parecer deve ser referido no preâmbulo da decisão-quadro.

2. A natureza deste parecer deve ser vista no contexto do exposto no ponto II. Tal como exposto no ponto II, não é de todo provável que o presente parecer, ou a abordagem da disponibilidade seguida pela proposta, conduza eventualmente à adopção de um instrumento jurídico. Um número considerável de Estados-Membros defende outras soluções.

3. Contudo, é evidente que a temática da disponibilização de informações em matéria de aplicação da lei além fronteiras internas ou, mais amplamente, o intercâmbio dessas informações, é prioritário na agenda dos Estados-Membros, tanto dentro como fora do Conselho e no Parlamento Europeu.

4. É de igual forma evidente que este assunto é altamente importante do ponto de vista da protecção dos dados pessoais, tal como o presente parecer demonstrará. A AEPD relembra que a presente proposta foi apresentada pela Comissão em relação estreita com a proposta de decisão-quadro do Conselho relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal, objecto de um parecer da AEPD, que foi apresentada em 19 de Dezembro de 2005.

5. A AEPD aproveitará esta ocasião para apresentar no presente parecer alguns pontos de vista gerais e de carácter mais fundamental relativamente à questão do intercâmbio de informações em matéria de aplicação da lei e às abordagens para regulamentar essa mesma matéria. Ao apresentar este parecer, a AEPD pretende assegurar-se de que a perspectiva da protecção de dados será devidamente tida em consideração em discussões futuras na matéria.

6. A AEPD estará disponível para novas consultas numa fase posterior, no seguimento de progressos importantes no processo legislativo desta proposta e de outras com ela relacionadas.

II. A PROPOSTA NO SEU CONTEXTO

7. O princípio da disponibilidade foi introduzido como um princípio de direito importante no Programa da Haia. Implica que a informação necessária para a luta contra o crime deva atravessar as fronteiras internas da UE sem obstáculos. O objectivo da presente proposta é implementar este princípio num acto jurídico vinculativo.

8. O intercâmbio de informações policiais entre diferentes países é um assunto recorrente entre os legisladores, dentro e fora do âmbito da UE. Recentemente, as seguintes iniciativas chamaram a atenção da AEPD.

9. Em primeiro lugar, a 4 de Junho de 2004, a Suécia propôs uma decisão-quadro relativa à simplificação do intercâmbio de dados e informações entre as autoridades de aplicação da lei dos Estados-Membros da União Europeia. Relativamente a esta proposta, o Conselho chegou a acordo sobre uma abordagem geral na sessão de 1 de Dezembro de 2005.

10. Em segundo lugar, a 27 de Maio de 2005, sete Estados Membros assinaram uma Convenção em Prüm (Alemanha) relativa à intensificação da cooperação transfronteiras, especialmente na luta contra o terrorismo, o crime transfronteiras e a emigração ilegal. Introduz, *inter alia*, medidas para melhorar o intercâmbio de informações relativas ao ADN e às impressões digitais. Qualquer Estado-Membro da União Europeia poderá aderir à Convenção. As Partes Contratantes pretendem incorporar as disposições da Convenção no quadro jurídico da União Europeia.

11. Em terceiro lugar, a disponibilização de informações em matéria de aplicação da lei através das fronteiras internas da União Europeia será também facilitada por outros instrumentos jurídicos, tal como as propostas relativas ao Sistema de Informação de Schengen de segunda geração (SIS II), a proposta de acesso para consulta do Sistema de Informação sobre Vistos (VIS) e a proposta de decisão-quadro relativa à organização e ao conteúdo do intercâmbio de informações extraídas de registos criminais entre os Estados-Membros. Nesta matéria, é também útil referir a Comunicação relativa ao reforço da eficácia, a operabilidade avançada e as sinergias entre as bases de dados europeias no domínio da Justiça e dos Assuntos Internos, emitida pela Comissão em 25 de Novembro de 2005.

12. Uma vez que foram apresentadas todas esta iniciativas, a presente proposta de decisão-quadro relativa à disponibilidade não deve ser examinada isoladamente, outras abordagens relativas ao intercâmbio de informações em matéria de aplicação da lei devem também ser tidas em consideração. A sua relevância é ainda maior devido ao facto de ser tendência actual no Conselho dar preferência a outras abordagens de como proceder ao intercâmbio de informações e ao conceito de disponibilidade, que não a abordagem geral proposta pela Comissão na presente proposta. Este texto da proposta poderá até não ser objecto de discussão no Conselho.

13. Para além disso, esta proposta está estreitamente ligada à proposta de decisão-quadro do Conselho relativa à protecção de dados pessoais. O presente parecer deve ser entendido em relação com o parecer mais aprofundado sobre esta última decisão-quadro.

14. No parecer sobre a proposta de decisão-quadro do Conselho relativa à protecção de dados pessoais, a AEPD sublinhou a importância de uma protecção de dados adequada enquanto consequência necessária de um instrumento jurídico sobre a disponibilidade. Para a AEPD, esse instrumento não deve ser adoptado sem garantias essenciais sobre a protecção de dados.

15. A AEPD toma a mesma posição quanto à adopção de outros instrumentos jurídicos que facilitem a circulação interna na UE das informações em matéria de aplicação da lei. Por conseguinte, a AEPD congratula-se por o Conselho e o Parlamento Europeu terem dado prioridade à proposta acima referida de decisão-quadro sobre a protecção de dados pessoais.

III. **O PRINCÍPIO DA DISPONIBILIDADE EM SI**

16. O princípio da disponibilidade em si é um princípio simples. As informações ao dispor de certas autoridades de um Estado-Membro devem ser fornecidas às autoridades equivalentes em outros Estados-Membros. As informações devem ser trocadas o mais rápida e facilmente possível entre as autoridades dos Estados-Membros e de preferência permitindo o acesso directo em linha.

17. As dificuldades surgem devido ao ambiente em que o princípio da disponibilidade tem de ser efectivado:

— Uma organização heterogénea dos serviços policiais e judiciários dos Estados-Membros, com controlos e equilíbrios diferentes.

— São incluídos diferentes tipos de informações sensíveis (tal como o ADN ou as impressões digitais).

— Diferentes maneiras de aceder às informações relevantes pelas autoridades competentes até mesmo dentro dos próprios Estados-Membros.

— É difícil assegurar que informações originárias de um outro Estado-Membro sejam correctamente interpretadas devido a diferenças nas línguas, nos sistemas tecnológicos (interoperabilidade) e nos sistemas jurídicos.

— Tem de ser incluído no vasto enumerado vigente de disposições legais que tratam do intercâmbio de informações em matéria de aplicação da lei entre países.

18. Independentemente deste ambiente complexo, é senso comum que este princípio não pode funcionar isoladamente. São necessárias medidas adicionais para assegurar que as informações possam ser efectivamente encontradas e estejam acessíveis. De qualquer forma, estas medidas devem ajudar as autoridades competentes para a aplicação da lei a apurar se as autoridades competentes para a aplicação da lei nos outros Estados-Membros têm informações relevantes à sua disposição e onde essas informações relevantes podem ser encontradas. Tais medidas adicionais podem consistir em interfaces que permitam o acesso directo a todas as informações ou informações específicas em posse de outro Estado-Membro. A proposta de decisão-quadro sobre a disponibilidade introduz, por esta razão, «dados de índice», dados que podem ser acedidos directamente além fronteiras.

19. Em termos gerais, o princípio da disponibilidade deve facilitar a circulação de informações entre os Estados-Membros. As fronteiras internas serão abolidas e os Estados-Membros terão de permitir que as informações disponíveis para as suas autoridades policiais sejam cada vez mais acessíveis às outras autoridades. Os Estados-Membros perdem competência para controlar a circulação de informações, o que também resulta no facto de já não poderem contar com a legislação nacional enquanto instrumento suficiente para uma protecção adequada das informações.

20. É por esta razão que a proposta necessita de atenção específica do ponto de vista da protecção dos dados pessoais. Em primeiro lugar, as informações que são normalmente confidenciais e bem protegidas devem ser facultadas às autoridades nos outros Estados-Membros. Em segundo lugar, para fazer o sistema funcionar, devem ser criados dados de índice, que serão facultados às autoridades nos outros Estados-Membros. A implementação deste princípio criará, por conseguinte, mais dados do que os actualmente disponíveis.

IV. **ELEMENTOS PRINCIPAIS**

Âmbito do princípio da disponibilidade

21. Primeiramente, é essencial definir a que tipo de informações se aplicará o princípio da disponibilidade. O âmbito de aplicação deste princípio é definido em termos gerais no artigo 2.º da proposta, em conjugação com o n.º 1 do artigo 1.º e a alínea a) do n.º 3 do artigo 3.º. O princípio aplicar-se-á às informações:

    — existentes;

    — enumeradas no Anexo II, que define seis tipos de informação;

    — acessíveis às autoridades competentes.

    Estes são os três elementos essenciais do âmbito do princípio na proposta da Comissão. O âmbito é seguidamente afinado no artigo 2.º. O n.º 1 do artigo 2.º limita a aplicação do princípio da disponibilidade à fase anterior à instauração de um processo, enquanto os n.ºs 2, 3 e 4 do artigo 2.º prevêem algumas restrições mais especificas.

22. Para compreender as consequências da proposta, é necessária uma análise mais profunda dos três elementos essenciais acima mencionados. Os primeiros dois elementos do âmbito são, por si só, razoavelmente claros. A definição «informações existentes» é elaborada no n.º 2 do artigo 2.º, que estabelece que a decisão-quadro não implica nenhuma obrigação de recolher e armazenar informações com o único objectivo de as tornar acessíveis, ao passo que a lista no Anexo II não pode ser interpretada de maneiras diferentes. É o terceiro elemento essencial, por si só, e em conjugação com os primeiros dois elementos, que precisa de ficar bem esclarecido.

23. A proposta não especifica se «informações acessíveis» são simplesmente informações já controladas pelas autoridades competentes ou se também incluem informações que podem vir a ser obtidas por essas autoridades. Para a AEPD, contudo, a proposta pode ser interpretada como contemplando as duas.

24. Efectivamente, enquanto o n.º 2 do artigo 2.º parece sugerir um âmbito mais restrito, especificando que a decisão-quadro «não implica qualquer obrigação de recolher e armazenar informações […] com o único objectivo de as tornar acessíveis», a alínea a) do artigo 3.º permite uma interpretação mais alargada, estipulando que se deve entender por «informações» as «informações existentes, enumeradas no Anexo II».

25. O Anexo II menciona pelo menos duas categorias de informações que são habitualmente controladas por outros que não a polícia. A primeira categoria é constituída pelas informações sobre as matrículas de veículos. Em muitos Estados-Membros, as bases de dados que contêm essas informações não são controladas pelas autoridades de aplicação da lei, apesar de estas autoridades acederem regularmente a elas. Deverá este tipo de informações ser considerada no âmbito da «informação disponível» que, de acordo com o artigo 1.º, deverá ser facultado às autoridades competentes equivalentes do outro Estado-Membro? A segunda categoria de informações enumeradas no Anexo II são números de telefone e outros dados sobre comunicações. Deverão estas informações ser consideradas «disponíveis» mesmo quando não são controladas pelas autoridades competentes, mas por companhias privadas?

26. Ademais, outras disposições da proposta, em particular a alínea d) do artigo 3.º e a alínea c) do n.º 1 do artigo 4.º, apoiam o ponto de vista de que «autoridades designadas» e até mesmo «partes designadas» possam controlar informações «disponíveis» para «autoridades competentes». Também decorre do texto da proposta que uma «autoridade competente» de um Estado-Membro é uma autoridade contemplada pela primeira alínea do artigo 26.º do TUE visto que cada autoridade nacional pode constituir uma «autoridade designada».

27. Para a AEPD, a aplicação do princípio da disponibilidade às informações que são controladas pelas autoridades designadas e pelas partes designadas implica as seguintes questões:

    — A alínea b) do n.º 1 do artigo 30.º prevê uma base jurídica suficiente tendo em conta que a informação tem de ser disponibilizada pelas autoridades designadas e pelas partes designadas a partir de bases de dados que não se inserem no quadro estabelecido no âmbito do terceiro pilar?

    — Aplicar-se-á a decisão-quadro relativa à protecção de dados pessoais como previsto, por exemplo, no artigo 8.º da proposta?

    — Caso não se aplique, o tratamento é feito de acordo com as obrigações decorrentes da Directiva 95/46/CE?

28. A implementação de um princípio tão vasto como o «princípio da disponibilidade» requer uma definição clara e precisa das informações que devem ser consideradas disponíveis. Por conseguinte, a AEPD recomenda:

— clarificar o âmbito.

— como primeira opção, limitar o âmbito do princípio da disponibilidade às informações controladas pelas autoridades competentes.

— como segunda opção, no caso de um âmbito mais alargado, assegurar salvaguardas suficientes para a protecção de dados pessoais. As questões colocadas no ponto 27 acima devem de ser tidas em consideração.

Outras questões relacionadas com o âmbito

29. De acordo com o n.º 1 do artigo 2.º da proposta, a decisão-quadro aplicar-se-á ao tratamento de informação anterior à instauração de um processo. O seu âmbito é mais limitado do que a proposta de decisão-quadro relativa à protecção dos dados pessoais integralmente aplicável à cooperação judiciária em matéria penal.

30. Para a AEPD, contudo, esta limitação não restringe, por si só, o âmbito da proposta à cooperação policial. Poderia incluir também cooperação judiciária em matéria penal visto que, em alguns Estados-Membros, as autoridades judiciárias também têm competências nas investigações criminais antes da instauração de um processo. Contudo, o facto de a proposta se basear unicamente na alínea b) do n.º 1 do artigo 30.º do TUE parece indicar que apenas se aplica à cooperação policial. Uma clarificação sobre este aspecto seria bem-vinda.

31. A presente proposta visa o fornecimento de informações à Europol, ao passo que a proposta de decisão-quadro relativa à protecção de dados pessoais exclui o tratamento de dados pessoais pela Europol. A AEPD recomenda limitar o intercâmbio de informações com a Europol aos objectivos da própria Europol, tal como mencionado no artigo 2.º da Convenção Europol e respectivo anexo. Ademais, devem ser tidas em conta as regras detalhadas relativas ao intercâmbio de informações com a Europol, já constantes de vários actos do Conselho.

Não haverá novas bases de dados que contenham dados pessoais

32. O ponto de partida da proposta é de que não levará à construção de novas bases de dados que contenham dados pessoais. Para tal, o n.º 2 do artigo 2.º é claro: não implica nenhuma obrigação de recolher e armazenar informações com o único objectivo de as tornar acessíveis. Do ponto de vista da protecção dados, esse é um elemento importante e positivo da proposta. A AEPD relembra o seu parecer sobre a proposta de directiva relativa à conservação de dados tratados no contexto do fornecimento de serviços electrónicos de comunicação ([1]), no qual enfatizava que as obrigações jurídicas que geram bases de dados substanciais induzem especiais riscos para a pessoa a quem os dados dizem respeito, nomeadamente por causa dos riscos de utilização indevida.

33. Contudo:

— é importante assegurar que esta proposta não promova uma interconexão incondicional de bases de dados e, por conseguinte, uma rede de bases de dados difícil de supervisionar.

— há uma excepção ao ponto de partida acima mencionado: o artigo 10.º da proposta que estipula que os dados de índice estejam acessíveis em linha. Os dados de índice não podem conter dados pessoais ou, em todo o caso, revelar a sua existência.

Acesso directo e indirecto à informação

34. A proposta prevê o acesso directo e indirecto às informações. O artigo 9.º da proposta contempla o acesso directo em linha a informações constantes das bases de dados às quais as respectivas autoridades nacionais têm acesso directo em linha. O artigo 10.º implica um acesso indirecto. Os dados de índice sobre informações que não estão acessíveis em linha devem ser disponibilizados para efeitos de consulta em linha pelas autoridades competentes equivalentes dos outros Estados-Membros e pela Europol. Quando a consulta dos dados de índice permite obter uma correspondência, a autoridade em causa pode emitir um pedido de informações e enviá-lo à autoridade designada para obter as informações identificadas pelos dados de índice.

35. O acesso directo não gera novas bases de dados, mas requer a interoperabilidade das bases de dados dos sistemas equivalentes competentes nos Estados-Membros. Ademais, introduzirá necessariamente uma nova utilização das bases de dados já existentes ao criar facilidades para todas as autoridades competentes dos Estados-Membros que até agora tinham estado à disposição somente das autoridades nacionais competentes. O acesso directo significará automaticamente que um número crescente de pessoas terá acesso às bases de dados e envolve, portanto, um risco crescente de utilização indevida.

([1]) Parecer de 26 de Setembro de 2005 sobre a proposta de directiva do Parlamento Europeu e do Conselho relativa à conservação dos dados relacionados com a oferta de serviços de comunicações electrónicas publicamente disponíveis e que altera a Directiva 2002/58/CE (COM(2005) 438 final).

36. No caso do acesso directo por uma autoridade competente de outro Estado-Membro, as autoridades designadas do Estado–Membro de origem não deterão o controlo do acesso e da utilização posterior dos dados. Esta consequência do acesso directo, tal como prevista pela proposta, tem de ser devidamente abordada já que:

— parece invalidar os poderes das autoridades designadas de recusar o fornecimento de informações (à luz do artigo 14.º);

— levanta questões sobre a responsabilidade da exactidão e a actualização das informações, após o acesso às mesmas. Como pode uma autoridade designada do Estado-Membro de origem assegurar que os dados são actualizados?

— não é somente a autoridade designada que já não consegue cumprir com as suas obrigações relativas à legislação da protecção de dados, mas é também a autoridade nacional para a protecção de dados do Estado-Membro de origem que já não pode supervisionar o cumprimento das obrigações porque não tem competência face às autoridades de aplicação da lei de outro Estado-Membro;

— estes problemas são ainda mais predominantes no caso de acesso a bases de dados de autoridades designadas e partes designadas, que não sejam autoridades de aplicação da lei (ver pontos 25-28 do presente parecer).

Esta consequência do acesso directo é uma razão importante pela qual a adopção da presente proposta deve depender da adopção de uma decisão-quadro relativa à protecção de dados pessoais. Subsiste um problema: é difícil perceber como as autoridades designadas poderiam recusar o fornecimento de informações à luz do artigo 14.º.

37. No que diz respeito ao acesso indirecto aos dados de índice que dão informações através de um sistema sim ou não («hit/no hit»), este não é um fenómeno recente. É a base do funcionamento dos sistemas europeus de informação em larga escala, tais como o Sistema de Informação Schengen. A criação de um sistema de dados de índice tem a vantagem de permitir aos Estados-Membros de onde provêm as informações controlarem a troca de informações dos seus ficheiros policiais. Quando a consulta dos dados de índice permite obter uma correspondência, a autoridade requerente pode emitir um pedido de informações relativo aos dados da pessoa em questão. Este pedido será devidamente avaliado pela autoridade requerida.

38. Todavia, é necessária uma análise adequada porque a criação de um sistema de dados de índice — em áreas onde estes sistemas não existiam até agora, para além dos sistemas europeus de informação em larga escala — pode gerar novos riscos para a pessoa a quem dizem respeito os dados. A AEPD realça que apesar dos dados de índice não conterem muitas informações sobre a pessoa em questão, a consulta dos dados de índice pode levar a um resultado altamente sensível. Pode revelar que uma pessoa faz parte de um ficheiro policial por infracções penais.

39. Por conseguinte, é primordial que o legislador comunitário estabeleça regras adequadas, pelo menos acerca da criação dos dados de índice, acerca da gestão de sistemas de arquivos adequados dos dados de índice e acerca da organização adequada do acesso aos dados de índice. Para a AEPD, a proposta não é satisfatória relativamente a estas matérias. Na fase actual, a AEPD faz três comentários:

— A definição de dados de índice não é clara. Não é perceptível se os dados de índice são considerados meta-dados, chaves primárias ou mesmo ambos. A noção de dados de índice precisa de ser clarificada, pois tem um impacto directo no nível de protecção de dados e nas salvaguardas necessárias.

— A proposta deve clarificar o papel dos pontos de contacto nacionais no que diz respeito aos dados de índice. O envolvimento dos pontos de contacto nacionais poderia ser necessário, especialmente no caso de a interpretação dos dados de índice requerer conhecimento especializado como é, por exemplo, o caso da possível correspondência de impressões digitais.

— A proposta deixa a adopção de disposições necessárias à criação dos dados de índice sob a alçada da legislação implementada em conformidade com o procedimento de comitologia previsto no artigo 19.º. Embora sejam necessárias regras de aplicação, as regras básicas para a criação dos dados de índice devem ser incluídas na própria decisão-quadro.

Autorização prévia das autoridades judiciárias

40. A troca de informações não deverá impedir os Estados-Membros de requerer a autorização prévia das autoridades judiciárias para transmitir as informações à autoridade requerente quando essas informações se encontram sujeitas a controlo judiciário no país requerido. Isto é importante já que, segundo um estudo acerca da competência policial na troca de dados pessoais ([1]), nem em todos os Estados-Membros a polícia pode autonomamente aceder a esses dados. Para a AEPD, o princípio da disponibilidade não deve contrariar a obrigação, ao abrigo do direito nacional, de obter uma autorização prévia para a informação, ou de, pelo menos, estabelecer regras específicas no que toca às categorias de dados para as quais é preciso obter autorização prévia, aplicável em todos os Estados-Membros.

([1]) Respostas ao questionário sobre a decisão-quadro relativa à simplificação do intercâmbio de dados e informações entre as autoridades de aplicação da lei dos Estados-Membros da União Europeia, nomeadamente no que respeita a infracções graves, incluindo actos terroristas (Doc. n.º 5815/1/05 do Conselho).

41. Esta obrigação deve ser interpretada em relação com o n.º 2 do artigo 1.º da proposta de decisão-quadro relativa à protecção de dados pessoais, que também prevê que o Estado-Membro transmissor tenha uma palavra a dizer sobre a ulterior utilização dos dados no Estado-Membro ao qual os dados foram transmitidos. A AEPD regista a importância deste princípio, que é necessário para assegurar que a disponibilidade não levará a contornar legislação nacional restritiva na ulterior utilização dos dados pessoais.

Observação final

42. Estes elementos requerem altos padrões de protecção de dados. Deve ser dada especial atenção à garantia dos princípios da limitação da finalidade e tratamento posterior bem como à exactidão e à fiabilidade das informações acessíveis (ver o parecer da AEPD sobre a proposta de decisão-quadro relativa à protecção de dados pessoais, IV.2 e IV.6).

V. OUTRAS ABORDAGENS

Proposta sueca

43. A proposta sueca não se restringe a tipos específicos de informações, pois cobre todos os dados e informações, até mesmo dados e informações mantidas por outros que não as autoridades competentes para a aplicação da lei. A proposta faz progredir a cooperação estabelecendo prazos para responder aos pedidos de informação e abolindo a discriminação entre o intercâmbio num Estado-Membro e o intercâmbio de informações transfronteiras. Não prevê medidas adicionais que assegurem que as informações possam ser efectivamente acessíveis. É, por este motivo, compreensível que a Comissão não ficasse satisfeita com a proposta sueca em si, enquanto instrumento para a disponibilidade ([1]).

44. A abordagem da proposta sueca tem as seguintes implicações gerais do ponto de vista da protecção de dados:

— É positivo que a proposta se limite estritamente ao tratamento de dados existentes e não leve à criação de novas bases de dados, nem sequer aos «dados de índice».

— Contudo, a ausência de «dados de índice»não é, por definição, um elemento positivo. Se beneficiarem de segurança adequada, os dados de índice podem facilitar uma pesquisa focalizada e, por conseguinte, uma pesquisa menos invasiva de dados de natureza sensível. Pode, de igual forma, permitir uma melhor filtragem dos pedidos e uma melhor supervisão.

— De qualquer forma, a proposta leva a um aumento do intercâmbio de dados pessoais transfonteiras, apresentando riscos para a protecção de dados pessoais, designadamente porque a competência dos Estados-Membros para controlar totalmente o permutador de dados fica afectada. Não dever ser adoptada independentemente da adopção da decisão-quadro relativa à protecção de dados pessoais.

([1]) Ver o documento de trabalho dos Serviços da Comissão anexo à proposta de decisão-quadro do Conselho sobre o intercâmbio de informações com base no princípio da disponibilidade, SEC(2005) 1270 de 12.10.2005.

Convenção de Prüm

45. A Convenção de Prüm apresenta outra abordagem relativamente ao princípio da disponibilidade. Enquanto a presente proposta de decisão-quadro apresenta uma abordagem geral — não prevendo regras específicas para o intercâmbio de tipos específicos de informação, mas sendo aplicável a todos os tipos de informações que estejam enumeradas no Anexo II (ver pontos 21-28 deste parecer) –, a abordagem da Convenção de Prüm é gradual.

46. Esta abordagem é, por vezes, denominada de «abordagem campo a campo». Aplica-se a tipos específicos de informações (ADN, dados sobre impressões digitais e matrículas de veículos) e estabelece também a obrigação de ter em consideração a natureza específica dos dados. A Convenção estabelece a obrigação de criar e manter ficheiros de análises do ADN para a investigação de infracções penais. Uma obrigação idêntica é também aplicável aos dados sobre impressões digitais. Quanto aos dados sobre matrículas de veículos, o acesso directo deve ser concedido aos pontos nacionais de contacto dos Estados-Membros.

47. A abordagem da Convenção de Prüm dá azo a três tipos de observações.

48. Em primeiro lugar, é evidente que a AEPD não apoia o processo conducente a esta Convenção, à margem do quadro institucional da União Europeia, e, consequentemente, sem o envolvimento real da Comissão. Ademais, isso traduz-se na inexistência de controlo democrático por parte do Parlamento e de controlo jurisdicional por parte do Tribunal de Justiça, o que resulta em menos garantias de que todos os interesses (públicos) ficam equitativamente equilibrados. Isso inclui a perspectiva da protecção de dados, ou seja, as instituições da União Europeia não têm a oportunidade de avaliar, antes de o sistema ser estabelecido, o impacto das escolhas políticas na protecção de dados pessoais.

49. Em segundo lugar, é óbvio que alguns elementos da Convenção de Prüm são claramente mais intrusivos relativamente à pessoa em causa do que a proposta de decisão-quadro relativa à disponibilidade. A Convenção conduz necessariamente à criação de novas bases de dados, o que, por si só, põe em causa a protecção de dados pessoais. Deve ser demonstrada a necessidade e a proporcionalidade da criação de novas bases de dados. Devem ser estabelecidas as salvaguardas necessárias à protecção de dados pessoais.

Uma «abordagem campo a campo»

50. Em terceiro lugar, tal como referido anteriormente, a Convenção segue uma «abordagem campo a campo». A AEPD já mencionou acima as dificuldades e incertezas relacionadas com o ambiente no qual o princípio da disponibilidade tem de ser aplicado. Nestas circunstâncias, é preferível, no entender da AEPD, não configurar um sistema para uma gama de dados, mas começar antes com uma abordagem mais cautelosa que envolva um tipo de dados e verificar em que medida o princípio da disponibilidade apoia efectivamente a acção policial, bem como os riscos específicos relativamente à protecção de dados pessoais. Com base nestas experiências, o sistema poderia eventualmente ser alargado a outros tipos de dados e/ou modificado a fim de ser mais eficaz.

51. Esta «abordagem campo a campo» preencheria também melhor os requisitos do princípio da proporcionalidade. Segundo a AEPD, a necessidade de um melhor intercâmbio de informações transfronteiras em matéria de aplicação da lei poderia justificar a adopção de um instrumento jurídico a nível da UE, mas, para ser proporcional, o instrumento deverá ser pertinente de maneira a conseguir o seu objectivo, que pode ser mais adequadamente estabelecido após um período com experiências práticas. Além disso, o instrumento não deverá prejudicar desproporcionalmente a pessoa em causa. O intercâmbio não deve relacionar mais tipos de dados do que os estritamente necessários, com a possibilidade de um intercâmbio anónimo de dados, devendo ocorrer sob condições rigorosas de protecção de dados.

52. Ademais, uma abordagem mais cautelosa como a defendida pela AEPD poderia — possivelmente adicionada à «abordagem campo a campo» — incluir o início da implementação do princípio da disponibilidade somente sob a forma de acesso indirecto, através dos dados de índice. A AEPD menciona este aspecto como um ponto a ser considerado na continuação do processo legislativo.

VI. **QUAIS DADOS?**

53. O Anexo II enumera os tipos de informações que podem ser obtidas nos termos da decisão-quadro ora proposta. Todos os seis tipos de informações aí enumerados são na maioria das vezes dados pessoais, porque todos estão relacionados com uma pessoa identificada ou identificável.

54. À luz da alínea g) do artigo 3.º da proposta, dados de índice são «os dados que servem para identificar claramente as informações e que podem ser consultados mediante uma pesquisa de rotina para saber se as informações estão ou não disponíveis». Na «Abordagem para a aplicação do princípio da disponibilidade» [1], os seguintes dados são classificados como dados de índice:

— a identificação das pessoas em causa;

— um número de identificação para os objectos em causa (veículos/documentos);

— impressões digitais/fotografias digitais.

Outro tipo de dados que poderiam ser considerados dados de índice seriam os perfis de ADN. Esta lista de dados de índice revela que os dados de índice podem conter dados pessoais e, por conseguinte, é necessária uma protecção adequada.

55. A AEPD trata especificamente da questão dos perfis de ADN. A análise do ADN tem provado representar um valor significativo para a investigação criminal e o intercâmbio eficaz de dados ADN pode ser essencial na luta contra o terrorismo. Contudo, é essencial que o conceito de dados ADN seja claramente definido e que as características destes dados sejam devidamente tomadas em consideração. De facto, do ponto de vista da protecção dos dados pessoais, existe uma grande diferença entre as amostras de ADN e perfis de ADN.

56. As amostras de ADN (frequentemente recolhidas e registadas pelas autoridades de aplicação da lei) devem ser consideradas especialmente sensíveis, uma vez que é mais provável que tenham a «imagem» completa do ADN. Podem fornecer informações acerca das características genéticas e do estado de saúde da pessoa, podendo ser pedidas por motivos totalmente diferentes tais como aconselhamento médico a pessoas ou casais jovens.

57. Pelo contrário, os perfis de ADN só contêm algumas informações parciais de ADN extraídas das amostras de ADN: podem ser usadas para verificar a identidade da pessoa, mas em princípio não revelam as características genéticas da pessoa. Não obstante, o progresso da ciência pode fazer aumentar as informações que podem ser reveladas pelos perfis de ADN e, por conseguinte, o que é considerado um perfil de ADN «inocente», numa dada altura, pode, numa fase posterior, revelar muito mais informações do que o esperado e necessário, e, em especial, informações relativas às características genéticas de um pessoa. A informação que pode ser revelada pelos perfis de ADN deve, por isso, ser considerada dinâmica.

58. Nesta perspectiva, a AEPD observa que tanto a Convenção de Prüm como a proposta da Comissão promovem o intercâmbio de dados do ADN entre os serviços de aplicação da lei, mas há diferenças substanciais na maneira como o fazem.

[1] Documento da Presidência para o Conselho, de 5 de Abril de 2005 (Doc. n.º 7641/05).

59. A AEPD congratula-se com o facto de a proposta da Comissão não estabelecer nenhuma obrigação de recolher dados ADN e de limitar claramente o intercâmbio de dados ADN aos perfis de ADN. O Anexo II define os perfis de ADN por intermédio de uma lista inicial comum dos marcadores ADN utilizados nas análises de ADN para fins judiciais nos Estados-Membros. Com base nos sete marcadores ADN da série normalizada europeia, tal como define o Anexo I na Resolução do Conselho de 25 de Junho de 2001 relativa ao intercâmbio de resultados de análises de ADN ([1]), esta lista garante que os perfis de ADN não conterão, quando forem obtidos, nenhumas informações sobre as características hereditárias específicas.

60. A AEPD sublinha que a referida Resolução do Conselho estabelece algumas salvaguardas muito importantes, que estão especificamente relacionadas com a natureza dinâmica dos perfis de ADN. De facto, a secção III da Resolução, após limitar os resultados do intercâmbio de análises de ADN às «zonas do cromossoma […] que, ao que se sabe, não contenham informação sobre características hereditárias específicas», recomenda ainda aos Estados-Membros que não usem os marcadores ADN que, devido a avanços na ciência, possam fornecer informações sobre as características hereditárias específicas.

61. A Convenção de Prüm apresenta uma abordagem diferente, pois obriga as partes contratantes a abrir e manter ficheiros de análises de ADN para a investigação de infracções penais. Por conseguinte, este facto resulta na criação de novas bases de dados ADN e numa crescente recolha de dados ADN. Ademais, não é claro que tipos de dados são incluídos nos «ficheiros de análises de ADN» e a Convenção não tem em consideração a evolução dinâmica dos perfis de ADN.

62. A AEPD realça que qualquer instrumento jurídico que estabeleça o intercâmbio dos dados ADN deve:

— limitar e definir claramente o tipo de informações ADN que podem ser intercambiadas (também relativamente à diferença fundamental entre amostras de ADN e perfis de ADN);

— definir normas técnicas comuns com vista a evitar que as variações nas práticas nas bases de dados ADN para fins judiciais possam levar a dificuldades e resultados imprecisos no intercâmbio de informações;

— estabelecer salvaguardas juridicamente vinculativas adequadas com o propósito de evitar que os avanços da ciência resultem na obtenção de dados pessoais, que não são apenas sensíveis mas também desnecessários para a finalidade que foram recolhidos, a partir dos perfis de ADN.

([1]) JO C 187, p. 1.

63. Nesta perspectiva, a AEPD confirma e integra aqui as observações já feitas no seu parecer sobre a decisão-quadro do Conselho relativa à protecção de dados pessoais (ponto 80). Nesse parecer, a AEPD sublinhou, relativamente aos dados ADN, que deviam ser previstas garantias específicas para garantir que a informação disponível só possa ser usada na prevenção, detecção ou investigação de infracções penais, que o nível de exactidão dos perfis de ADN seja cuidadosamente tido em conta e possa ser contestado pela pessoa em causa através de meios prontamente disponíveis e que o respeito pela dignidade das pessoas seja plenamente assegurado ([2]).

64. Estas considerações levam também à conclusão de que a legislação sobre a criação de ficheiros de ADN e o intercâmbio de dados desses ficheiros só deve ser adoptada após uma avaliação de impacto, na qual se possam ter avaliado devidamente os riscos e os benefícios. A AEPD recomenda que esta legislação estipule a avaliação regular após a sua entrada em vigor.

65. Finalmente, o Anexo II inclui outros tipos de informações que podem ser intercambiadas. Inclui informações provenientes de entidades privadas, dado que os números de telefone e outros dados de comunicação, bem como os dados de tráfego das comunicações, provêem normalmente de operadores telefónicos. A exposição de motivos confirma que os Estados-Membros são obrigados a assegurar que as informações relevantes em matéria de aplicação da lei controladas por autoridades ou entidades privadas designadas para este efeito sejam partilhadas com as autoridades competentes equivalentes dos outros Estados-Membros e com a Europol. Visto que a proposta se aplica a dados pessoais provenientes de entidades privadas, o quadro jurídico aplicável deve, segundo a AEPD, conter garantias adicionais que visam a protecção da pessoa em causa por forma a assegurar a exactidão da informação.

VII. **PRINCÍPIOS DA PROTECÇÃO DE DADOS**

66. Se bem que as regras relativas à protecção de dados pessoais não são especificamente estabelecidas na proposta de decisão-quadro do Conselho, noutros instrumentos, como a Convenção de Prüm ou a proposta sueca, existem algumas disposições legais específicas aplicáveis em matéria de protecção de dados. A falta de regras específicas sobre a protecção de dados pessoais na proposta de disponibilidade só é aceitável na medida em que as regras gerais constantes da proposta de decisão-quadro relativas à protecção de dados no âmbito do terceiro pilar forem inteiramente aplicáveis e prevejam uma protecção suficiente. Ademais, as regras relativas à protecção de dados pessoais estabelecidas em instrumentos específicos — como a proposta sueca e a Convenção de Prüm — não devem baixar o nível de protecção garantido pelo quadro geral. A AEPD recomenda o aditamento de uma cláusula específica sobre os conflitos possíveis entre as diferentes regras relativas à protecção de dados.

([2]) Na mesma ordem de ideias, cf. igualmente «Relatório Intercalar sobre a Aplicação dos Princípios da Convenção 108 à Recolha e Tratamento de Dados Biométricos» do Conselho da Europa, de Fevereiro de 2005.

67. Neste ponto, a AEPD gostaria de realçar novamente, recordando o seu parecer sobre o projecto de decisão-quadro relativa à protecção de dados pessoais, a importância de ver aplicadas, a todo o tratamento, regras consistentes e globais relativas à protecção de dados, no âmbito da cooperação policial. Além disso, a AEPD reitera os outros aspectos focados nesse parecer. No presente parágrafo, salientam-se as seguintes questões relativas à protecção de dados:

— Tratamento legal de dados pessoais. A AEPD apoia a abordagem de que a informação possa estar disponível somente no caso de ter sido recolhida legalmente (tal como previsto no n.º 2 do artigo 2.º relativamente às informações recolhidas por meio de medidas coercivas). O tratamento legal de dados pessoais garantiria que as informações disponibilizadas e intercambiadas pudessem também ser usadas devidamente numa acção judicial. Efectivamente, apesar das informações tratadas após a instauração de um processo não se inscreverem no âmbito de aplicação do instrumento proposto, ainda é provável que as informações trocadas anteriormente pelas autoridades de aplicação da lei acabem num processo criminal.

— A qualidade dos dados pessoais tem importância específica, já que o princípio da disponibilidade propicia que as informações sejam usadas pelas autoridades de aplicação da lei a operar fora do contexto no qual os dados foram recolhidos. Estas autoridades têm mesmo acesso directo às bases de dados de outros Estados-Membros. A qualidade dos dados pessoais só pode ser garantida se a sua exactidão for devida e adequadamente verificada, se as informações forem diferenciadas de acordo com as diferentes categorias de pessoas envolvidas (vítimas, suspeitos, testemunhas, etc.) e se, quando necessário, o grau de exactidão estiver indicado (ver parecer da AEPD relativa à protecção de dados pessoais, IV.6).

Estes pontos deixam, mais uma vez, clara a razão pela qual as regras sobre a protecção de dados e, nomeadamente, as regras sobre a exactidão, devem ser aplicáveis a todos os tipos de tratamento, inclusive a nível nacional. Caso contrário, os dados pessoais que estão directamente acessíveis poderiam ser incorrectos, fora de prazo e assim afectar tanto os direitos da pessoa em causa como a eficácia das investigações.

— Limitação da finalidade. De acordo com o princípio da disponibilidade, as autoridades competentes equivalentes dos outros Estados-Membros podem ter acesso aos dados pessoais. Contudo, as competências das autoridades de aplicação da lei podem diferir substancialmente de país para país. É, por isso, essencial garantir que o princípio básico de limitação da finalidade seja respeitado, apesar dos diferentes alcances das competências das diversas autoridades competentes que trocam os dados. As informações recolhidas e tratadas por uma determinada autoridade com um determinado objectivo não podem ser posteriormente usadas para um outro fim por força de competências diferentes, talvez mais alargadas, das autoridades receptoras.

Por conseguinte, a AEPD congratula-se com o artigo 7.º da decisão-quadro proposta, que deve ser lido enquanto especificação das regras gerais estabelecidas na decisão-quadro proposta relativa à protecção de dados pessoais. Ademais, a AEPD regista que a avaliação da equivalência entre autoridades diferentes (que na proposta actual é remetida para o procedimento de comitologia) deve ser efectuada cuidadosamente e com o devido respeito pelo princípio de limitação da finalidade.

— Os limites temporais para armazenar as informações intercambiadas devem também ser vistos à luz do princípio de limitação da finalidade: as informações acessíveis ou intercambiadas com uma finalidade devem ser apagadas assim que já não forem necessárias para esse efeito. Proceder assim evitaria duplicações de bases de dados desnecessárias, permitindo, contudo, às autoridades acederem novamente à informação disponibilizada (actualizada), caso ela seja necessária para alguma finalidade legítima.

— Registo das informações transmitidas de acordo com o princípio da disponibilidade. O registo deve ocorrer em ambos os lados, tanto no Estado-Membro requerido como no requerente. Devem manter-se não só registos de acesso, mas também registos de intercâmbios (ver parecer da AEPD relativo à protecção de dados pessoais, ponto 133), de maneira a garantir que as autoridades nacionais competentes confiem umas nas outras e não percam por completo o controlo da informação disponibilizada. A necessidade da rastreabilidade da informação também implica a possibilidade de actualizar e/ou corrigir as informações.

— Direitos das pessoas a quem os dados dizem respeito. Os sistemas de intercâmbio de informações entre as autoridades da UE responsáveis pela aplicação da lei aumentam as situações em que os dados pessoais são (temporariamente) tratados pelas autoridades competentes em Estados-Membros diferentes. Isto significa, por um lado, que devem ser criadas normas comuns a nível da UE em matéria dos direitos da pessoa a quem os dados dizem respeito e, por outro lado, as pessoas a quem os dados dizem respeito devem poder exercer os seus direitos, na medida do permitido pelas regras em matéria de protecção dos dados no quadro do terceiro pilar, tanto em relação às autoridades que disponibilizam os dados como em relação às autoridades que acedem e tratam esses dados.

— Supervisão. A AEPD sublinha que, conforme o caso, mais do que uma autoridade nacional de controlo pode ser competente para controlar o tratamento de dados pessoais efectuado com base nas propostas actuais. A este respeito, o acesso directo em linha a informações policiais exige uma supervisão e coordenação reforçadas por parte das autoridades nacionais competentes para a protecção de dados.

VIII. CONCLUSÕES

Conclusões gerais relacionadas com o princípio da disponibilidade

68. A AEPD aproveita a ocasião para apresentar, neste parecer, alguns pontos de vista gerais e mais fundamentais relativamente ao intercâmbio de informações em matéria de aplicação da lei e às abordagens tendo em vista a regulamentação desta matéria. A AEPD estará disponível para uma nova consulta, numa fase posterior, no seguimento de progressos no processo legislativo relativo a esta proposta ou de outras propostas relacionadas com ela.

69. Para a AEPD, o princípio da disponibilidade deve ser aplicado sob a forma de um acto jurídico vinculativo através de uma abordagem mais prudente e gradual que envolva um tipo de dados e para controlar em que medida o princípio da disponibilidade pode efectivamente apoiar a aplicação da lei, bem como os riscos específicos para a protecção dos dados pessoais. Esta abordagem mais prudente poderia consistir em começar com a aplicação do princípio da disponibilidade somente através do acesso indirecto, através dos dados de índice. Com base nestas experiências, o sistema poderia eventualmente ser alargado a outros tipos de dados e/ou modificado de maneira a ser mais eficaz.

70. Não deve ser adoptado nenhum instrumento jurídico que aplique o princípio da disponibilidade sem a adopção prévia de garantias essenciais relativas à protecção de dados, tal como previsto na proposta de decisão-quadro relativa à protecção de dados pessoais.

Recomendações destinadas a modificar a presente proposta

71. A AEPD recomenda a clarificação do âmbito do princípio da disponibilidade da seguinte maneira:

— Aditar uma definição clara e precisa dos dados que serão considerados disponíveis.

— Como primeira opção, limitar o âmbito do princípio da disponibilidade à informação controlada pelas autoridades competentes.

— Como segunda opção, no caso de um âmbito mais alargado, garantir as salvaguardas necessárias para a protecção de dados pessoais. As questões levantadas no ponto 27 deste parecer devem ser tomadas em consideração.

72. A AEPD faz as seguintes observações relativamente ao acesso directo às bases de dados por parte de uma autoridade competente de outro Estado-Membro:

— O assunto tem de ser devidamente abordado já que, no caso do acesso directo, as autoridades designadas do Estado-Membro de origem não têm controlo sobre o acesso e a utilização posterior dos dados.

— A proposta não pode promover uma interconexão incondicional das bases de dados e, deste modo, uma rede de bases de dados que será difícil de supervisionar.

73. A decisão-quadro deve ser mais precisa quanto à criação de um sistema de dados de índice. Mais especificamente:

— A proposta deve, pelo menos, prever regras adequadas sobre a criação dos dados de índice, sobre a gestão de ficheiros de dados de índice e sobre a organização adequada do acesso aos dados de índice.

— A definição de dados de índice precisa de ser clarificada.

— A proposta deve clarificar o papel dos pontos de contacto nacionais no que diz respeito aos dados de índice.

— As regras básicas para a criação dos dados de índice devem ser incluídas na própria decisão-quadro e não deixadas a cargo de disposições de aplicação nos termos do procedimento de comitologia.

74. A AEPD assinala que a proposta de decisão, na medida em que estabelece o intercâmbio dos dados ADN, deve:

— limitar e definir claramente o tipo de informações ADN que podem ser intercambiadas (também relativamente à diferença fundamental entre amostras de ADN e perfis de ADN);

— definir normas técnicas comuns com vista a evitar que as variações nas práticas nas bases de dados ADN para fins judiciais possam levar a dificuldades e resultados imprecisos no intercâmbio de informações;

— estabelecer salvaguardas juridicamente vinculativas e adequadas com o propósito de evitar que os avanços da ciência resultem na obtenção de dados pessoais, que não são apenas sensíveis mas também desnecessários para a finalidade com que foram recolhidos, a partir dos perfis de ADN;

— só ser adoptada depois de uma avaliação de impacto.

75. A AEPD aconselha limitar o intercâmbio de informações com a Europol aos fins da própria Europol, tal como previsto no artigo 2.º da Convenção Europol e respectivo anexo.

Feito em Bruxelas, em 28 de Fevereiro de 2006.

Peter HUSTINX

Autoridade Europeia para a Protecção de Dados