AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS

Parecer da Autoridade Europeia para a Protecção de Dados sobre:

— a proposta de decisão do Conselho relativa ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen de segunda geração (SIS II) (COM(2005)230 final);

— a proposta de regulamento do Conselho e do Parlamento Europeu relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen de segunda geração (SIS II) (COM (2005) 236 final) e

— a proposta de regulamento do Parlamento Europeu e do Conselho relativo ao acesso ao Sistema de Informação de Schengen de segunda geração (SIS II) dos serviços dos Estados-Membros competentes para a emissão de certificados de matrícula dos veículos (COM(2005) 237 final)

(2006/C 91/11)

A AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS,

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

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

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

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

Tendo em conta o pedido de parecer apresentado pela Comissão nos termos do n.º 2 do artigo 28.º do Regulamento (CE) n.º 45/2001, recebido em 17 de Junho de 2005.

APROVOU O SEGUINTE PARECER:

1. INTRODUÇÃO

1.1. Antecedentes

O Sistema de Informação de Schengen (SIS) é um sistema informático à escala da UE que foi criado para compensar a supressão dos controlos nas fronteiras internas no interior do espaço Schengen. O SIS permite às autoridades competentes dos Estados-Membros a troca de informações para efeitos do controlo de pessoas e objectos nas fronteiras externas ou no interior do território, bem como para efeitos de emissão de vistos e autorizações de residência.

A Convenção Schengen entrou em vigor em 1995 como acordo intergovernamental. O SIS, enquanto parte da Convenção Schengen, foi posteriormente integrado no âmbito da UE pelo Tratado de Amesterdão.

O actual sistema será substituído por um novo Sistema de Informação Schengen II de «segunda geração», permitindo deste modo o alargamento do espaço Schengen aos novos Estados-Membros da UE. Este novo sistema possuirá também novas funcionalidades. As disposições de Schengen, que foram elaboradas num quadro intergovernamental, serão integralmente transpostas para instrumentos jurídicos europeus clássicos.

Em 1 de Junho de 2005, a Comissão Europeia apresentou três propostas relativas à criação do SIS II, nomeadamente:

— uma proposta de regulamento baseado no Título IV do Tratado CE (vistos, asilo, imigração e outras políticas relacionadas com a livre circulação de pessoas) relativo aos aspectos do primeiro pilar (imigração) do SIS II, a seguir designada «a proposta de regulamento»;

— uma proposta de decisão baseada no Título VI do Tratado CE (cooperação policial e judiciária em matéria penal) relativa à utilização do SIS para fins do terceiro pilar, a seguir designada «a proposta de decisão»;

— uma proposta de regulamento baseada no Título V (transportes) relativo especificamente ao acesso aos dados do SIS pelos serviços competentes para o registo de veículos; esta proposta será abordada separadamente (ver ponto 4.6 infra).

Convém lembrar a este propósito que a Comissão apresentará nos próximos meses uma comunicação sobre a interoperabilidade e maior sinergia entre os sistemas de informação da UE (SIS, VIS e Eurodac).

O SIS II é composto por uma base de dados central denominada «Sistema Central de Informação de Schengen» (CS-SIS) cuja gestão operacional será assegurada pela Comissão em ligação com os pontos de acesso nacionais determinados por cada Estado-Membro (NI-SIS). Os gabinetes SIRENE asseguram o intercâmbio de todas as informações suplementares (informações relacionadas com indicações SIS II, mas não armazenadas neste sistema).

Os Estados-Membros fornecem dados ao SIS II sobre pessoas procuradas para efeitos de detenção, entrega ou extradição, pessoas procuradas no âmbito de processos judiciais, pessoas que devem ser colocadas sob vigilância ou sujeitas a controlos específicos, pessoas a quem deve ser recusada a entrada nas fronteiras externas e sobre objectos perdidos ou roubados. Um conjunto de dados designados «indicações» introduzidas no SIS permite às autoridades competentes identificar pessoas ou objectos.

O SIS II apresenta novas características: acesso alargado ao SIS (Europol, Eurojust, procuradores públicos nacionais, serviços competentes para a emissão de certificados de matrícula de veículos), ligações a indicações, aditamento de novas categorias de dados, nomeadamente dados biométricos (impressões digitais e fotografias), bem como uma plataforma técnica a partilhar com o Sistema de Informação sobre Vistos. Estes acrescentos têm alimentado os debates durante anos sobre a mudança da finalidade do SIS que passaria de um instrumento de controlo para um sistema de informação e investigação.

1.2. **Avaliação genérica das propostas**

1. A AEPD congratula-se com o facto de ser consultado com base no n.º 2 do artigo 28.º do Regulamento (CE) n.º 45/2001. Todavia, dado o carácter obrigatório desta disposição, o presente parecer deve ser mencionado no preâmbulo dos textos.

2. A AEPD congratula-se com as propostas por diversas razões. A transformação de uma estrutura intergovernamental em instrumentos jurídicos europeus encerra várias consequências positivas. o valor jurídico das regras relativas ao SIS será tornado mais claro; o Tribunal de Justiça passará a ser competente para interpretar o instrumento do primeiro pilar; será assegurada a participação, pelo menos parcial, do Parlamento Europeu (embora numa fase algo tardia do processo).

3. Além disso, quanto à substância, uma parte significativa das propostas é dedicada à protecção dos dados, o que traz algumas melhorias bem-vindas comparado com a situação actual. Refiram-se a título de exemplo as medidas a favor das vítimas de usurpação de identidade, o alargamento do Regulamento (CE) n.º 45/2004 às actividades de tratamento pela Comissão no âmbito do Título VI, uma melhor definição dos motivos que levam à introdução de indicações de indivíduos para efeitos de não admissão.

4. Por outro lado, é evidente o grande cuidado que foi posto na elaboração das propostas que são complexas devido à complexidade intrínseca do sistema que regem. A maioria dos comentários do presente parecer destinam-se a esclarecer ou completar disposições, mas não implicam uma reformulação total.

Todavia, não obstante esta apreciação globalmente positiva, podem ser formuladas algumas reservas, nomeadamente as que se seguem:

1. É, em muitos casos, difícil descortinar a intenção subjacente ao texto; a ausência de memorando justificado é altamente lamentável. Dada a natureza extremamente complexa destes documentos, essa teria sido uma exigência básica. Nalguns casos, a sua falta não deixa ao leitor outra alternativa senão recorrer a conjecturas.

2. Por outro lado, é lamentável que não tenha sido efectuado nenhum estudo de impacto. O facto de a primeira versão do sistema já estar a funcionar não serve de justificação dadas as diferenças consideráveis entre os dois sistemas. Em especial, o impacto da introdução de dados biométricos deveria ter sido objecto de reflexão mais aprofundada.

3. O quadro jurídico da protecção de dados é muito complexo já que se baseia na aplicação combinada da *lex generalis* e da *lex specialis*. Importa assegurar que, mesmo quando se está a desenvolver legislação específica, o quadro de protecção de dados existente na Directiva 95/46/CE e no Regulamento (CE) n.º 45/2001 continue aplicável na íntegra. A aplicação combinada de vários instrumentos jurídicos não deve dar origem a discrepâncias entre regimes nacionais no que diz respeito a aspectos fundamentais nem diminuir o actual nível de protecção de dados.

4. O acesso por muitas novas autoridades que não visam a finalidade primeira do «controlos de pessoas e objectos» deve ser acompanhado de salvaguardas mais rigorosas.

5. As propostas baseiam-se, em grande medida, noutros instrumentos jurídicos que ainda estão em fase de elaboração (alguns ainda nem sequer foram propostos). A AEPD está consciente das dificuldades intrínsecas da actividade legislativa num ambiente complexo e em constante mutação. Todavia, tendo em conta as consequência para os interessados e a incerteza jurídica daí decorrente, considera que tal não é aceitável.

6. Verifica-se uma certa confusão na repartição das competências entre Estados-Membros e a Comissão. Ora, a clareza não só é indispensável para o bom funcionamento do sistema como também é uma condição básica para assegurar um controlo abrangente do sistema.

1.3. **Estrutura do parecer**

O presente parecer é estruturado em torno dos seguintes eixos: começa por clarificar o quadro jurídico aplicável ao SIS II. A seguir, aborda a definição da finalidade do SIS II e os elementos que diferem significativamente do actual sistema. O ponto 5 contém comentários sobre os papéis respectivos da Comissão e dos Estados-Membros no âmbito do funcionamento do SIS II. O ponto 6 versa sobre os direitos dos interessados ao passo que o ponto 7 trata do controlo, a nível nacional e da AEPD, bem como da cooperação entre autoridades de protecção de dados. O ponto 8 propõe alguns comentários e possíveis alterações que se prendem com a segurança; os pontos 9 e 10 abordam respectivamente a comitologia e a interoperabilidade. Por último, as principais conclusões relativas a cada um desses pontos são sublinhadas num resumo.

2. QUADRO JURÍDICO APLICÁVEL

2.1. Quadro jurídico do SIS II aplicável em matéria de protecção de dados

As propostas referem como quadro jurídico para a protecção de dados a Directiva 95/46/CE, a Convenção 108 e o Regulamento n.º 45/2001. São igualmente importantes outros instrumentos.

A fim de esclarecer este contexto e de recordar os principais pontos de referência da nossa análise, convém enumerar os seguintes pontos:

— O respeito pela vida privada é garantido na Europa desde a adopção em 1950 da Convenção para a Protecção dos Direitos do Homem e das Liberdades Fundamentais (a seguir designada «CEDH») do Conselho da Europa. O artigo 8.º da CEDH estipula o «direito ao respeito pela vida privada e familiar».

  De acordo com o n.º 2 do artigo 8.º não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver «prevista na lei» e constituir uma providência que, numa «sociedade democrática, seja necessária» para a protecção de interesses importantes. Na jurisprudência do Tribunal Europeu dos Direitos do Homem, estas condições conduziram à requisitos suplementares relativas à qualidade da base jurídica para a ingerência, a proporcionalidade das medidas e à necessidade de salvaguardas adequadas contra abusos.

— O direito ao respeito pela vida privada e a protecção dos dados pessoais foram mais recentemente consignados nos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia. Nos termos do artigo 52.º da Carta reconhece-se que estes direitos podem estar sujeitos a restrições desde que estejam preenchidas condições correspondentes às do artigo 8.º da CEDH.

— O n.º 2 do artigo 6.º do Tratado UE prevê que a União respeitará os direitos fundamentais tal como os garante a CEDH.

Os três textos que se aplicam explicitamente ao SIS II são os seguintes:

— A Convenção n.º 108 do Conselho da Europa para a protecção das pessoas no tratamento informatizado de dados de carácter pessoal, de 28 de Janeiro de 1981 (a seguir designada a «*Convenção 108*») desenvolveu princípios básicos da protecção das pessoas singulares no que respeita ao tratamento de dados pessoais. Todos os Estados-Membros ratificaram esta Convenção que se aplica igualmente às actividades desenvolvidas nos domínios policial e judiciário. A Convenção 108 constitui actualmente o regime de protecção de dados aplicável à Convenção SIS, juntamente com a Recomendação R(87) 15 do Comité dos Ministros do Conselho da Europa, de 17 de Setembro de 1987, relativa à utilização de dados pessoais pela polícia.

— 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 (JO L 281, p. 31), a seguir designada «*Directiva 95/46/CE*». Convém recordar que, na maior parte dos Estados-Membros, a legislação nacional que transpõe esta directiva abrange igualmente actividades de tratamento desenvolvidas no domínio da polícia e da justiça.

— 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, a seguir designado «*Regulamento (CE) n.º45/2001/CE*».

A interpretação da Directiva 95/46/CE e do Regulamento (CE) n.º 45/2001 deve assentar em parte na jurisprudência do Tribunal Europeu dos Direitos Humanos na matéria nos termos da Convenção para a Protecção dos Direitos do Homem e das Liberdades Fundamentais (CEDH). Por outras palavras, a directiva e o regulamento devem ser interpretados à luz dos direitos fundamentais na medida em que dizem respeito ao tratamento de dados pessoais susceptível de violar as liberdades fundamentais, nomeadamente o direito à vida privada. A jurisprudência do Tribunal de Justiça Europeu aponta igualmente nesse sentido ([1]).

([1]) Refira-se neste contexto o acórdão proferido pelo Tribunal de Justiça no processo Österreichischer Rundfunk e outros (Processos Apensos C-465/00, C-138/01 e C-139/01, Acórdão de 20 de Maio de 2003, Tribunal Pleno, (2003) Col. I-4989). O Tribunal debruçou-se sobre uma lei austríaca que prevê a transferência de dados sobre vencimentos de funcionários públicos ao Tribunal de Contas austríaco e à sua subsequente publicação. No seu acórdão, o Tribunal estabelece uma série de critérios inspirados no artigo 8.º da Convenção para a Protecção dos Direitos do Homem que devem ser utilizados para efeitos de aplicação da Directiva 94/46/CE na medida em que esta directiva permite certas restrições do direito à vida privada.

Em 4 de Outubro de 2005, a Comissão apresentou uma proposta de decisão-quadro do Conselho relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal [1] (a seguir designada a «*proposta de decisão-quadro*»). Esta decisão-quadro destina-se a substituir a Convenção 108 como legislação de referência da proposta de decisão SIS II que terá certamente repercussões sobre o regime de protecção de dados neste contexto (ver ponto 2.2.5 infra).

2.2. **Regime jurídico de protecção de dados do SIS II**

2.2.1. *Observação geral*

A base jurídica necessária para o SIS II é constituída por quatro instrumentos separados. Todavia, como se refere nos considerandos, este facto «não afecta o princípio de que o SIS II constitui um sistema de informação único e de que deve funcionar como tal. Certas disposições destes instrumentos devem, por isso, ser idênticas.»

A estrutura dos dois documentos é fundamentalmente semelhante, sendo o texto dos Capítulos I a III praticamente idêntico. O facto de o SIS II constituir um sistema de informação único com duas bases jurídicas diferentes reflecte-se igualmente no regime bastante complexo de protecção de dados.

Este regime encontra-se em parte definido nas próprias propostas a «*lex specialis*» é completada por uma legislação de referência («*lex generalis*») diferente consoante o sector (Comissão, Estados-Membros no primeiro pilar e Estados-Membros no terceiro pilar).

Esta estrutura levanta a questão de saber como lidar com conjuntos de regras específicas na sua relação com a lei geral. No caso em apreço, a AEPD considera que a regra específica aplica a regra genérica. Por conseguinte, a *lex specialis* deve estar sempre em conformidade com a *lex generalis*, que desenvolve (especifica ou completa), mas não é concebida como excepção a esta última.

Quanto à questão da regra aplicável em casos específicos, aplica-se o princípio de que a *lex specialis* tem prioridade, mas quando esta for omissa ou pouco clara, impõe-se o recurso à *lex generalis*.

De acordo com esta estrutura, existem três combinações diferentes de *lex generalis* e *lex specialis* que podem ser resumidas do seguinte modo.

2.2.2. *Regime aplicável à Comissão*

Sempre que está envolvida a Comissão, aplica-se o Regulamento n.º 45/2001, incluindo o papel da AEPD, quer se trate actividades desenvolvidas no âmbito do primeiro (proposta de regulamento) ou do terceiro pilar (proposta de decisão). O considerando (21) da proposta de decisão afirma: «O Regulamento (CE) n.º 45/2001 (…) é aplicável ao tratamento de dados pessoais pela Comissão quando este tratamento é realizado para o exercício de actividades que se inscrevem, total ou parcialmente, no âmbito de aplicação do direito comunitário. Uma parte do tratamento de dados pessoais no SIS II inscreve-se no âmbito do direito comunitário.»

As razões são de ordem prática: com efeito, seria extremamente difícil determinar, no que diz respeito à Comissão, se os dados são tratados no âmbito de actividades abrangidas pela legislação do primeiro ou do terceiro pilar.

Além disso, aplicar um único instrumento jurídico a todas as actividades desenvolvidas pela Comissão no contexto do SIS II não só é mais razoável do ponto de vista prático como também aumenta a coerência (assegurando, de acordo com o considerando (21) uma «aplicação sistemática e uniforme das regras relativas à protecção das liberdades e dos direitos fundamentais das pessoas no que respeita ao tratamento de dados pessoais.») Por conseguinte, a AEPD congratula-se com o reconhecimento pela Comissão de que o Regulamento n.º 45/2001 é aplicável a todas as actividades de tratamento de dados por esta Instituição no âmbito do SIS II.

2.2.3. *Regime aplicável aos Estados-Membros*

A situação dos Estados-Membros é mais complexa. O tratamento de dados pessoais em aplicação da proposta de regulamento rege-se pelo próprio regulamento, bem como pela Directiva 95/46/CE. Da leitura do considerando (14) da proposta de regulamento ressalta claramente que a directiva deve ser considerada como «*lex generalis*» ao passo que o Regulamento SIS II tem a função de *lex specialis*. As consequências são diversas e serão enumeradas a seguir.

Quanto à proposta de decisão, o instrumento jurídico de referência para a protecção de dados (*lex generalis*) é a Convenção 108, o que nalguns pontos pode explicar diferenças significativas entre os regimes de protecção de dados no âmbito dos primeiro e terceiro pilares.

2.2.4. *Impacto sobre o nível da protecção de dados*

A título de comentário geral sobre esta arquitectura da protecção de dados, a AEPD sublinha o seguinte:

— A aplicação da proposta de regulamento enquanto *lex specialis* da Directiva 95/46/CE (e por analogia, da proposta de decisão como *lex specialis* da Convenção 108) nunca deverá conduzir a uma diminuição do nível da protecção de dados assegurado pela directiva ou pela convenção. A AEPD formulará recomendações para o efeito (ver por exemplo o direito de recurso).

[1] COM (2005) 475 final).

— Do mesmo modo, a aplicação combinada de instrumentos jurídicos não pode resultar numa diminuição do nível de protecção de dados assegurado ao abrigo da actual Convenção de Schengen (ver por exemplo as observações que se seguem sobre o artigo 13.º da Directiva 95/46/CE).

— A aplicação de dois instrumentos diferentes, por necessária que seja devido ao quadro legislativo europeu, não deve conduzir a discrepâncias injustificadas entre a protecção das pessoas indivíduos em causa em função do tipo de dados tratados a seu respeito. Tal deve ser evitado tanto quanto possível. As recomendações que se seguem procuram aumentar a coerência na medida do possível (ver por exemplo os poderes das autoridades de controlo nacionais).

— O quadro legislativo é de tal modo complexo que poderá facilmente dar azo a alguma confusão na aplicação prática. Nalguns casos, é difícil determinar a articulação da *lex generalis* com a *lex specialis* e seria útil clarificar esta questão nas propostas. Além disso, neste contexto legal complexo, afigura-se muito útil a sugestão feita pela ACC Schengen no seu parecer sobre a base jurídica proposta para o SIS II (27 de Setembro de 2005) no sentido de se elaborar um «vademecum» que enumere todos os direitos existentes relativamente ao SIS II e estabelecer uma clara hierarquia da legislação aplicável.

Para concluir, o presente parecer procura assegurar um elevado nível de protecção de dados, coerência e clareza para garantir aos interessados a necessária segurança jurídica.

2.2.5. *Impacto da proposta de decisão sobre a protecção de dados no âmbito do terceiro pilar*

A Convenção 108 enquanto instrumento de referência para a protecção de dados da proposta de decisão SIS II será substituída pela Decisão-quadro sobre a protecção de dados no âmbito do terceiro pilar ([1]). Este facto não vem referido na proposta, mas decorre da proposta de decisão-quadro. que estipula no n.º 2 do artigo 34.º que «Qualquer referência à Convenção n.º 108 do Conselho da Europa, de 28 de Janeiro de 1981, relativa à protecção das pessoas no que diz respeito ao tratamento automatizado de dados pessoais deve entender-se como uma referência à presente decisão-quadro.» A AEPD emitirá nas próximas semanas um parecer sobre o projecto de decisão-quadro e não entrará numa análise pormenorizada do seu conteúdo no presente parecer. Todavia, sempre que a aplicação da Decisão-quadro seja susceptível de ter um impacto significativo sobre o regime de protecção de dados no âmbito do SIS II, este facto será sublinhado.

([1]) Substituirá igualmente o regime geral de protecção de dados da Convenção de Schengen (artigos 126.º a 130.º). Este regime não se aplica ao SIS.

2.2.6. *Aplicação do artigo 13.º da Directiva 95/46/CE e do artigo 9.º da Convenção 108*

O artigo 13.º da Directiva 95/46/CE e o artigo 9.º da Convenção 108 prevêem que os Estados-Membros podem tomar medidas legislativas para restringir o âmbito das obrigações e dos direitos nelas previstos, sempre que essas restrições sejam necessárias para salvaguardar outros interesses importantes (p. ex. a segurança nacional, a defesa, a segurança pública) ([2]).

Os considerandos da proposta de regulamento e da proposta de decisão referem que os Estados-Membros podem fazer uso desta possibilidade aquando da transposição dos textos a nível nacional. Nesse caso, deve ser aplicado um teste duplo: a aplicação do artigo 13.º da Directiva 95/46/CE deve obedecer ao artigo 8.º da CEDH e não deve conduzir a uma diminuição do actual regime de protecção de dados.

Este princípio é ainda mais fundamental no caso do SIS II, uma vez que o sistema deve ser previsível. Dado que os Estados-Membros estão a trocar dados, deve ser possível saber com razoável grau de certeza como estes dados serão tratados a nível nacional.

Neste contexto, importa assinalar um aspecto particularmente preocupante que poderá conduzir a uma diminuição do actual nível de protecção de dados. Com efeito, o artigo 102.º da Convenção de Schengen prevê um sistema em que a utilização dos dados está sujeita a regras e restrições rigorosas «Qualquer utilização de dados não conforme com os n.ºs 1 a 4 será considerada como desvio de finalidade face ao direito nacional de cada parte contratante.» Todavia, tanto a Directiva 95/46/CE como a Convenção 108 prevêem que a possibilidade de excepções na legislação nacional nomeadamente ao princípio da limitação às finalidades. Tal entraria em contradição com o sistema actual na Convenção de Schengen que não admite o desvio da legislação nacional do princípio básico da limitação da finalidade e utilização.

A aprovação da decisão-quadro em nada alteraria esta constatação: é mais importante manter o rigoroso respeito pelo princípio da limitação da finalidade para o tratamento de dados SIS II do que assegurar um tratamento conforme à decisão-quadro.

([2]) Como já foi referido, os Estados-Membros que recorrerem a essa possibilidade devem fazê-lo de acordo com o artigo 8.º da CEDH.

A AEPD sugere que seja introduzida nas propostas relativas ao SIS II (nomeadamente no artigo 21.º da proposta de regulamento e no artigo 40.º da proposta de decisão) uma disposição semelhante à do n.º 4 do artigo 102.º da Convenção de Schengen, que limite a possibilidade de os Estados-Membros preverem uma utilização dos dados que não esteja prevista nos textos do SIS II. Uma alternativa seria a restrição explícita na proposta de decisão e na proposta de regulamento do âmbito das excepções autorizadas de acordo com o artigo 13.º da directiva ou do artigo 9.º da Convenção, prevendo-se, por exemplo, que os Estados-Membros apenas podem restringir os direitos de acesso e informação, mas não os princípios que regem a qualidade dos dados.

3. **FINALIDADE**

Nos termos do artigo 1.º de ambos os documentos («Estabelecimento e objectivo geral do SIS II»), o SIS II é estabelecido «a fim de permitir que as autoridades competentes dos Estados-Membros cooperem através do intercâmbio de informações para efeitos da realização de controlos de pessoas e objectos» e «contribuirá para manter um elevado nível de segurança num espaço sem controlos nas fronteiras internas entre os Estados-Membros».

A finalidade do SIS II é expressa em termos relativamente gerais e as disposições acima referidas não constituem, em si mesmos uma indicação exacta do âmbito (significado) deste objectivo.

O objectivo do SIS II afigura-se muito mais lato do que o objectivo do actual SIS, tal como estabelecido no artigo 92.º da Convenção de Schengen que refere concretamente «(…)disporem da lista de pessoas indicadas e de objectos, aquando dos controlos nas fronteiras e das verificações e outros controlos de polícia e aduaneiros e(…)» e (no que respeita às indicações do artigo 96.º) para efeitos do processo de emissão de vistos, da emissão de títulos de residência e da administração dos estrangeiros (…).

Este objectivo mais lato deve-se igualmente ao facto de terem sido acrescentadas ao SIS II novas funcionalidades e acessos que não correspondem ao objectivo primeiro de controlos de pessoas e de objectos, fazendo antes parte de um instrumento de investigação. Está nomeadamente previsto o acesso por parte das autoridades que utilizarão os dados do SIS II para fins próprios e não para fins do SIS II (ver mais adiante). Por outro lado, será generalizada a ligação de indicações, o que constitui um elemento típico de um instrumento de investigação policial.

Levantam-se igualmente questões relacionadas com o motor de busca biométrico que será desenvolvido nos próximos anos e que permite pesquisas no sistema que ultrapassam as necessidades de um sistema de controlo.

Para concluir, as propostas têm um âmbito muito mais lato do que o quadro existente, o que requer salvaguardas suplementares. Na sua análise, a AEPD não focará tanto a definição geral do artigo 1.º enquanto tal, mas sim as funcionalidades e outras partes constitutivas do SIS II.

4. **ALTERAÇÕES SIGNIFICATIVAS NO SIS II**

Este capítulo incide sobretudo nos novos elementos introduzidos pelo SIS II, nomeadamente a biometria, a nova concepção do acesso, com especial atenção para o acesso pela Europol e pela Eurojust, as autoridades encarregadas do registo de veículos, a ligação de indicações e o acesso pelas diferentes autoridades aos dados relativos à imigração.

4.1. **Biometria**

As propostas relativas ao SIS II introduzem a possibilidade de tratar um nova categoria de dados que merece especial atenção, nomeadamente os dados biométricos. Como já foi sublinhado no parecer da AEPD sobre o Sistema de Informação sobre Vistos ([1]), a natureza intrinsecamente sensível dos dados biométricos requer salvaguardas específicas que foram omitidas nas propostas relativas ao SIS II.

De um modo geral pode dizer-se que se assiste a uma crescente tendência para utilizar dados biométricos nos sistemas de informação à escala da UE (VIS, EURODAC, Sistema de Informação sobre cartas de condução, etc.) sem que haja uma análise cuidadosa dos riscos envolvidos e das salvaguardas necessárias.

A necessidade de aprofundar a reflexão foi igualmente sublinhada na recente resolução sobre biometria da Conferência Internacional dos Comissários para a Protecção de Dados em Montreux ([2]). Até à data, a técnica tem sido posta exclusivamente no desenvolvimento de normas que aumentem a interoperabilidade dos sistemas, descurando-se a melhoria da qualidade dos processo biométricos.

([1]) Parecer da AEPD sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo ao Sistema de Informação sobre Vistos e ao intercâmbio de dados entre os Estados-Membros sobre os vistos de curta duração, de 23 de Março de 2005, ponto 3.4.2.

([2]) 27.ª Conferência internacional dos Comissários da Protecção dos Dados e da Vida Privada que se realizou em Montreux, em 16 de Setembro de 2005; resolução sobre a utilização da biometria em passaportes, bilhetes de identidade e documentos de viagem.

Seria útil definir um conjunto de obrigações ou exigências comuns relacionadas com a especificidade desses dados, bem como uma metodologia para a sua implementação. Estes requisitos comuns poderiam incluir nomeadamente os seguintes elementos (cuja necessidade é ilustrada com as propostas relativas ao SIS II:

— **Avaliação orientada do impacto:** Convém sublinhar que as propostas ainda não foram objecto de uma avaliação do impacto da utilização da biometria. ([1])

— **Tónica no processo de registo:** A fonte dos dados biométricos e a forma como serão recolhidos não são especificadas. Sucede porém que a fase do registo é um passo crítico em todo o processo da identificação biométrica que não pode ser definido apenas em anexos ou em debates a nível de subgrupos uma vez que condicionará directamente o resultado final do processo, ou seja o nível da taxa de erro de rejeição ou de aceitação.

— **Importância do nível de exactidão:** A utilização da biometria para efeitos de identificação (comparação de um com muitos elementos), apresentada na proposta como a futura implementação de um «motor de busca da dados biométricos» é mais problemática porque os resultados deste processo são menos exactos do que a utilização dos dados para efeitos de autenticação ou controlo (comparação de dois elementos). A identificação biométrica não deve, pois, constituir a única forma de identificação ou a única via de acesso a outras informações.

— **Procedimento de segurança:** Devem ser implementados processos de segurança facilmente acessíveis a fim de respeitar a dignidade das pessoas que tenham sido identificadas por engano e de evitar que sobre elas recaia o ónus das deficiências do sistema.

A utilização de dados biométricos sem a devida avaliação preliminar revela igualmente que se sobrestima a fiabilidade da biometria. Os dados biométricos são dados «vivos» que evoluem com o tempo e as amostras armazenadas na base de dados apenas representam um retrato instantâneo de um elemento dinâmico. A sua permanência não é absoluta e requer controlo. A exactidão dos dados biométricos deve sempre ser conferida com outros elementos, pois nunca será absoluta.

([1]) A avaliação poderia assentar nos chamados sete pilares da sabedoria referidos em Biometria na fronteira: avaliar o impacto sobre a sociedade IPTS, DG-JRC, EUR 21585 EN, Parte 1.2, página 32.

A possível utilização dos dados do SIS II para efeitos de investigação encerra graves riscos para os interessados se as provas biométricas passarem a assumir importância maior ou exagerada, como ficou patente nalguns casos no passado ([2]).

Por conseguinte, as propostas devem reconhecer e sensibilizar para as capacidades reais da biometria para fins de identificação.

4.2. **Acesso aos dados do SIS II**

4.2.1 *Uma nova visão do acesso*

As autoridades que têm acesso aos dados do SIS são definidos para cada indicação. Em princípio, aplica-se um critério duplo para conceder o acesso aos dados do SIS: o acesso deve ser garantido às autoridades no pleno respeito do objectivo geral do SIS e da finalidade específica de cada indicação.

Tal decorre da definição de indicação que se encontra tanto na proposta de regulamento como na proposta de decisão (n.º 1 do artigo 3.º de ambos os instrumentos: *'..entende-se por... «indicação», um conjunto de dados inseridos no SIS II para permitir que as autoridades competentes procedam à identificação de uma pessoa ou de um objecto com vista à adopção de uma conduta específica)*. O n.º 2 do artigo 39.º da proposta de decisão reforça esta posição e estipula que «*Os dados referidos no n.º 1 só são utilizados para identificar uma pessoa com vista à execução de uma conduta específica a adoptar em conformidade com a presente decisão.*» A este respeito, o SIS II continua a ter as características de um sistema sim ou não no qual cada indicação é inserida para um fim determinado (entrega, recusa de entrada, …)

As autoridades com acesso aos dados do SIS estão efectivamente sujeitos a uma limitação da utilização dos dados uma vez que, em princípio, apenas podem aceder aos dados para tomar medidas específicas.

Todavia, algumas autorizações de acesso previstas nas novas propostas não se coadunam com esta lógica: com efeito, destinam-se a fornecer informações à autoridade, mas não lhe permitem identificar a pessoa nem tomar a medida prevista na indicação.

([2]) Em Junho de 2004, um advogado de Portland (EUA) foi preso durante duas semanas porque o FBI relacionou as suas impressões digitais com as encontradas nos atentados à bomba em Madrid (no saco plástico que continha o detonador). Revelou-se que o processo de correspondência tinha erros que levaram a uma interpretação errada.

Concretamente, trata-se do:

— acesso a dados sobre a imigração por parte das autoridades de asilo;

— acesso a dados sobre a imigração por parte das autoridades responsáveis pela atribuição do estatuto de refugiado;

— acesso da Europol a indicações sobre a extradição, a vigilância discreta e documentos roubados;

— acesso da Eurojust a dados sobre a extradição e localização.

Todas estas autoridades têm em comum no que respeita aos dados SIS II

o facto de não poderem adoptar a conduta específica referida na definição de indicação. Apenas têm acesso aos dados como fonte de informação para os seus fins próprios.

Mesmo entre estas autoridades, há que distinguir entre as autoridades com acesso para os seus próprios fins, subordinado a um objectivo bem específico, e as autoridades (nomeadamente a Europol e a Eurojust) às quais não é imposto nenhuma finalidade específica para poderem ter acesso aos dados. As autoridades de asilo, por exemplo, têm um acesso para um fim específico, mesmo que esse fim não seja mencionado na indicação. Podem aceder a todos os dados sobre a imigração «com vista a determinar se o requerente de asilo permaneceu ilegalmente noutro Estado-Membro». A Europol e a Eurojust, por seu lado, têm acesso aos dados incluídos em certas categorias de indicações «necessários para a execução das suas funções».

Em suma, o acesso aos dados SIS II é concedido em três casos:

— acesso para a execução da indicação;

— acesso para fins que não o SIS II, mas bem delimitados nas propostas;

— acesso para efeitos que não o SIS II, sem delimitação concreta.

A AEPD considera que quanto mais geral for a finalidade do acesso mas rigorosas devem ser as salvaguardas a implementar. Passamos a enumerar as salvaguardas gerais e, em seguida, será abordada a situação específica da Europol e da Eurojust.

4.2.2 *Condições para conceder o acesso*

1. O acesso só pode ser autorizado se for compatível com a finalidade genérica do SIS II e se for conforme com a sua base jurídica.

   Isto significa, na prática, que o acesso aos dados sobre imigração em conformidade com a proposta de regulamento deve promover a implementação de políticas relacionadas com a parte do acervo de Schengen relativa à circulação de pessoas.

   Do mesmo modo, o acesso a indicações previsto pela decisão deve visar a promoção da cooperação operacional entre autoridades policiais e judiciárias em matéria penal.

   Neste contexto, a AEPD chama a atenção para o capítulo sobre o acesso ao SIS II por parte dos serviços competentes para a emissão dos certificados de matrícula de veículos (ver ponto 4.6 adiante).

2. Deve ser comprovada a necessidade do acesso aos dados do SIS II, bem como a impossibilidade ou grande dificuldade de obter os dados por outros meios menos invasivos. Este aspecto deveria ter sido mencionado na exposição dos motivos e, como aliás já foi dito, é lamentável que tenha sido omitido.

3. A utilização que será dada aos dados deve ser definida de modo explícito e restritivo.

   Por exemplo, as autoridades de asilo podem aceder aos dados sobre a imigração «com vista a determinar se o requerente de asilo permaneceu ilegalmente noutro Estado-Membro». A Europol e a Eurojust, por seu lado, têm acesso aos dados incluídos em certas categorias de indicações «necessários para a execução das suas funções». Ora, esta situação não é suficientemente definida (ver adiante).

4. As condições de acesso devem ser bem definidas e restritas. Em especial, só devem ter acesso ao SIS II os serviços no interior destas organizações que são chamados a trabalhar com esses dados. Esta obrigação está prevista no artigo 40.º da proposta de decisão e no n.º 2 do artigo 21.º da proposta de regulamento e deve ser completada por uma disposição que obrigue as autoridades nacionais a manter uma lista actualizada de pessoas autorizadas a aceder ao SIS II. O mesmo se aplica à Europol e à Eurojust.

5. O facto de essas autoridades terem acesso aos dados do SIS II nunca pode servir de justificação para introduzir ou manter dados no sistema que não sejam úteis para a indicação da qual fazem parte. Não podem ser acrescentadas novas categorias de dados com o argumento de que esses dados seriam úteis a outros sistemas de informação. Por exemplo, o artigo 39.º da proposta de decisão prevê a introdução nas indicações de dados sobre a autoridade emissora. Estes dados não são necessários para tomar determinadas medidas (detenção, vigilância, …) e a única razão para serem introduzidos será provavelmente a sua utilidade para a Europol ou a Eurojust. Deveriam ser estabelecidas regras claras para o tratamento desses dados.

6. O período de conservação dos dados não pode ser alargado se não for necessário para os fins para os quais foram inseridos. Ou seja, mesmo que a Europol ou a Eurojust tenham acesso a esses dados, tal não é razão suficiente para os manter no sistema (por exemplo, logo que a pessoa procurada tenha sido extraditada, devem ser suprimidos os dados, mesmo que possam ser úteis à Europol). Mais uma vez, neste caso, será necessária uma controlo cuidadoso para assegurar a aplicação deste princípio pelas autoridades nacionais.

4.2.3 *Acesso da Europol e da Eurojust*

a. *Motivos de acesso*

O acesso da Europol e da Eurojust a alguns dados do SIS já foi objecto de debate antes da sua introdução pela Decisão do Conselho de 24 de Fevereiro de 2005 ([1]). De todas as autoridades com acesso para fins próprios, estes dois organismos beneficiam de um acesso autorizado nos mais amplos termos. Embora a utilização desses dados seja discriminada no Capítulo XII, os motivos para autorizar o acesso não estão à partida suficientemente definidos, tanto mais se tivermos em conta que as missões da Europol e da Eurojust evoluirão muito provavelmente ao longo do tempo.

A AEPD insta a Comissão a definir de modo restritivo as tarefas cuja execução justifica o acesso da Europol e da Eurojust.

b. *Restrição dos dados*

A fim de evitar «a pesca de dados» por parte da Europol e da Eurojust e de assegurar que apenas tenham acesso aos dados «necessários para a execução das suas funções», a ACC Schengen, no seu parecer de 27 de Setembro de 2005 sobre as propostas relativas ao SIS II, sugeriu limitar o acesso da Europol e da Eurojust aos dados relativos a pessoas singulares cujos nomes já constem dos respectivos ficheiros. Assim, assegurar-se-ia que estas organizações se limitassem a consultar as indicações pertinentes para os respectivos fins. A AEPD apoia esta recomendação.

c. *Aspectos de segurança*

A AEPD congratula-se com o registo obrigatório de todas as operações executadas em linha pela Europol e pela Eurojust, bem como com a proibição de copiar ou descarregar partes do sistema.

O artigo 56.º da proposta de decisão prevê «um ou dois» pontos de acesso para a Europol e a Eurojust. Por muito compreensível que possa ser que os Estados-Membros precisem de mais do que um ponto de acesso, em virtude da descentralização das suas autoridades competentes o estatuto e as actividades da Europol e da Eurojust não justificam este pedido. Importa sublinhar igualmente que do ponto de vista da segurança, a multiplicação dos pontos de acesso aumenta o risco de abusos, devendo por conseguinte ser justificado de modo preciso com elementos mais coerentes. Por conseguinte, na ausência de argumentos convincentes, a AEPD sugere que se autorize apenas um ponto de acesso à Europol e à Eurojust.

4.3. **Ligações de indicações**

O artigo 26.º do regulamento e o artigo 46.º da decisão prevêem que os Estados-Membros podem criar um ligação entre as indicações em conformidade com a legislação nacional por forma a estabelecer uma relação entre duas ou mais indicações.

É certo que as ligações entre indicações podem ser úteis no âmbito de controlos (por exemplo, um mandado de detenção relativo a um ladrão de automóveis pode ser relacionado com um veículo roubado), no entanto, a introdução de ligações entre indicações é uma característica típica de um instrumento de investigação policial.

A ligação entre indicações pode ter um impacto importante sobre os direitos do interessado uma vez que deixa de ser «avaliado» com base em dados exclusivamente relacionados com o próprio, mas sim com base na sua eventual associação com outras pessoas. Os indivíduos cujos dados estão ligados a dados relativos a criminosos ou pessoas procuradas serão provavelmente tratados com maior suspeita do que outros. A ligação entre indicações equivale a um alargamento dos poderes de investigação do SIS porque possibilitará o registo de alegadas organizações ou redes (por exemplo, se forem ligados dados sobre imigrantes ilegais a dados sobre traficantes). Por último, uma vez que a criação de ligações é deixada à legislação nacional, poderá dar-se o caso de haver ligações ilegais num Estado-Membro mas que podem ser criadas noutro, com a consequente alimentação do sistema com dados «ilegais».

([1]) Decisão 2005/211/JAI do Conselho, de 24 de Fevereiro de 2005, relativa à introdução de novas funções no Sistema de Informação Schengen, incluindo a luta contra o terrorismo (JO, L 68 de 15.3.2005, p. 44)

As conclusões do Conselho de 14 de Junho de 2004 relativas aos requisitos funcionais do SIS II estipulam que cada ligação deve assentar numa exigência operacional bem definida e numa relação claramente definida e respeitar o princípio da proporcionalidade. Além disso, não pode afectar os direitos de acesso. De qualquer modo, uma vez que a ligação de indicações constitui uma operação de tratamento, deve respeitar as disposições nacionais que transpõem a Directiva 95/46/CE e/ou a Convenção 108.

As propostas reiteram que a existência de ligações não pode alterar os direitos de acesso (com efeito, caso contrário daria acesso a dados cujo tratamento seria ilegal ao abrigo da legislação nacional, em violação do artigo 6.º da directiva).

A AEPD sublinha a importância de uma interpretação rigorosa do artigo 26.º da proposta de regulamento e do artigo 46.º da proposta de decisão. Para tanto, importa tornar bem claro que às autoridades que não têm o direito de acesso a certas categorias de dados não só é vedado o acesso a ligações a estas categorias como nem sequer devem estar ao corrente da sua existência. A visualização das ligações deve ser impossível sempre que não haja um direito de acesso aos dados ligados.

Além disso, a AEPD gostaria de ser consultada sobre as medidas técnicas tomadas para o efeito.

4.4. **Indicações para efeitos de não admissão**

4.4.1. *Motivos para inclusão*

A utilização de «indicações de nacionais de países terceiros para efeitos de não admissão» (artigo 15.º do regulamento) tem um impacto significativo sobre as liberdades individuais: uma pessoa indicada ao abrigo desta disposição deixa de ter acesso ao espaço Schengen por vários anos. Até à data, esta indicação é a mais utilizada em termos do número de pessoas indicadas. Tendo presentes as consequências desta indicação, bem como o número de pessoas envolvidas, deve ser posto grande cuidado na sua concepção e implementação. Embora esta consideração também seja válida para outras indicações, a AEPD dedicará um capítulo específico a esta indicação porque levanta problemas específicos que se prendem com os motivos de inclusão.

A nova indicação de não admissão constitui uma melhoria em relação à situação actual, mas não é totalmente satisfatória uma vez que se baseia em grande parte em instrumentos que ainda não foram aprovados nem sequer propostos.

A melhoria reside numa descrição mais exacta dos motivos de inclusão dos dados. A actual redacção da Convenção de Schengen conduziu a uma situação caracterizada por diferenças significativas entre Estados-Membros no que respeita ao número de pessoas indicadas ao abrigo do artigo 96.º da Convenção. A ACC Schengen levou a cabo um estudo exaustivo ([1]) sobre a questão e formulou recomendações no sentido de que os «decisores políticos deveriam ponderar a harmonização dos motivos na base de uma indicação nos diferentes Estados-Membros».

A redacção do artigo 15.º é mais pormenorizada o que merece aprovação.

Além disso, o n.º 2 do artigo 15.º enumera um lista de casos em que as pessoas não podem ser indicadas por residirem legalmente no território de um Estado-Membro ao abrigo de diferentes estatutos. Embora não seja possível inferir da actual Convenção de Schengen, a prática mostrou que a aplicação deste mecanismo acusa igualmente variações entre Estados-Membros. Por conseguinte, a clarificação constitui um elemento positivo.

Todavia, esta disposição é igualmente alvo de sérias críticas uma vez que se baseia em grande parte num texto que ainda não foi aprovado, nomeadamente a directiva relativa ao «regresso».

Desde a aprovação das propostas relativas ao SIS II, a Comissão propôs uma directiva relativa a normas e procedimentos comuns nos Estados-Membros para o regresso de nacionais de países terceiros em situação irregular (em 1 de Setembro de 2005), mas enquanto este texto não for ultimado não pode ser considerado uma base válida para inserir dados num sistema. Constitui nomeadamente uma violação do artigo 8.º CEDH visto que uma ingerência na vida privada de pessoas deve ser justificada designadamente por uma legislação clara e acessível.

Por conseguinte, a AEPD insta a Comissão a retirar esta disposição ou a reformulá-la com base na legislação existente por forma a que os interessados saibam exactamente quais as medidas que as autoridades podem tomar a seu respeito.

4.4.2. *Acesso a indicações introduzidas ao abrigo do artigo 15.º*

O artigo 18.º define as autoridades que têm acesso a estas indicações e os respectivos fins. Os n.ºs 1 e 2 do artigo 18.º determinam as autoridades que dispõem de acesso às indicações introduzidas por força da directiva relativa ao regresso. Também aqui se aplica o que foi dito anteriormente.

([1]) Relatório da Autoridade Comum de Controlo Schengen sobre a utilização feita das indicações ao abrigo do artigo 96.º do Sistema de Informação de Schengen, Bruxelas, 20 de Junho de 2005.

O n.º 3 do artigo 18.º da proposta de regulamento concede o acesso às autoridades responsáveis pela atribuição do estatuo de refugiado de acordo com uma directiva que ainda nem sequer foi proposta. Na ausência de um texto disponível, a AEPD vê-se obrigada a reiterar os comentários acima tecidos.

4.4.3. *Período de conservação de indicações introduzidas ao abrigo do artigo 15.º*

Nos termos do artigo 20.º, as indicações não podem ser mantidas por um período superior ao período de não admissão estabelecido na decisão (de afastamento ou regresso). Esta disposição obedece às regras em matéria de protecção de dados. Além disso, as indicações serão apagadas automaticamente ao fim de cinco anos salvo decisão contrária dos Estados-Membros que introduziram os dados no SIS II.

Deverá ser previsto um controlo adequado a nível nacional que garanta que não haja nenhuma prorrogação automática injustificada do período de conservação e que os Estados-Membros apaguem os dados antes do fim do prazo de cinco anos na eventualidade de um período de não admissão mais curto.

4.5. **Períodos de conservação**

Embora o princípio de conservação se mantenha inalterado (regra geral, as indicações devem ser apagadas do SIS logo que tenham sido tomadas as medidas nelas exigidas), as propostas levarão a um alargamento geral do período de conservação das indicações.

A Convenção de Schengen previa um reexame da necessidade de continuar a armazenar os dados no prazo máximo de três anos a contar da sua introdução (ou um ano no caso de dados introduzidos para fins de vigilância discreta). As novas propostas prevêem a supressão automática (com possibilidade de oposição por parte do Estado-Membro emissor) no prazo de 5 anos dos dados sobre imigração, de 10 anos dos dados sobre detenção, pessoas desaparecidas e pessoas procuradas no âmbito de processos judiciais e de 3 anos dos dados sobre pessoas colocadas sob vigilância discreta.

Embora, em princípio, os Estados-Membros sejam obrigados a apagar os dados uma vez concretizada a finalidade da indicação, tal implica um aumento significativo do período máximo de conservação (triplicando-o na maior parte dos casos) sem qualquer justificação por parte da Comissão. No caso dos dados sobre imigração, presume-se que o prazo de cinco anos esteja relacionado com a duração da interdição de admissão proposta no projecto de directiva relativa ao regresso. Nos restantes casos, a AEPD não vê qualquer justificação.

O potencial impacto sobre os interessados indicados no SIS pode ter consequências consideráveis nas vidas das pessoas. Tal é particularmente preocupante no caso de indicações de pessoas para efeitos de vigilância discreta ou controlos específicos uma vez que estas indicações podem ser emitidas com base em suspeitas.

A AEPD gostaria de ver uma justificação séria para este alargamento dos períodos de conservação de dados. Na ausência de uma justificação plausível, sugere a redução destes períodos para a actual duração, com especial destaque para o caso das indicações inseridas para efeitos de vigilância discreta ou controlos específicos.

4.6. **Acesso pelos serviços competentes para a emissão dos certificados de matrícula dos veículos**

A principal questão prende-se com a escolha de uma base jurídica deveras contestável. A Comissão não aduz argumentos convincentes para o recurso a uma base jurídica «transportes» do primeiro pilar (transportes) que permitiria o acesso ao SIS por parte dos serviços administrativos para efeitos de prevenção e luta contra o crime (tráfico de veículos roubados). A necessidade de uma justificação forte e de uma base jurídica sólida para autorizar o acesso ao SIS II já foi sublinhada no ponto 4.2.2 do presente parecer.

A AEPD remete para os comentários tecidos sobre a matéria pela ACC Schengen no seu parecer sobre a base jurídica proposta para o SIS II. Em especial, deve ser acatada a sugestão da ACC Schengen no sentido de alterar a proposta de decisão a fim de incluir este acesso.

5. PAPEL DA COMISSÃO E DOS ESTADOS-MEMBROS

É indispensável descrever e repartir claramente as responsabilidades no âmbito do SIS II, não só com vista ao bom funcionamento do sistema mas também em termos de controlo. A repartição das competências de controlo decorre da descrição das responsabilidades, de onde a necessidade de clareza absoluta.

5.1. **Papel da Comissão**

A AEPD congratula-se com o Capítulo III de ambas as propostas que descreve o papel e as responsabilidades da Comissão no âmbito do SIS II («gestor operacional»). A falta desta clarificação fez sentir-se na proposta VIS. Todavia, este capítulo por si só não define de modo exaustivo o papel da Comissão. Com efeito, como se refere no ponto 9 do presente parecer, a Comissão participa igualmente na implementação e gestão do sistema através do procedimento de comitologia.

Em termos de protecção de dados, a Comissão tem um papel que lhe é reconhecido já nos sistemas VIS e Eurodac, ou seja o de responsável pela gestão operacional. Junto com o seu papel importante a nível do desenvolvimento e manutenção do sistema, este papel deve ser encarado como o um papel de controlador *sui generis*. Como já foi dito no parecer da AEPD sobre o VIS, este papel corresponde mais ao de um processador, por ser mais limitado do que o de um controlador normal, uma vez que a Comissão não tem acesso aos dados tratados no SIS II.

Dado que o SIS II assentará em sistemas complexos, alguns dos quais apoiados em tecnologias emergentes, a AEPD insiste em que seja reforçada a responsabilidade da Comissão para manter os sistemas actualizados mediante a aplicação das melhores tecnologias disponíveis em matéria de segurança e protecção de dados.

Por conseguinte, convém aditar ao artigo 12.º das propostas que a Comissão deve propor periodicamente a implementação de novas tecnologias que correspondam ao estado-da-arte neste domínio e que reforcem os níveis de protecção e de segurança dos dados, facilitando igualmente as tarefas das autoridades nacionais que têm acesso a estes dados.

5.2. **Papel dos Estados-Membros**

A situação dos Estados-Membros não é muito clara uma vez que é bastante difícil saber qual (quais) a(s) autoridade(s) responsável (responsáveis) pelo controlo dos dados.

As propostas descrevem o papel de gabinete nacional SIS II (para garantir o acesso das autoridades competentes ao SIS II), bem como das autoridades SIRENE (para assegurar o intercâmbio de todas as informações suplementares). Cabe igualmente aos Estados-Membros assegurar o funcionamento e a segurança dos seus «SN» («sistema nacional»). Não é claro se esta última responsabilidade incumbe a uma das autoridades acima referidas. Em todo o caso, há que clarificar este aspecto.

Em termos de protecção de dados, a Comissão e os Estados-Membros devem ser considerados controladores conjuntos encarregados de responsabilidades específicas. Reconhecer estas missões complementares é a única forma de garantir o controlo de todos os domínios de actividades do SIS II.

6. **DIREITOS DA PESSOA EM CAUSA**

6.1. **Informação**

6.1.1. *Proposta de regulamento*

O artigo 28.º da proposta de regulamento prevê o direito de informação da pessoa em causa inspirado principalmente no artigo 10.º da Directiva 95/46. Trata-se de uma alteração bem-vinda relativamente à situação actual uma vez que a Convenção não prevê explicitamente qualquer direito de informação. Podem, no entanto, ser introduzidas algumas melhorias no seguintes pontos:

Algumas informações devem ser acrescentadas à lista no intuito de assegurar um tratamento justo da pessoa em causa ([1]). Estas informações prendem-se com o período de conservação dos dados, a existência do direito de pedir um reexame ou um recurso da decisão de inserir uma indicação (nalguns casos, ver n.º 3 do artigo 15.º da proposta de regulamento), a possibilidade de obter assistência da autoridade de protecção de dados e a existência de vias de recursos.

A proposta de regulamento é omissa no que respeita ao momento em que a informação deve ser prestada. Ora, esta omissão pode impossibilitar o exercício dos seus direitos pelo interessado. A fim de tornar estes direitos efectivos, o regulamento deve prever um prazo exacto para a prestação das informações, em função da autoridade que inseriu a indicação.

Uma solução prática poderia consistir em aditar informações sobre a indicação na decisão que motivou a mesma: quer uma decisão judicial ou administrativa baseada numa ameaça à ordem pública ou à segurança pública (…) quer uma decisão de regresso ou ordem de afastamento acompanhada de uma interdição de readmissão. Este aditamento poderia ser introduzido no artigo 28.º do regulamento.

6.1.2. *Proposta de decisão*

O artigo 50.º da decisão prevê que a informação é prestada a pedido do interessado e enumera os possíveis motivos de recusa. É compreensível que haja restrições deste direito tendo em conta a natureza dos dados e contexto em que são tratados.

Todavia, o direito de informação não deve depender de um pedido do interessado (nesse caso, tratar-se-ia da definição de um pedido de acesso). Supõe-se que a necessidade de «pedir» informação se justifica nos casos em que o interessado não pode ser informado por se desconhecer o seu paradeiro.

Seria preferível aditar uma derrogação ao direito de informação nos casos em que a prestação de informação se revele impossível ou envolva um esforço desproporcionado. O artigo 50.º da decisão deverá ser alterado em conformidade.

([1]) O parecer da AEPD sobre a criação do Sistema de Informação sobre Vistos vai no mesmo sentido. (ver ponto 3.10.1)

Esta solução seria igualmente coerente com a aplicação da proposta de decisão-quadro sobre a protecção de dados no âmbito do terceiro pilar.

6.2. **Acesso**

Tanto a proposta de regulamento como a proposta de decisão estipulam prazos para a resposta a pedidos de acesso, o que constitui uma evolução positiva. Todavia, uma vez que as modalidades de exercício do direito de acesso são definidas a nível nacional, é legitimo perguntar como os prazos estipulados nas propostas se coadunam com os procedimentos nacionais, em especial se os Estados-Membros preverem prazos mais curtos para responder a um pedido de acesso. Deve ficar bem claro que se aplicam os prazos mais favoráveis ao interessado.

6.2.1. *Proposta de regulamento*

Convém notar que as restrições do direito de acesso («a comunicação da informação ao interessado será recusada se for susceptível de prejudicar a execução da tarefa legal consignada na indicação, ou a protecção dos direitos e liberdades de outrem») actualmente previstas na Convenção de Schengen não constam da proposta de regulamento.

Todavia, isto deve-se provavelmente à Directiva 95/46/CE que prevê (no artigo 13.º) a possibilidade de excepções nas legislações nacionais. Em todo o caso, convém sublinhar que o recurso ao artigo 13.º na legislação nacional para limitar o direito de acesso deve estar sempre em conformidade com o artigo 8.º CEDH e ser reservado a casos limitados.

6.2.2. *Proposta de decisão*

A proposta de decisão retoma a limitação do direito de acesso da Convenção de Schengen. A proposta de decisão-quadro contém essencialmente as mesmas limitações do direito de acesso de modo que a aprovação deste instrumento não traz alterações significativas neste domínio.

Uma vez que em vários Estados-Membros o acesso aos dados em matéria de aplicação da lei é «indirecto» (ou seja, passa pela autoridade nacional de protecção de dados), será útil obrigar as autoridades de protecção de dados a cooperar activamente no exercício do direito de acesso.

6.3. **Direito de reexame ou recurso da decisão de inserir uma indicação**

O n.º 3 do artigo 15.º do regulamento institui um direito de obter um reexame ou de introduzir um recurso se a decisão de inserir uma indicação for tomada por uma autoridade administrativa.

Trata-se de um aditamento bem-vindo comparado com a Convenção de Schengen em vigor que sublinha a necessidade de informar completa e atempadamente o interessado, como já foi referido no ponto 6.1 supra. Com efeito, sem esta informação este novo direito teria carácter meramente teórico.

6.4. **Vias de recurso**

O artigo 30.º da proposta de regulamento e o artigo 52.º da proposta de decisão prevêem o direito de propor uma acção ou de apresentar reclamação junto dos tribunais de qualquer Estado-Membro se ao interessado for recusado o direito de acesso, de rectificação ou apagamento dos dados que lhe dizem respeito ou de obter informações ou reparação.

Tal como está formulada («No território de qualquer Estado-Membro»), esta disposição sugere que um queixoso deve estar fisicamente presente no território para instaurar a sua acção em tribunal. Esta limitação territorial não se justifica e pode esvaziar de sentido o direito de recurso uma vez que frequentemente o queixoso vai instaurar uma acção precisamente porque lhe é negado o acesso ao território de Schengen. Além disso, no que diz respeito à proposta de regulamento, sendo a directiva a *lex generalis*, deve ser tido em conta o seu artigo 22.º que estipula que «qualquer pessoa» poderá recorrer judicialmente seja qual for o seu local de residência. A proposta de decisão, por seu lado, também não prevê uma limitação territorial. A AEPD sugere que se suprima a limitação territorial dos artigos 30.º e 52.º.

7. **CONTROLO**

7.1. **Observação preliminar: partilha das responsabilidades**

As propostas repartem a responsabilidade pelo controlo entre as autoridades nacionais de controlo ([1]) e a AEPD de acordo com as respectivas atribuições. Esta abordagem corresponde à das propostas relativas à lei aplicável e às responsabilidades pelo funcionamento e utilização do SIS II, bem como à necessidade de um controlo efectivo.

Por conseguinte, a AEPD congratula-se com a abordagem seguida no artigo 31.º da proposta de regulamento e no artigo 53.º da proposta de decisão. Todavia, para melhorar a compreensão e clarificar as respectivas tarefas, a AEPD propõe que cada artigo seja subdividido em várias disposições, cada qual dedicada a um nível de controlo, a exemplo do que sucede na proposta VIS.

([1]) As autoridades de controlo da Europol e da Eurojust são igualmente envolvidas, embora em menor medida.

7.2. **Controlo pelas autoridades nacionais de protecção de dados**

Nos termos do artigo 31.º da proposta de regulamento e do artigo 53.º do a proposta de decisão, os Estados-Membros devem assegurar que uma autoridade independente controla a legalidade do tratamento dos dados pessoais do SIS II.

O artigo 53.º da proposta de decisão acrescenta o direito de qualquer pessoa de solicitar à autoridade de controlo que verifique a legalidade do tratamento dos dados que lhe dizem respeito. Uma disposição análoga não foi incluída na proposta de regulamento dado que a directiva se aplica a título de *lex generalis*. Por conseguinte, é forçoso concluir que as autoridades nacionais de protecção de dados podem exercer, no tocante ao SIS II, todas as competências que lhes são atribuídas pelo artigo 28.º da Directiva 95/46/CE, incluindo a verificação da legalidade do tratamento dos dados. O n.º 1 do artigo 31.º do regulamento vem clarificar a sua missão, mas não pode constituir uma limitação dos seus poderes. O reconhecimento destas competências deveria ser clarificado no texto da proposta de regulamento.

A proposta de decisão, por seu lado, atribui responsabilidades mais alargadas às autoridades de controlo nacionais porque a sua *lex generalis* é outra. Contudo, não se afigura razoável que as autoridades de controlo tenham missões e competências diferentes consoante a categoria dos dados tratados, o que, aliás, seria uma situação difícil de gerir na prática. Por conseguinte, tal deve ser evitado, quer reconhecendo a estas autoridades as mesmas competências no texto da própria proposta de directiva quer remetendo para outra *lex generalis* (nomeadamente a Decisão-quadro relativa à protecção de dados no âmbito do terceiro pilar), conferindo mais competências às autoridades de protecção de dados.

7.3. **Controlo pela AEPD**

A AEPD assegura que as actividades de tratamento de dados por parte da Comissão se processem de acordo com as propostas. Por outro lado, a AEPD deveria poder exercer todas as competências que lhe são atribuídas pelo Regulamento n.º 45/2001, tendo em conta, no entanto, os poderes limitados da Comissão no que respeita aos dados propriamente ditos.

Convém acrescentar que, nos termos da alínea f) do artigo 46.º do Regulamento n.º 45/2001, a AEPD deve «cooperar com as autoridades nacionais de controlo …na medida do necessário ao cumprimento das suas obrigações respectivas». A cooperação com os Estados-Membros para efeitos de controlo do SIS II não assenta apenas nas propostas, mas também no Regulamento n.º 45/2001.

7.4. **Controlo conjunto**

As propostas reconhecem igualmente a necessidade de coordenar as actividades de controlo desenvolvidas pelas diferentes autoridades envolvidas. O artigo 31.º da proposta de regulamento e o artigo 53.º da proposta de decisão estipulam que «as autoridades nacionais de controlo e a Autoridade Europeia para a Protecção de Dados cooperem estreitamente entre si. Para este efeito, a Autoridade Europeia para a Protecção de Dados organiza uma reunião pelo menos uma vez por ano.»

A AEPD congratula-se com esta proposta que contém os elementos essenciais para estabelecer a cooperação, que é efectivamente crucial, entre as autoridades responsáveis pelo controlo a nível nacional e europeu. Convém sublinhar que as propostas prevêem reuniões pelo menos uma vez por ano; no entanto, esta periodicidade deve ser considerada mínima.

Estas disposições (artigo 31.º da proposta de regulamento e o artigo 53.º da proposta de decisão) poderão contudo beneficiar de algumas clarificações do conteúdo dessa coordenação. A ACC é competente para analisar questões que se prendem com a interpretação ou aplicação da Convenção, estudar problemas que possam surgir no âmbito do exercício do controlo independente ou do direito de acesso e elaborar propostas harmonizadas de soluções conjuntas para problemas existentes.

As novas propostas não podem conduzir a uma restrição do actual âmbito de controlo comum. Se não houver dúvidas de que as autoridades de protecção de dados podem exercer relativamente ao SIS II todas as competências em matéria de controlo que lhes são atribuídas ao abrigo da Directiva, a cooperação destas autoridades pode abranger um vasto leque de aspectos do controlo do SIS II, incluindo as tarefas da actual ACC conforme definidas no artigo 115.º da Convenção de Schengen.

Todavia, para não deixar margem para dúvidas, seria útil introduzir uma referência explícita neste sentido nas propostas.

8. **SEGURANÇA**

A gestão e o respeito de um nível máximo de segurança do SIS II constitui uma condição fundamental para assegurar a protecção de dados pessoais armazenados na base de dados. A fim de conseguir este nível satisfatório de protecção, devem ser implementadas salvaguardas adequadas contra os riscos potenciais inerentes à infra-estrutura do sistema e às pessoas envolvidas. Esta temática é abordada em várias partes da propostas, embora seja susceptível de alguns melhoramentos.

Com efeito, os artigos 10.º e 13.º da proposta incluem diversas medidas relativas à segurança dos dados, discriminando os tipos de abusos que devem ser evitados. A AEPD congratula-se com a inclusão nestes artigos de disposições sobre o (auto-) controlo sistemático das medidas de segurança.

Todavia, o artigo 59.º da proposta de decisão e o artigo 34.º da proposta de regulamento relativos ao acompanhamento e à avaliação não deveriam cingir-se aos aspectos relacionados com os resultados, a eficácia em termos de custos e a qualidade dos serviços, devendo incidir igualmente sobre requisitos legais, nomeadamente no domínio da protecção de dados. A AEPD recomenda, por conseguinte, que o âmbito destes artigos seja alargado ao acompanhamento e apresentação de relatórios sobre a legalidade do tratamento.

Além disso, para completar o disposto na alínea f) do n.º 1 do artigo 10.º ou do artigo 18.º da proposta de decisão e no artigo 17.º do regulamento relativo ao pessoal autorizado que tem acesso aos dados, deve ser aditado que os Estados-Membros (bem como a Europol e a Eurojust) devem assegurar a disponibilidade de perfis exactos dos utilizadores (aos quais devem ter acesso as autoridades nacionais de controlo para verificação). Para além destes perfis dos utilizadores, deve ser elaborada uma lista exaustiva da identidade dos utilizadores e actualizada permanentemente pelos Estados-Membros. O mesmo se aplica *mutatis mutandis* à Comissão.

Estas medidas de segurança são completadas por salvaguardas a nível do acompanhamento e da organização. O artigo 14.º das propostas descreve as condições e os fins para os quais devem ser mantidos registos de todas as operações de tratamento de dados. Estes registos não devem ser conservados apenas para monitorizar a protecção de dados e garantir a segurança dos dados, mas também para consolidar o auto-controlo regular do SIS II estipulado no artigo 10.º. Os relatórios de auto-controlo contribuirão para a execução efectiva das tarefas das autoridades de controlo que poderão assim identificar os pontos mais fracos e neles centrar a sua atenção no âmbito do seu próprio exercício de controlo.

Como foi referido anteriormente no presente parecer, a multiplicação dos pontos de acesso ao sistema deve ser devidamente justificada visto que com ela aumentam automaticamente os riscos de abuso. A demonstração concreta da necessidade de um segundo ponto de acesso deve, pois, ser exigida na alínea b) do n.º 1 do artigo 4.º das propostas.

A necessidade de cópias nacionais do sistema central não é bem explicada nos dois textos e dá origem a sérias preocupações no que respeita ao risco global e à segurança do sistema, nomeadamente:

— A multiplicação de cópias aumento o risco de abusos (em especial tendo em conta a existência de novos dados tais como os dados biométricos);

— Os dados abrangidos por essas cópias não são bem definidos;

— As exigências em termos de exactidão, qualidade e disponibilidade constantes do artigo 9.º constituem importantes desafios técnicos e aumentam, por conseguinte, os custos em função da tecnologia mais avançada disponível;

— O controlo destas cópias pelas autoridades nacionais requererá recursos humanos e financeiros suplementares que nem sempre estarão disponíveis.

Perante os riscos envolvidos, a AEPD não está convencida da necessidade (tendo em conta as tecnologias disponíveis) nem da mais-valia do recurso a cópias nacionais. Por conseguinte, recomenda que se ponha de parte a possibilidade de os Estados-Membros recorrerem a cópias nacionais.

Todavia, a serem desenvolvidas cópias nacionais, a AEPD recorda que a sua utilização nacional deve pautar-se pelo princípio rigoroso da limitação da finalidade. Na mesma ordem de ideias, as pesquisas na cópia nacional devem obedecer sempre às mesmas modalidades que as pesquisas na base de dados central.

A legalidade do tratamento de dados pessoais baseia-se no estrito respeito pela segurança e integridade dos dados. A AEPD acompanhará estes processos de modo eficaz se puder controlar não apenas a segurança dos dados, mas também a sua integridade mediante a análise dos registos disponíveis. Importa, pois, aditar a «integridade dos dados» ao n.º 6 do artigo 14.º.

9. **COMITOLOGIA**

As propostas prevêem procedimentos de comitologia nalguns casos que exigem decisões tecnológicas para a implementação ou a gestão do SIS II. Por razões semelhantes, afirmou-se no parecer sobre o VIS que estas decisões terão um impacto significativo na correcta aplicação do princípio da finalidade e da proporcionalidade.

A AEPD recomenda que as decisões com impacto substancial na protecção de dados, designadamente o acesso e a introdução de dados, a troca de informações suplementares, a qualidade dos dados a compatibilidade de indicações, o respeito dos requisitos técnicos pelas cópias nacionais, sejam tomadas por via de um regulamento ou uma decisão, de preferência segundo o procedimento de co-decisão ([1]).

([1]) Ver na mesma linha de ideias, o parecer da AEPD sobre o Sistema de Informação sobre Vistos, ponto 3.12 e o parecer da AEPD sobre a proposta de directiva relativa à conservação de dados tratados no contexto do fornecimento de serviços electrónicos de comunicação emitido em 26 de Setembro de 2005, ponto 60.

Em todos os outros casos com impacto na protecção de dados, deve ser dada à AEPD a possibilidade de prestar aconselhamento sobre as escolhas destes comités.

O papel consultivo da AEPD deve ser incluído nos artigos 60.º e 601.º da decisão e no artigo 35.º do regulamento

No caso mais específico das regras técnicas para as ligações entre indicações (artigo 26.º do regulamento e artigo 46.º da decisão), deve ser explicada a necessidade de um comité diferente (consultivo para a decisão e regulamentar para o regulamento).

10. **INTEROPERABILIDADE**

Ainda se aguarda a comunicação da Comissão sobre a interoperabilidade dos sistemas emergentes da UE, o que torna difícil avaliar correctamente a mais-valia das sinergias previstas mas ainda não definidas.

Neste contexto, a AEPD gostaria de remeter para a declaração do Conselho de 25 de Março de 2004 sobre a luta contra o terrorismo que convida a Comissão a apresentar propostas tendentes a aumentar a interoperabilidade e as sinergias entre sistemas de informação (SIS, VIS e Eurodac). Por outro lado, recorda os debates em curso sobre o organismo que poderá ser encarregado da gestão dos diferentes sistemas de grande escala no futuro (ver igualmente ponto 3.8 do presente parecer).

A AEPD já afirmou no seu parecer sobre o Sistema de Informação sobre Vistos que a interoperabilidade é um pré-requisito crítico e vital para a eficiência de sistemas informáticos de grande escala como o SIS II e oferece a possibilidade de reduzir os custos globais de forma coerente e evitar sobreposições naturais de elementos heterogéneos.

— A interoperabilidade pode igualmente contribuir para o objectivo de manter um elevado nível de segurança num espaço sem controlos nas fronteiras internas entre os Estados-Membros através da aplicação do mesmo padrão processual a todos os elementos constitutivos desta política. No entanto, é fundamental distinguir entre dois níveis de interoperabilidade:

  — A interoperabilidade entre Estados-Membros da UE é altamente desejável; com efeito, as indicações enviadas pelas autoridades de um Estado-Membro têm de ser interoperáveis com as enviadas pelas autoridades de outro Estado-Membro.

  — A interoperabilidade entre sistemas concebidos para finalidades diferentes ou com sistemas de países terceiros é bastante mais questionável.

Entre as salvaguardas utilizadas para limitar a finalidade do sistema e evitar a «deformação do sistema», a utilização de diferentes padrões tecnológicas pode contribuir para essa limitação. Além disso, qualquer forma de interacção entre dois sistemas diferentes deverá ser exaustivamente documentada. A interoperabilidade nunca deve levar a uma situação em que uma autoridade não habilitada a aceder ou a utilizar certos dados possa obter esse acesso através de outro sistema de informação. Tanto quanto é possível deduzir da leitura das propostas, parece que nos primeiros anos de funcionamento do SIS II não haverá nenhum Sistema Automático de Identificação Dactiloscópica (AFIS), sendo feito apenas referência a um futuro motor de busca de identificadores biométricos. Caso esteja previsto um cenário que implique o recurso ao AFIS de outros sistemas da UE, tal deve ser claramente documentado, prevendo-se as salvaguardas necessárias para estas sinergias.

A AEPD gostaria de sublinhar mais uma vez que a interoperabilidade dos sistemas não pode ser implementada em violação do princípio da limitação da finalidade e que qualquer proposta sobre esta questão lhe deve ser submetida.

11. **RESUMO DAS CONCLUSÕES**

11.1. **Generalidades**

1. A AEPD congratula-se com vários aspectos positivos destas propostas que nalguns pontos constituem uma melhoria quando comparado com a situação actual. Reconhece que as disposições relativas à protecção de dados foram, de um modo geral, elaboradas com grande cuidado.

2. A AEPD sublinha que, não obstante a sua complexidade, o novo regime legal deve:

   — assegurar um elevado nível de protecção de dados;

   — ser previsível para os cidadãos e para as autoridades que partilham dados;

   — ser coerente na sua aplicação a diferentes contextos (primeiro ou terceiro pilar).

3. Além disso, a introdução de novos elementos no SIS II que aumenta o seu possível impacto na vida das pessoas deve ser acompanhada de salvaguardas mais rigorosas identificadas no parecer. Em especial:

— O acesso aos dados do SIS II só pode ser concedido a novas autoridades mediante justificação da necessidade absoluta. O acesso deve ser tão restrito quanto possível, tanto em termos de dados acessíveis como de pessoas autorizadas.

— A ligação entre indicações nunca deve conduzir, ainda que de forma indirecta, a uma alteração dos direitos de acesso.

— Legislação que não tenha sido aprovada não pode ser considerada uma base válida para inserir dados no SIS II (indicações para a não admissão)

— A base jurídica do acesso por parte de serviços competentes para a emissão dos certificados de matrícula dos veículos deve ser reanalisada visto que se destina principalmente à luta contra a criminalidade.

— A AEPD reconhece que a utilização de dados biométricos é susceptível de melhorar a eficácia do sistema e de ajudar as vítimas de usurpação de identidade. Todavia, afigura-se que o impacto desta inserção não foi estudado com suficiente rigor, sendo sobrestimada a fiabilidade desses dados.

11.2. **Observações específicas**

1. A AEPD congratula-se com o reconhecimento pela Comissão de que o Regulamento (CE) n.º 45/2001 se aplica a todas as actividades de tratamento de dados pela Comissão no âmbito do SIS II uma vez que contribuirá para uma aplicação sistemática e uniforme das regras relativas à protecção das liberdades e dos direitos fundamentais das pessoas no que respeita ao tratamento de dados pessoais

2. A fim de assegurar uma limitação rigorosa da finalidade a nível nacional, a AEPD recomenda que seja introduzida nas propostas relativas ao SIS II (nomeadamente no artigo 21.º da proposta de regulamento e no artigo 40.º da proposta de decisão) uma disposição semelhante à do n.º 4 do artigo 102.º da Convenção de Schengen, que limite a possibilidade de os Estados-Membros preverem uma utilização dos dados que não esteja prevista nos textos do SIS II.

3. O acesso de qualquer autoridade aos dados SIS II deve estar sujeito a regras rigorosas:

— O acesso deve ser compatível com a finalidade genérica do SIS II e conforme com a sua base jurídica.

— A necessidade de acesso aos dados SIS II deve ser demonstrada.

— A utilização que será dada aos dados deve ser definida de modo explícito e restritivo.

— As condições de acesso devem ser bem definidas e restritas. Em especial, deve existir uma lista actualizada de pessoas habilitadas a aceder ao SIS II, também para a Europol e a Eurojust.

— O facto de essas autoridades terem acesso aos dados do SIS II nunca pode servir de justificação para introduzir ou manter dados no sistema que não sejam úteis para a indicação da qual fazem parte.

— O período de conservação dos dados não pode ser alargado se não for necessário para os fins para os quais foram inseridos.

4. Nos casos específicos da Europol e da Eurojust, a AEPD insta a Comissão a definir de modo restritivo as tarefas cuja execução justifica o acesso da Europol e da Eurojust. O acesso da Europol e da Eurojust deve, além disso, ser restrito aos dados relativos a pessoas cujos nomes já constem dos respectivos ficheiros. Recomenda-se igualmente a conceder apenas um ponto de acesso à Europol e à Eurojust.

5. No tocante às indicações relativas à não admissão, insta a Comissão a retirar ou a reformular as disposições baseadas em legislação ainda não adoptada, por forma a que os interessados saibam exactamente quais as medidas que as autoridades podem tomar a seu respeito.

6. Os períodos de conservação dos dados foram alargados sem qualquer justificação plausível. Na ausência de uma justificação convincente, estes períodos deveriam ser reduzidos para a actual duração, em especial no caso das indicações inseridas para efeitos de vigilância discreta ou controlos específicos.

7. Conforme descrito, a Comissão desempenha o papel de responsável pela gestão operacional. Juntamente com as suas importantes funções a nível do desenvolvimento e manutenção do sistema, estas atribuições fazem dela um controlador *sui generis*. Na realidade, desempenha mais as funções de um processador, mais limitadas do que as de um controlador normal, uma vez que a Comissão não tem acesso aos dados tratados no SIS II.

   Nesta perspectiva, convém aditar ao artigo 12.º de ambas as propostas que a Comissão deve propor periodicamente a implementação de novas tecnologias que correspondam ao estado-da-arte neste domínio e que reforcem os níveis de protecção e de segurança dos dados.

8. No tocante ao papel dos Estados-Membros, haverá que clarificar quais as autoridades responsáveis pelo controlo.

9. No tocante à informação do interessado:

   — Na proposta de regulamento, devem ser aditadas algumas informações à lista: o período de conservação dos dados, a existência do direito de pedir um reexame ou um recurso da decisão de emitir uma indicação, a possibilidade de obter assistência da autoridade de protecção de dados e a existência de vias de recursos.

     Além disso, no que diz respeito ao momento em que esta informação é dada, fornecer informações sobre a indicação na decisão que motivou a mesma.

   — Na proposta de decisão, o artigo 50.º deve ser alterado por forma a que o direito à informação não esteja sujeito a um pedido do interessado.

10. É positiva a fixação de prazos de resposta a um pedido de acesso nas propostas. Sempre que na legislação nacional estejam previstos prazos, deve ficar bem claro que se aplicam os prazos mais favoráveis ao interessado.

    Além disso, será útil prever que as autoridades de protecção de dados devem cooperar activamente no exercício do direito de acesso.

11. No que diz respeito ao direito de recurso, a AEPD sugere que se suprima a limitação territorial nos artigos 30.º e 52.º.

12. No tocante aos poderes das autoridades nacionais de protecção de dados:

   — No regulamento: convém ter presente que podem exercer no que respeita ao SIS II todas as competências que lhes são atribuídas por força do artigo 28.º da Directiva 95/46/CE, devendo este facto ser clarificado no texto da proposta.

   — Na proposta de decisão: as autoridades de controlo devem ser dotadas dos mesmos poderes que no regulamento/directiva.

13. No que diz respeito às competências da AEPD: deve poder exercer todas as competências que lhe são atribuídas pelo Regulamento n.º 45/2001, tendo em conta, no entanto, os poderes da Comissão em relação aos dados propriamente ditos.

14. Quanto à coordenação do controlo: As propostas reconhecem igualmente a necessidade de coordenar as actividades de controlo desenvolvidas pelas diferentes autoridades envolvidas. A AEPD congratula-se com o facto de conterem os elementos essenciais para estabelecer a cooperação entre as autoridades responsáveis pelo controlo a nível nacional e europeu. Estas disposições (artigo 31.º da proposta de regulamento e o artigo 53.º da proposta de decisão) poderão contudo beneficiar de algumas clarificações do conteúdo dessa coordenação.

15. Os artigos 10.º e 13.º da proposta incluem diversas medidas relativas à segurança dos dados; a inclusão de disposições relativas ao (auto-) controlo das medidas de segurança é positiva.

   — Todavia, o artigo 59.º da proposta de decisão e o artigo 34.º da proposta de regulamento relativos ao acompanhamento e à avaliação não deveriam cingir-se aos aspectos relacionados com os resultados, a eficácia em termos de custos e a qualidade dos serviços, devendo incidir igualmente sobre requisitos legais, nomeadamente no domínio da protecção de dados. Estas disposições devem ser alteradas em conformidade.

   — Além disso, para completar ao disposto na alínea f) do n.º 1 do artigo 10.º ou no artigo 18.º da proposta de decisão e do artigo 17.º do regulamento, deve ser aditado que os Estados-Membros, a Europol e a Eurojust devem assegurar a disponibilidade de perfis exactos dos utilizadores (aos quais devem ter acesso as autoridades nacionais de controlo para verificação). Para além destes perfis dos utilizadores, deve ser elaborada uma lista exaustiva da identidade dos utilizadores e actualizada permanentemente pelos Estados-Membros. O mesmo se aplica à Comissão.

   — A legalidade do tratamento de dados pessoais baseia-se no estrito respeito pela segurança e integridade dos dados. A AEPD deve poder monitorizar não apenas a segurança dos dados, mas também a sua integridade mediante a análise dos registos disponíveis. Importa, pois, aditar a «integridade dos dados» ao n.º 6 do artigo 14.º.

16. A utilização de cópias nacionais pode acarretar muitos riscos suplementares. A AEPD não está convencida da necessidade (tendo em conta as tecnologias disponíveis) nem da mais-valia do recurso a cópias nacionais. Recomenda que se evite ou, pelo menos, limite rigorosamente a possibilidade de utilização de cópias nacionais pelos Estados-Membros. Todavia, a serem desenvolvidas, a AEPD recorda que a sua utilização nacional deve obedecer ao princípio rigoroso da limitação da finalidade. Do mesmo modo, as pesquisas na cópia nacional devem obedecer sempre às mesmas modalidades que as pesquisas na base de dados central.

17. Quanto à comitologia: as decisões com impacto substancial na protecção de dados devem ser tomadas por via de um regulamento ou uma decisão, de preferência segundo o procedimento de co-decisão. Sempre que se recorre ao procedimento de comitologia, o papel consultivo da AEPD deve ser incluído nos artigos 60.º e 601.º da decisão e no artigo 35.º do regulamento.

18. A interoperabilidade dos sistemas não pode ser implementada em violação do princípio da limitação da finalidade, e que qualquer proposta sobre esta questão deve ser submetida à AEPD.

Feito em Bruxelas, em 19 de Outubro de 2005.

Peter HUSTINX

Autoridade Europeia para a Protecção de Dados