PARECER DA AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS

sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo ao Sistema de informação sobre vistos (VIS) e ao intercâmbio de dados entre os Estados-Membros sobre os vistos de curta duração (COM(2004)835 final)

(2005/C 181/06)

A AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS,

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

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

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

Tendo em conta 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 25 de Janeiro de 2005,

ADOPTOU O SEGUINTE PARECER:

1. INTRODUÇÃO

1.1. Observações preliminares

A criação do Sistema de Informação sobre Vistos (VIS) constitui um importante elemento da política comum de vistos da UE, tendo sido já objecto de vários instrumentos conexos.

— Em Abril de 2003, foi apresentado um estudo de viabilidade [1] sobre o VIS, encomendado pela Comissão.

— Em Setembro de 2003, a Comissão propôs uma alteração [2] ao anterior Regulamento que estabelece um modelo-tipo de visto. O principal objectivo consistia em introduzir dados biométricos (imagem facial e duas impressões digitais) nesse novo modelo de visto. Tais dados biométricos ficariam armazenados numa micropastilha (*microchip*).

[1] Sistema de Informação sobre Vistos, relatório final, encomendado pela CE e realizado por Trasys, abril de 2003.
[2] COM(2003) 558 final, em conjugação com 2003/0217 (CNS) e 2003/0218 (CNS).

— Em Junho de 2004, foi lançado por decisão do Conselho [1] o processo de criação do Sistema de Informação sobre Vistos, proporcionando assim a base jurídica para a sua inclusão no orçamento da UE. A referida decisão propôs o estabelecimento de uma base de dados central que contivesse informações relativas aos pedidos de visto e previu um procedimento de «comitologia» por forma a permitir a gestão do desenvolvimento técnico do VIS.

Em Dezembro de 2004, a Comissão aprovou uma proposta de regulamento relativo ao VIS e ao intercâmbio de dados entre os Estados-Membros sobre os vistos de curta duração [2] (a seguir designado «a proposta»), a qual constitui o objecto do presente parecer. Foi anexado à proposta um estudo de avaliação de impacto exaustiva [3] (a seguir designada «AIE»).

No entanto, tal como referido na exposição de motivos, serão necessários outros instrumentos jurídicos para complementar o presente regulamento, nomeadamente para:

— alterar as Instruções Consulares Comuns sobre vistos destinadas às missões diplomáticas e postos consulares de carreira das Partes Contratantes da Convenção de Schengen (a seguir designadas por «Instruções Consulares Comuns»), na sequência da introdução de dados biométricos nos procedimentos;

— desenvolver um novo mecanismo para o intercâmbio de dados com a Irlanda e o Reino Unido;

— efectuar o intercâmbio de dados sobre vistos de longa duração.

Tal como decidido pelo Conselho (Justiça e Assuntos Internos) de 5-6 de Junho de 2003 e enunciado no n.º 2 do artigo 1.º da Decisão do Conselho de Junho de 2004 acima referida, o VIS baseia-se numa arquitectura centralizada, sendo composto por uma base de dados em que são armazenados os ficheiros relativos aos pedidos de visto, ou seja, o chamado Sistema Central de Informação sobre Vistos (CS-VIS), e por uma Interface Nacional (NI-VIS) nos Estados-Membros. Cada Estado-Membro designará [4] uma autoridade central nacional ligada à Interface Nacional e através da qual as suas autoridades competentes poderão ter acesso ao CS-VIS.

1.2. **Principais elementos da proposta do ponto de vista da protecção de dados**

A proposta tem por objectivo melhorar a administração da política comum de vistos facilitando o intercâmbio de dados entre Estados-Membros mercê da criação de uma base de dados central. O regulamento prevê a introdução de dados biométricos (fotografia e impressões digitais) durante o processo de pedido de visto, e o armazenamento desses dados na base de dados central.

Seria também possível utilizar dados biométricos na vinheta autocolante, tal como a Comissão propõe num regulamento de alteração relativo ao modelo-tipo de visto, mediante a introdução de uma fotografia e impressões digitais, armazenadas numa micropastilha (aguarda-se a decisão do Conselho sobre esta proposta, a tomar com base nos resultados da análise em curso).

A proposta descreve pormenorizadamente as diferentes operações efectuadas com os dados (introdução, alteração, apagamento e consulta) e os diferentes tipos de dados a acrescentar no VIS em função do estatuto do pedido (aceitação, recusa, etc..)

A proposta estipula um período de conservação de cinco anos para os dados relativos a cada pedido.

A proposta enumera de forma restritiva as autoridades competentes que terão acesso ao VIS, além das autoridades responsáveis pelos vistos, que terão acesso ao VIS, e define os direitos de acesso concedidos a essas autoridades, ou seja:

— as autoridades competentes para efectuar o controlo de vistos nas fronteiras externas e dentro do território do Estado-Membro

— as autoridades competentes em matéria de imigração

---

[1] 2004/512/CE, JO L 213 de 15.6.2004, p. 5.
[2] COM(2004)835 final em conjugação 2004/0287 (COD).
[3] Estudo para a Avaliação de Impacto Exaustiva do Sistema de Informação sobre Vistos, Relatório Final EPEC, Dezembro de 2004.
[4] N.º 2 do artigo 24.º da proposta.

— as autoridades competentes em matéria de asilo

Ao descrever o funcionamento do VIS e as correspondentes responsabilidades, a proposta salienta que a Comissão efectua o tratamento dos dados do VIS em nome dos Estados-Membros. Refere ainda a necessidade de utilizar registos das operações de tratamento de dados a fim de garantir a segurança dos dados, e especifica as responsabilidades que incumbem a uns e a outros para assegurar esse nível de segurança.

A proposta contém um capítulo sobre protecção de dados em que é especificado o papel das autoridades nacionais e da Autoridade Europeia para a Protecção de Dados (a seguir designada «AEPD»).

A proposta confia a implementação técnica do VIS e a selecção das tecnologias necessárias ao comité instituído pelo n.º 1 do artigo 5.º do Regulamento (CE) n.º 2424/2001, relativo ao desenvolvimento da segunda geração do Sistema de Informação de Schengen (SIS II).

Vem anexa à proposta uma avaliação de impacto exaustiva encomendada pela Comissão e conduzida pelo EPEC (*European Policy Evaluation Consortium*), em que se conclui que o VIS associado à utilização de dados biométricos constitui actualmente a melhor solução para melhorar a política comum de vistos .

2. **QUADRO PERTINENTE**

A proposta terá um impacto considerável sobre a vida privada e outros direitos fundamentais das pessoas; por conseguinte, é necessário confrontá-la com os princípios relativos à protecção de dados. Expõem-se a seguir os principais pontos de referência para a nossa análise.

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

  Segundo o n.º 2 do artigo 8.º, qualquer ingerência da autoridade pública no exercício deste direito só é permitida se «estiver prevista na lei» e for «necessária» numa «sociedade democrática» para a protecção de interesses importantes. Na jurisprudência do Tribunal Europeu dos Direitos do Homem, estas condições conduziram a requisitos suplementares no que respeita à qualidade da base jurídica para tal ingerência, à proporcionalidade da medida e à necessidade de garantias das adequadas contra os abusos.

  Os princípios fundamentais para a protecção das pessoas no que se refere ao tratamento dos dados pessoais foram desenvolvidos na Convenção para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal, elaborada pelo Conselho da Europa e aprovada em 1981.

— Mais recentemente, o direito ao respeito pela vida privada e a protecção dos dados pessoais foram estabelecidos nos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia, integrada na Parte II da nova Constituição da UE.

  No artigo 52.º da Carta reconhece-se que estes direitos podem estar sujeitos a restrições, desde que estejam reunidas condições semelhantes às aplicáveis nos termos do artigo 8.º da CEDH. Essas condições devem ser tidas em consideração de cada vez que é avaliada uma proposta de eventual ingerência.

Actualmente, na legislação da UE as regras básicas em matéria de protecção de dados estão previstas nos seguintes instrumentos:

— 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). Esta directiva passará a ser citada como «Directiva 95/46/CE». A directiva estabelece em pormenor os princípios face aos quais a proposta vai ser aquilatada, na medida em que se aplique aos Estados-Membros. Trata-se do instrumento mais relevante, uma vez que a proposta será aplicada em combinação com a legislação nacional de implementação da directiva. A eficácia das disposições e garantias propostas dependerá, pois, da eficácia dessa combinação em cada caso particular.

— 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 (JO L 8, p. 1). Este regulamento, que passará a ser citado como «Regulamento (CE) n.º 45/2001», estabelece princípios similares aos da Directiva 95/46/CE, sendo relevante neste contexto na medida em que a proposta se aplique às actividades da Comissão, a par das disposições do regulamento. Por conseguinte, esta combinação também nos merece alguma atenção.

A Directiva 95/46/CE e o Regulamento (CE) n.º 45/2001 devem ser lidos em conjugação com outros instrumentos. Por outras palavras, na medida em que digam respeito ao tratamento de dados pessoais susceptível de violar direitos fundamentais, em especial o direito à vida privada, a directiva e o regulamento deverão ser interpretados à luz dos direitos fundamentais. Tal decorre igualmente da jurisprudência do Tribunal de Justiça Europeu ([1]).

— Por último, a AEPD incluirá também na sua análise o Parecer n.º 7/2004 de 11 de Agosto de 2004 do Grupo da Protecção de Dados (Grupo do artigo 29.º) ([2]), «sobre a inserção de elementos biométricos nos títulos de residência e nos vistos tendo em conta a criação do Sistema de Informação sobre Vistos (VIS)» . Neste parecer, o Grupo manifestou preocupações quanto a vários elementos da proposta. A AEPD tenciona verificar se e de que modo a proposta atendeu a essas preocupações.

3. **ANÁLISE DA PROPOSTA**

3.1. **Generalidades**

A AEPD reconhece que a continuação do desenvolvimento da política comum de vistos exige um intercâmbio eficaz dos dados pertinentes. O VIS é um dos mecanismos que pode assegurar uma grande fluidez no intercâmbio de informações. No entanto, esse novo instrumento deverá limitar-se à recolha e ao intercâmbio de dados, na medida em que tal recolha e tal intercâmbio sejam necessários para o desenvolvimento de uma política comum de vistos e sejam proporcionados a este objectivo.

A criação do VIS poderá ter consequências positivas para outros interesses públicos legítimos, mas isso não altera a finalidade do VIS. A limitação da finalidade do sistema desempenha um papel muito importante na determinação do conteúdo e uso legítimos do sistema, e por conseguinte também na concessão do direito de acesso ao VIS (ou a uma parte dos seus dados) às autoridades dos Estados-Membros que o solicitem por interesses públicos legítimos.

Além disso, a proposta introduz a utilização de dados biométricos no VIS. A AEPD reconhece a vantagem do recurso à biometria, mas salienta que a utilização desse tipo de dados tem um grande impacto, sugerindo portanto a inserção de salvaguardas rigorosas para a utilização dos dados biométricos.

O presente parecer deverá ser lido à luz destas considerações gerais. Refira-se ainda que o presente parecer deveria ser mencionado no preâmbulo do regulamento, antes dos considerandos («Tendo em conta o parecer ….»).

([1]) Neste contexto, é de referir o acórdão do Tribunal de Justiça nos Processos «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) Colect. I-4989). O Tribunal debruçou-se sobre uma lei austríaca que prevê a comunicação ao Tribunal de Contas austríaco de dados relativos aos salários de empregados do sector público, e a subsequente publicação desses dados. Neste acórdão, o Tribunal estabelece uma série de critérios inspirados no artigo 8.º da Convenção Europeia dos Direitos do Homem, critérios esses que deverão ser utilizados ao aplicar a Directiva 95/46/CE na medida em que esta directiva dê margem para certas restrições ao direito à vida privada.

([2]) Trata-se de um grupo consultivo independente, instituído pela Directiva 95/46/CE e composto por representantes das autoridades competentes em matéria de protecção de dados dos Estados-Membros, da AEPD e da Comissão.

3.2. **Finalidade**

A finalidade do VIS tem uma importância crucial, à luz não só do artigo 8.º da CEDH mas também do quadro geral da protecção de dados. O artigo 6.º da Directiva 95/46/CE estipula que os dados pessoais devem ser «recolhidos para finalidades determinadas, explícitas e legítimas, e que não serão posteriormente tratados de forma incompatível com essas finalidades.» . Só uma definição clara das finalidades permitirá uma correcta avaliação da proporcionalidade e adequação do tratamento dos dados pessoais, o que é determinante devido à natureza dos dados (nomeadamente os dados biométricos) e à amplitude da operação de tratamento que se tem em vista.

A finalidade do VIS encontra-se claramente definida no n.º 2 do artigo 1.º da proposta:

> «O VIS melhorará a administração da política comum em matéria de vistos, a cooperação consular e a consulta entre as autoridades consulares centrais ao facilitar o intercâmbio de dados entre Estados-Membros sobre os pedidos de vistos e as decisões relativas aos mesmos».

Por conseguinte, todos os elementos do VIS devem ser instrumentos necessários e proporcionados à consecução deste objectivo político, no interesse da política comum em matéria de vistos.

O n.º 2 do artigo 1.º da proposta enumera também os benefícios obtidos com a melhoria da política de vistos, como por exemplo:

a) Prevenir as ameaças à segurança interna;

b) Facilitar a luta contra a fraude;

c) Facilitar os controlos nos pontos de passagem das fronteiras externas.

A AEPD encara estes elementos como exemplos das consequências positivas da criação do VIS e da melhoria da política comum de vistos, mas não como finalidades autónomas de per si.

Esta visão traz consigo duas consequências principais nesta fase:

— A AEPD tem consciência de que as autoridades de aplicação da lei estão interessadas em ter acesso ao VIS; o Conselho aprovou em 7 de Março de 2005 conclusões nesse sentido. Como o VIS tem por finalidade a melhoria da política comum de vistos, convém observar que a concessão de um acesso de rotina às autoridades de aplicação da lei não seria conforme com esta finalidade. Embora nos termos do artigo 13.º da Directiva 95/46/CE seja possível conceder tal acesso numa base *ad hoc*, em circunstâncias específicas e sob reserva das salvaguardas adequadas, não é permitida a concessão de um acesso sistemático.

  Em termos mais gerais, a avaliação da proporcionalidade e da necessidade é crucial se de futuro forem tomadas decisões quanto a conceder ou não a algumas outras autoridades o acesso ao VIS. As tarefas para as quais o acesso for concedido devem ser consentâneas com as finalidades do VIS.

— A referência explícita à «prevenção das ameaças à segurança interna dos Estados-Membros» na alínea a) é pouco feliz. As principais vantagens do VIS serão a prevenção da fraude e da busca do visto mais fácil, mais conhecida por *visa shopping* (a luta contra a fraude é também a principal razão da inclusão dos dados biométricos no sistema) ([1]). A prevenção das ameaças à segurança deverá, por conseguinte, ser vista como um benefício «secundário», ainda que muito apreciável.

  A AEPD recomenda que seja tornada mais explícita no texto do n.º 2 do artigo 1.º esta distinção entre «finalidade» e «vantagens», por exemplo da seguinte maneira:

  «O VIS tem por finalidade melhorar a administração da política comum em matéria de vistos, a cooperação consular e a consulta entre as autoridades consulares centrais ao facilitar o intercâmbio de dados entre Estados-Membros sobre pedidos de vistos e as decisões relativas aos mesmos. Deste modo, contribuirá igualmente …»

([1]) Na AIE este aspecto vem claramente apontado (p. 6, §2.7).: «*as ineficiências no combate ao* visa shopping *e à fraude e na realização de controlos estão a causar também ineficiências no que se refere à segurança interna dos Estados-Membros*». Tal implica que as ameaças à segurança se devem, em parte, a uma política de vistos ineficaz. Neste contexto, a primeira coisa a fazer é melhorar a política de vistos, principalmente através do combate à fraude e da melhoria dos controlos. Da melhoria da política de vistos resultará a melhoria da segurança.

A este respeito, é também interessante notar que nas «Directrizes para a criação de um sistema comum de intercâmbio de dados relativos aos vistos», aprovadas pelo Conselho JAI em 13 de Junho de 2002 [1], a prevenção das ameaças à segurança interna vem mencionada no final da lista das finalidades. O mesmo se poderia fazer no caso da presente proposta; tal redacção ficaria muito mais consentânea com a finalidade do VIS.

3.3. **Qualidade dos dados**

Nos termos do artigo 6.º da Directiva 95/46/CE, os dados pessoais devem ser também «adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e para que são tratados posteriormente» . Este requisito prende-se com a proporcionalidade do VIS em si mesmo, mas também com os dados a recolher e armazenar no VIS e com a sua posterior utilização, bem como com as salvaguardas suplementares aplicáveis nesse contexto. Estes elementos são igualmente essenciais para a avaliação da proposta à luz do artigo 8.º da CEDH.

A criação do VIS representa incontestavelmente uma considerável interferência no gozo do direito à vida privada, quanto mais não seja pela sua escala e pelas categorias de dados pessoais tratados. Por conseguinte, no seu parecer n.º 7/2004, o Grupo do artigo 29.º declarou que gostaria de saber «em que estudos e estimativas sobre a amplitude e gravidade dos fenómenos em causa são dadas razões imperiosas de segurança ou de ordem pública que justifiquem uma tal abordagem».

A AEPD atentou cuidadosamente nas provas apresentadas na AIE. Embora essas provas não sejam inteiramente concludentes, parece haver razões suficientes para justificar a criação do VIS com a finalidade de melhorar a política comum de vistos.

Neste contexto, pareceria caber dentro da margem de apreciação do legislador decidir sobre a criação do VIS enquanto instrumento destinado a melhorar as condições de emissão dos vistos pelos Estados-Membros. Tal sistema poderia, como tal, enquadrar-se na criação progressiva de um espaço de liberdade, segurança e justiça, tal como previsto no Tratado CE, e constituir mais um passo nesse sentido.

No entanto, a criação e utilização do VIS não poderá nunca levar a que deixe de ser possível assegurar, neste domínio, um elevado nível de protecção dos dados pessoais. Faz parte das funções consultivas da AEPD examinar até que ponto o VIS irá afectar o actual nível de protecção de dados das pessoas em causa.

Posto isto, o parecer da AEPD incidirá principalmente nas seguintes questões:

— a proporcionalidade e adequação dos dados, e a sua utilização (por ex., categorias de dados, acesso aos dados para cada tipo de autoridade interessada, e período de conservação dos dados);

— o funcionamento do sistema (por ex. responsabilidades e segurança);

— os direitos das pessoas em causa (por ex. informação, possibilidade de corrigir ou apagar dados inexactos ou irrelevantes);

— a monitorização e a supervisão do sistema.

Para além dos parágrafos que se seguem, a proposta não suscita comentários importantes no que se refere às categorias de dados a inserir no VIS e à sua utilização. As disposições pertinentes foram redigidas com o devido cuidado e afiguram-se, no seu conjunto, coerentes e adequadas.

---

[1] «Decisão-Quadro do Conselho, de 13 de Junho de 2002, relativa à luta contra o terrorismo (2002/475/JAI)», JO L 164 de 22.6.2002, p. 3.

3.4. **Biometria**

3.4.1. *Impacto da utilização da biometria*

A utilização da biometria nos sistemas de informação nunca é uma escolha sem significado, especialmente quando o sistema em questão diz respeito a um tão grande número de pessoas. A biometria não é apenas mais uma tecnologia da informação. A biometria altera irrevogavelmente a relação entre o corpo e a identidade, na medida em que faz com que as características do corpo humano possam ser «lidas» por uma máquina e ficar sujeitas a um posterior tratamento. Mesmo que as características biométricas não possam ser lidas pelo olho humano, podem ser lidas e utilizadas por instrumentos apropriados, sempre e para onde quer que a pessoa se desloque.

Por mais útil que a biometria possa ser para determinados efeitos, a sua utilização generalizada terá um enorme impacto na sociedade e deverá ser objecto de um debate amplo e aberto. A AEPD não pode deixar de constatar que tal debate não chegou a ter verdadeiramente lugar antes da elaboração da proposta. Este facto sublinha ainda mais a necessidade de prever salvaguardas rigorosas para a utilização dos dados biométricos, e de proceder a uma reflexão cuidada e um debate no decurso do processo legislativo.

3.4.2. *Especificidade dos dados biométricos*

Tal como já foi salientado em vários pareceres do Grupo do artigo 29.º ([1]), a inserção e o tratamento de dados biométricos para efeitos de documentos de identidade deverão ser acompanhados por salvaguardas particularmente sólidas e rigorosas. Com efeito, devido a certas características específicas, os dados biométricos são altamente sensíveis.

É verdade que é praticamente impossível perder os dados biométricos de uma determinada pessoa, ao contrário do que se passa com uma senha ou uma chave. Estes dados oferecem uma *distintividade quase absoluta*, ou seja, a cada pessoa correspondem características biométricas únicas. Estas características mantêm-se praticamente sem alteração ao longo da vida de uma pessoa, o que lhes confere um carácter de *permanência*. Todas as pessoas possuem os mesmos «elementos» físicos, o que dá também às características biométricas uma dimensão de *universalidade*.

Contudo, é quase impossível anular os dados biométricos: um dedo ou um rosto dificilmente se alteram. Esta característica, positiva sob vários pontos de vista, leva a um grave inconveniente no caso da *usurpação de identidade*: o armazenamento numa base de dados de impressões digitais e de uma fotografia associadas a uma identidade usurpada poderá levar a problemas graves e permanentes para o possuidor efectivo dessa identidade. Além disso, mercê da sua própria natureza, os dados biométricos *não são secretos*, e podem mesmo *deixar vestígios* (impressões digitais, ADN), que permitem a recolha destes dados *sem que o seu possuidor disso se aperceba*.

Devido a estes riscos, que são inerentes à natureza das características biométricas, será necessário implementar salvaguardas importantes (especialmente em termos de respeito pelo princípio da limitação da finalidade, de restrição de acesso, e de medidas de segurança).

3.4.3. *Imperfeição técnica das impressões digitais*

As principais vantagens dos dados biométricos acima descritas (universalidade, distintividade, permanência, usabilidade, etc) nunca são absolutas, o que tem um impacto directo sobre a eficiência dos procedimentos previstos no regulamento para o registo e a verificação dos dados biométricos.

Segundo as estimativas efectuadas ([2]), vai até 5 % a percentagem das pessoas que não podem ser registadas (por as suas impressões digitais não serem legíveis, ou por as mesmas nem sequer existirem). A AIE anexa à proposta previu cerca de 20 milhões de requerentes de visto para 2007, o que significa que poderá ir até 1 milhão o número das pessoas que não poderão seguir o processo «normal» de registo, com as consequências que daí advirão para o pedido de visto e o controlo nas fronteiras.

([1]) Parecer 7/2004 sobre a inserção de elementos biométricos nos títulos de residência e nos vistos, tendo em conta a criação do Sistema de Informação sobre Vistos (VIS) (Markt/11487/04/EN — WP 96) e Documento de Trabalho sobre biometria (MARKT/10595/03/EN — WP 80).

([2]) A. Sasse, *Cybertrust and CrimePrevention:Usability and Trust in Information Systems*, em «Foresight cybertrust and crime prevention project». 04/1151, 10 de Junho de 2004, p. 7, e Technology Assessment, «Using Biometrics for Border Security», United States General Accounting Office, GAO-03-174, Novembro de 2002.

A identificação biométrica é também, por definição, um processo estatístico. É normal uma taxa de erro de 0,5 a 1 % ([1]), o que significa que o sistema de controlo nas fronteiras externas terá uma taxa de falsa rejeição situada entre 0,5 e 1 %. Esta taxa é afinada por um limiar baseado na política de risco das autoridades competentes (corresponde a uma proporção estabelecida entre o número de pessoas falsamente rejeitadas e o das falsamente admitidas). Por conseguinte, é exagerado considerar que estas tecnologias proporcionarão uma «identificação exacta» da pessoa em causa, tal como afirmado no 9.º considerando do regulamento proposto.

Segundo um recente estudo de prospecção ([2]) encomendado pelo Comité LIBE do Parlamento Europeu, deverão existir procedimentos de recuperação de falhas (*fallback procedures*) a fim de estabelecer salvaguardas essenciais para a inserção de dados biométricos atendendo a que estes não são nem acessíveis a todos nem completamente exactos. Tais procedimentos deverão ser implementados e utilizados a fim de respeitar a dignidade das pessoas que poderão não ser bem enquadradas no processo de registo e de evitar transferir para essas pessoas o ónus das imperfeições do sistema ([3]).

Por conseguinte, a AEPD recomenda que sejam elaborados e incluídos na proposta procedimentos de recuperação de falhas. Tais procedimentos não deverão diminuir o nível de segurança da política de vistos nem estigmatizar as pessoas com impressões digitais ilegíveis.

3.5. **Categorias específicas de dados**

Certas categorias de dados (além dos dados biométricos) requerem uma atenção especial: dados relativos aos motivos de recusa de visto (3.5.1) e dados relativos aos outros membros de um grupo (3.5.2).

3.5.1. *Motivos de recusa de visto*

O n.º 2 do artigo 10.º da proposta prevê que, sejam incluídos no processo os dados relativos aos motivos de recusa sempre que tenha sido tomada uma decisão de recusa de visto,. Esses motivos de recusa são completamente estandardizados.

— Os dois primeiros motivos, enunciados nas alíneas a) e b), são de carácter principalmente administrativo: não apresentação de documento de viagem válido, ou de documentos válidos que comprovem o objectivo e as condições da estada prevista.

— A alínea c) menciona «um alerta relativo ao requerente para efeitos de recusa de entrada», o que implica uma consulta da base de dados SIS.

— Por último, a alínea d) menciona como motivo de recusa de visto o facto de que o requerente «representa uma ameaça para a ordem pública, a segurança interna, a saúde pública ou as relações internacionais de qualquer um dos Estados-Membros».

([1])

Biometria	Face	Impressões digitais	Íris
FTE % Não registo	n/d	4	7
FNMR % taxas de rejeição	4	2,5	6
FMR1 % taxas de erro de concordância de verificação	10	< 0,01	< 0,001
FMR2 % taxas de erro de concordância de identificação em BD > 1 m (%)	40	0,1	n/a
FMR3 % taxas de erro de concordância de escrutínio em BD =500 (%)	12	< 1	n/a

A. K. Jain et al., *Biometrics: A grand Challenge*, [*Um enorme desafio*] Proceedings of International Conference on Pattern Recognition [Trabalhos da Conferência Internacional sobre Reconhecimento Automático de Padrões], Cambridge, Reino Unido, Agosto de 2004

([2]) *Biometrics at the frontiers: assessing the impact on Society*, [*Biometria nas fronteiras: avaliação do impacto na sociedade*] Fevereiro de 2005, Instituto de Prospectiva Tecnológica, DG Centro Comum de Investigação, CE.

([3]) *Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data*, [*Relatório intercalar sobre a aplicação dos princípios da Convenção 108 à recolha e tratamento de dados biométricos*], Conselho da Europa, 2005., página 11

Todos os motivos de recusa devem ser aplicados com grande cuidado, atendendo às consequências que acarretam para a vida da pessoa em causa. Além disso, alguns deles, nomeadamente os previstos nas alíneas c) e d), levarão ao tratamento de «dados sensíveis» na acepção do artigo 8.º da Directiva 95/46/CE.

A AEPD gostaria de chamar mais especificamente a atenção para a condição relacionada com a saúde pública, que parece ser vaga e implica o tratamento de dados muito sensíveis. De acordo com os comentários a cada artigo anexos à proposta, a menção da ameaça à saúde pública baseia-se na «proposta de regulamento do Conselho que estabelece o código comunitário relativo ao regime de passagem das fronteiras pelas pessoas» (COM (2004)391 final).

A AEPD está ciente de que o critério da «saúde pública» é amplamente utilizado na legislação comunitária relativa à liberdade de circulação das pessoas, e aplicado de forma muito estrita, tal como se pode ver pela Directiva 2004/38/CE do Parlamento Europeu e do Conselho, de 29 de Abril de 2004, relativa ao direito de livre circulação e residência dos cidadãos da União e dos membros das suas famílias no território dos Estados-Membros. O artigo 29.º desta directiva estabelece as condições exigidas para considerar que existe uma ameaça para a saúde pública: «As únicas doenças susceptíveis de justificar medidas restritivas da livre circulação são as doenças com potencial epidémico definidas pelos instrumentos pertinentes da Organização Mundial de Saúde, bem como outras doenças infecciosas ou parasitárias contagiosas, desde que sejam objecto de disposições de protecção aplicáveis aos nacionais do Estado-Membro de acolhimento.»

— No entanto, convém notar que a proposta acima referida não passa, por enquanto, de uma proposta, e que a inclusão, no Regulamento VIS, da condição de não representar uma ameaça para a saúde pública fica sujeita à aprovação do código comunitário.

— Além disso, a ser aprovado, este motivo de recusa de entrada deverá ser interpretado de forma restrita. Com efeito, a proposta de código comunitário baseia-se, por seu turno, na Directiva 2004/38/CE que acabamos de citar.

A AEPD recomenda, por conseguinte, que seja incluída no texto da proposta uma referência ao artigo 29.º da Directiva 2004/38/CE a fim de assegurar que a expressão «ameaça para a saúde pública» seja entendida à luz dessa disposição. De qualquer modo, atendendo à sensibilidade dos dados, estes só deverão ser tratados se a ameaça para a saúde pública for real, actual e suficientemente grave.

3.5.2. *Dados sobre outros membros de um grupo*

O ponto 7 do artigo 2.º define os «membros do grupo» como «os outros requerentes com os quais o requerente viaja, incluindo o cônjuge e os filhos que o acompanham». O comentário aos artigos menciona que as definições contidas no artigo 2.º da proposta se referem ao Tratado ou ao acervo de Schengen em matéria de política de vistos, com excepção de alguns termos, nomeadamente «membros do grupo», que são especificamente definidos para efeitos do presente regulamento. Por conseguinte, pode-se partir do princípio que esta definição não se refere à definição de «visto colectivo» dada no ponto 2.1.4 das Instruções Consulares Comuns. O comentário aos artigos refere-se a «requerentes que viajam em grupo com outros requerentes, por exemplo no âmbito de um acordo EDA, ou juntamente com familiares».

A AEPD salienta que é necessário dar uma definição precisa e abrangente de «membros do grupo» no regulamento. Na actual versão da proposta, devido ao facto de não haver uma referência precisa ao Tratado ou ao acervo de Schengen, forçoso nos é constatar que a definição é demasiado vaga. De acordo com esta formulação, «membros do grupo» poderia abranger colegas, outros clientes da mesma agência de viagens que participassem numa viagem organizada, etc. As consequências são, efectivamente, muito importantes:

nos termos do artigo 5.º do projecto de regulamento, o processo de requerimento de um requerente ficará ligado aos processos de requerimento dos outros membros do grupo.

3.6. **Conservação dos dados**

O artigo 20.º do projecto de regulamento prevê um período de conservação de cinco anos para cada processo de requerimento de visto. A determinação de um prazo razoável é uma opção política que compete ao legislador comunitário.

Não existem elementos — sobretudo se atendermos às razões mencionadas no comentário aos artigos — que apontem para a conclusão de que a opção política adoptada na presente proposta é pouco razoável ou susceptível de trazer consigo consequências inaceitáveis, desde que tenham sido estabelecidos todos os mecanismos de correcção apropriados. Isto significa que se deve assegurar a possibilidade de corrigir ou apagar os dados a partir do momento em que estes deixem de estar exactos, e em particular a partir do momento em que uma pessoa tenha adquirido a nacionalidade de um Estado-Membro, ou tenha adquirido um estatuto que já não requeira a sua inclusão no sistema.

Além disso, enquanto estiverem incluídos no sistema, os dados não podem de forma alguma condicionar uma nova decisão. Alguns motivos de recusa (alerta sobre o requerente para efeitos de recusa de entrada e, em particular, ameaça para a saúde pública) têm uma validade temporal limitada. O facto de terem constituído motivos válidos para recusar a entrada em determinado momento não deverá influenciar uma nova decisão. A situação deverá ser inteiramente reexaminada de cada vez que for apresentado um novo pedido de visto, devendo esta obrigação ser explicitada no regulamento, conforme adequado.

3.7. **Acesso aos dados e sua utilização**

3.7.1. *Observações preliminares*

A título de observação preliminar, a AEPD reconhece o manifesto cuidado posto no sistema que regula o acesso aos dados do VIS e a utilização desses dados. Cada autoridade tem acesso a diferentes dados para diferentes efeitos. É uma abordagem acertada, que a AEPD não pode senão encorajar. As observações que se seguem têm por fito aplicar essa abordagem da forma mais completa possível.

3.7.2. *Controlos dos vistos nos pontos de passagem controlo das fronteiras externas e dentro do território*

No caso dos controlos de vistos nas fronteiras externas, o artigo 16.º do regulamento proposto enuncia com clareza duas finalidades precisas:

— «verificar a identidade da pessoa», o que significa, segundo a definição dada, proceder a uma comparação «um por um»;

— «verificar a autenticidade do visto». Tal como proposto nas normas da ICAO, a micropastilha do visto poderá utilizar um sistema de chave pública/privada (PKI) para conduzir este processo de autenticação.

Estas duas finalidades podem perfeitamente ser alcançadas se as autoridades competentes para realizar os controlos dos vistos tiverem apenas acesso à micropastilha protegida. Um acesso à base de dados central do VIS seria, por conseguinte, desproporcionada neste caso específico. Esta última opção levaria a que houvesse um maior número de autoridades ligadas ao VIS, o que poderia aumentar o risco de utilização abusiva. Poderia também ser uma opção mais dispendiosa, uma vez que aumentariam também significativamente as necessidades em termos de acesso securizado e controlado ao VIS e de formação especificamente relacionada com esse acesso.

Além disso, a AEPD tem dúvidas quanto à conveniência do acesso aos dados tal como previsto no n.º 2 do artigo 16.º. Com efeito, a alínea a) do n.º 2 estipula que, se uma primeira pesquisa revelar que o VIS contém dados relativos ao requerente, (o que em princípio deveria ser o caso), a autoridade competente pode consultar outros dados, mais uma vez para efeitos de verificação da identidade. Esses dados dizem respeito a todas as informações relativas ao pedido, bem como a fotografias, a impressões digitais e a qualquer visto anteriormente emitido, anulado, revogado ou prorrogado.

Se a verificação da identidade já tiver dado resultado, não é de modo algum evidente a razão pela qual continuam a ser necessários os restantes dados. Estes últimos só deveriam estar verdadeiramente acessíveis, e em condições restritivas, no caso de os procedimentos de verificação terem falhado. Nesse caso, os dados mencionados no n.º 2 do artigo 16.º contribuirão adequadamente para um procedimento de recuperação de falhas (*fallback procedure*) ajudando a apurar a identidade da pessoa em causa. O acesso a esses dados não deveria, pois, ser facultado ao pessoal de cada um dos pontos de controlo das fronteiras, mas ser apenas concedido, de forma mais restritiva, aos funcionários incumbidos de casos difíceis.

Por último, é necessário precisar melhor a definição de «autoridades autorizadas a efectuar pesquisas». Em particular, não se esclarece o que são «as autoridades competentes para efectuar controlos no território do Estado-Membro». A AEPD parte do princípio de que se trata das autoridades competentes para efectuar os controlos dos *vistos,* e considera que o artigo 16.º deverá ser alterado neste sentido.

3.7.3. *Utilização dos dados para efeitos de identificação e regresso de imigrantes clandestinos, e para efeitos dos procedimentos de asilo*

Nos casos descritos nos artigos 17.º, 18.º e 19.º (regresso de imigrantes clandestinos e procedimentos de asilo), o VIS é utilizado para efeitos de identificação. Entre os dados que podem ser utilizados para efeitos de identificação contam-se as fotografias. No entanto, no estado actual da tecnologia relacionada com o reconhecimento facial automatizado para sistemas TI de tão grande escala, as fotografias não podem ser utilizadas para efeitos de identificação (um para muitos); não permitem obter um resultado fiável. Não devem, pois, ser consideradas como dados adequados para efeitos de identificação.

Por conseguinte, a AEPD aconselha vivamente que as «fotografias» sejam retiradas da primeira parte destes artigos e mantidas na segunda parte (as fotografias podem ser utilizadas como instrumento para verificar a identidade de alguém, mas não para identificar numa base de dados de grande escala).

Outra possibilidade seria alterar o artigo 36.º no sentido de as funcionalidades relativas ao tratamento das fotografias para efeitos de identificação só serem implementadas quando esta tecnologia for considerada fiável (eventualmente após o parecer de um comité técnico).

3.7.4. *Publicação das autoridades às quais é facultado o acesso*

O artigo 4.º do projecto de regulamento prevê que seja publicada no Jornal Oficial da União Europeia a lista das autoridades competentes, designadas em cada Estado-Membro, às quais será facultado o acesso ao VIS. Esta publicação deveria ser feita com uma periodicidade regular (anual), de modo a manter a informação actualizada em caso de mudanças de situação a nível nacional. A AEPD salienta a importância desta publicação enquanto instrumento de controlo indispensável, tanto a nível europeu como a nível nacional e local.

3.8. **Responsabilidades**

Recorde-se que o VIS se vai basear numa arquitectura centralizada, com uma base de dados central em que serão armazenadas todas as informações sobre os vistos, e interfaces nacionais localizadas nos Estados-Membros que possibilitam às autoridades competentes nacionais o acesso a esse sistema central. Segundo os considerandos 14.º e 15.º do projecto de regulamento, a Directiva 95/46/CE é aplicável ao tratamento dos dados pessoais pelos Estados-Membros para efeitos do presente regulamento, e o Regulamento (CE) n.º 45/2001 é aplicável às actividades da Comissão ligadas à protecção de dados. Tal como referido em ambos os considerandos neste contexto, a proposta visa clarificar certos pontos, nomeadamente no que respeita à responsabilidade pela utilização dos dados e ao controlo da protecção de dados.

Na realidade, esses pontos parecem estar relacionados com alguns aspectos fundamentais sem os quais o sistema de salvaguardas previsto na Directiva 95/46/CE e no Regulamento (CE) n.º 45/2001 não seria aplicável ou não estaria plenamente em conformidade com a proposta. A aplicabilidade da lei nacional ao abrigo da Directiva pressupõe normalmente que haja um responsável pelo tratamento estabelecido nesse Estado-Membro (artigo 4.º), ao passo que a aplicabilidade do Regulamento depende do tratamento dos dados pessoais por uma instituição ou organismo da Comunidade no exercício de actividades total ou parcialmente abrangidas pelo âmbito de aplicação do direito comunitário (artigo 3.º).

Nos termos do n.º 2 do artigo 23.º do projecto de regulamento, os dados serão «tratados pelo VIS em nome dos Estados-Membros». Nos termos do n.º 3 do artigo 23.º, os Estados-Membros designarão a autoridade que será considerada como responsável pelo tratamento em conformidade com a alínea d) do artigo 2.º da Directiva 95/46/CE. Esta disposição parece querer dizer que, de acordo com o sistema da Directiva, a Comissão deverá ser considerada como subcontratante. Esta interpretação é confirmada pelo comentário aos artigos ([1]).

Tal formulação tende a subestimar o papel importantíssimo — e na realidade crucial — da Comissão, tanto na fase de desenvolvimento do sistema como no decurso do seu funcionamento normal. É difícil associar exactamente o papel da Comissão ao conceito de responsável pelo tratamento ou de subcontratante; trata-se quer de um subcontratante com poderes pouco usuais (entre os quais o que se prende com a concepção do sistema), quer de um responsável pelo tratamento com restrições (uma vez que os dados são introduzidos e utilizados pelos Estados-Membros). A Comissão desempenha realmente no VIS um papel que não pode deixar de ser reconhecido como *sui generis* ([2]).

Este significativo papel deverá ser reconhecido através de uma descrição completa das tarefas da Comissão, e não através de uma redacção que não corresponde exactamente à realidade, por ser demasiado restritiva, não adianta nada para o funcionamento do VIS e apenas serve para gerar confusão. Importa referi-lo também atendendo à necessidade de assegurar a coerência e a eficácia da supervisão do VIS (ver igualmente ponto 3.11). Por conseguinte, a AEPD recomenda que se suprima o n.º 2 do artigo 23.º.

A AEPD gostaria de salientar que a descrição completa das tarefas da Comissão no que respeita ao VIS será ainda mais importante se a Comissão decidir confiar as tarefas de gestão a outro organismo. Na «Ficha Financeira» anexa à proposta é aventada a possibilidade de uma transferência dessas tarefas para a Agência Europeia de Gestão da Cooperação Operacional nas Fronteiras Externas. Neste contexto, é essencial que a Comissão não deixe pairar qualquer incerteza quanto ao âmbito das suas competências, por forma a que o seu sucessor conheça bem os limites do seu campo de actuação.

3.9. **Segurança**

A gestão e a observância de um nível máximo de segurança no âmbito do VIS constitui uma condição prévia para assegurar a devida protecção dos dados pessoais armazenados na sua base de dados. A fim de obter esse nível de protecção satisfatório, é necessário implementar as devidas salvaguardas, de modo a poder enfrentar os potenciais riscos relacionados com a infra-estrutura do sistema e as pessoas envolvidas. Este aspecto, é debatido em várias partes da proposta e merece ser melhorado.

Os artigos 25.º e 26.º da proposta contêm várias medidas relativas à segurança dos dados e especificam os tipos de utilizações abusivas que é necessário impedir. Estas disposições poderiam, contudo, ser utilmente completadas por medidas destinadas a assegurar um acompanhamento e informação sistemáticos sobre a eficácia das medidas de segurança anteriormente mencionadas. Mais especificamente, a AEPD recomenda que sejam aditadas nestes artigos disposições relativas a uma (auto-)auditoria das medidas de segurança.

Esta recomendação está relacionada com o artigo 40.º da proposta, relativo à monitorização e avaliação. Tal deverá abranger não só os aspectos relacionados com os resultados, a relação custo-eficácia e a qualidade dos serviços, mas também a observância dos requisitos legais, em especial no domínio da protecção de dados. A AEPD recomenda, portanto, que o âmbito de aplicação do artigo 40.º seja alargado à monitorização e apresentação de relatórios sobre a legalidade do tratamento.

Além disso, em complemento da alínea c) do n.º 4 do artigo 24.º e da alínea e) do n.º 2 do artigo 26.º referentes ao pessoal devidamente autorizado a ter acesso aos dados, haverá que acrescentar que os Estados-Membros deverão assegurar a existência de perfis do utilizador definidos com precisão (que deverão ser mantidos ao dispor das autoridades nacionais de controlo para efeitos de verificação). Para além destes perfis do utilizador, os Estados-Membros deverão elaborar e manter permanentemente actualizada uma lista completa das identidades dos utilizadores. O mesmo se aplica à Comissão: a alínea b) do n.º 2 do artigo 25.º deverá, pois, ser completada no mesmo sentido.

([1]) Ver página 40 da proposta.

([2]) Apesar de a definição de responsável pelo tratamento na Directiva 95/46/EC e no Regulamento (CE) n.º 45/2001 também prever a possibilidade de existirem mais responsáveis pelo tratamento com responsabilidades diferentes.

Estas medidas de segurança são completadas por salvaguardas em matéria de monitorização e de organização. O artigo 28.º da proposta descreve as condições e as finalidades a ter em conta para determinar a obrigação de manter registos de todas as operações de tratamento de dados. Tais registos serão mantidos não só para controlar a protecção dos dados e garantir a segurança dos mesmos mas também para realizar periodicamente uma auto-auditoria do VIS. Os relatórios de auto-auditoria ajudarão as autoridades de controlo a executar eficazmente as suas tarefas, permitindo-lhes detectar os pontos fracos e centrar a sua atenção nesses pontos quando procederem elas próprias à auditoria.

3.10. **Direitos da pessoa em causa**

3.10.1. *Informação da pessoa em causa*

O fornecimento de informações à pessoa em causa é da maior importância para assegurar um tratamento leal dos dados e constitui uma garantia indispensável dos direitos da pessoa. O artigo 30.º da proposta segue, no essencial, o artigo 10.º da Directiva 95/46/CE.

Esta disposição poderia, no entanto, beneficiar de algumas alterações destinadas a enquadrá-la melhor no âmbito do VIS. A referida directiva prevê, com efeito, que sejam fornecidas certas informações, mas dá margem a que sejam facultadas mais informações, se necessário ([1]). Por conseguinte, o artigo 30.º deverá ser alterado por forma a incluir os seguintes elementos:

— As pessoas em causa deverão ser também informadas sobre o período de conservação aplicável aos dados que lhes dizem respeito.

— A alínea e) do n.º 1 do artigo 30.º menciona «a existência do direito de acesso aos dados relativos à pessoa em questão e do direito de rectificação desses dados». Deveria ser mais preciso e mencionar «o direito de acesso, e o direito de *solicitar a* rectificação *ou o apagamento* desses dados». A este respeito, as pessoas em causa deverão ser informadas da possibilidade de solicitar aconselhamento ou assistência às autoridades de controlo pertinentes.

— Por último, a alínea a) do n.º 1 do artigo 30.º menciona a informação sobre a identidade do responsável pelo tratamento e do seu eventual representante. Atendendo a que o responsável pelo tratamento está sempre estabelecido no território da União Europeia, não há necessidade de prever esta última eventualidade.

3.10.2. *Direitos de acesso, de rectificação e de apagamento*

A última frase do n.º 1 do artigo 31.º estipula que «este acesso aos dados só pode ser concedido por um Estado-Membro». Pode deduzir-se que tal significa que o acesso aos dados ou a sua comunicação não podem ser concedidos pela Unidade Central, mas por qualquer Estado-Membro. A AEPD recomenda que se refira explicitamente que tal comunicação pode ser solicitada em qualquer Estado-Membro.

Além disso, a redacção desta disposição parece implicar igualmente que o acesso não pode ser negado, e será dado sem autorização do Estado-Membro responsável. Isto explicaria a razão de as autoridades nacionais terem de cooperar para aplicar os direitos previstos nos n.ºs 2, 3 e 4 do artigo 21.º mas não no n.º 1 do mesmo artigo ([2]).

3.10.3. *Assistência pelas autoridades de controlo*

O n.º 2 do artigo 33.º estipula que a obrigação das autoridades nacionais de controlo de assistirem e aconselharem a pessoa em causa subsistirá durante todo o processo (perante o tribunal). O significado deste número não é claro. As autoridades nacionais de controlo têm atitudes diferentes em relação ao seu papel durante o processo judicial. Isto soa como se tivessem de desempenhar um papel de conselheiro do queixoso no tribunal, o que em muitos países não é possível.

([1]) Com efeito, menciona *«outras informações (…) desde que sejam necessárias, tendo em conta as circunstâncias específicas da recolha dos dados, para garantir à pessoa em causa um tratamento leal dos mesmos»*.

([2]) Por conseguinte, o n.º 3 do artigo 31.º relativo à cooperação entre as autoridades nacionais no exercício dos direitos de rectificação ou de apagamento poderia ser alterado neste sentido, por uma questão de clareza: «*Se o pedido, tal como previsto no n.º 2 do artigo 31.º*». Os pedidos previstos no n.º 1 do artigo 31.º (Acesso) não implicam cooperação entre autoridades.

3.11. **Controlo**

Esta proposta prevê a partilha da função de controlo entre as autoridades nacionais de controlo e a AEPD, o que é compatível com a abordagem que a proposta faz da legislação aplicável e das responsabilidades pela operação e utilização do VIS e com a necessidade de um controlo eficaz. A AEPD congratula-se pois com esta abordagem prevista nos artigos 34.º e 35.º.

As autoridades nacionais de controlo verificam a legalidade do tratamento de dados pessoais pelos Estados-Membros, *incluindo a respectiva transmissão para e do VIS*. A AEPD controla as actividades da Comissão (…) *incluindo a legalidade da transmissão dos dados pessoais entre as Interfaces Nacionais e o Sistema Central de Informação sobre os Vistos*. Isto poderá resultar em sobreposição, uma vez que tanto as autoridades de controlo como a AEPD são ao mesmo tempo responsáveis pelo controlo da legalidade da transmissão de dados entre as interfaces nacionais e o Sistema Central de Informação sobre os Vistos.

A AEPD sugere portanto uma alteração do artigo 34.º a fim de esclarecer que as autoridades nacionais de controlo verificam a legalidade do tratamento dos dados pessoais pelo Estado-Membro, incluindo a sua transmissão para e das Interfaces Nacionais do VIS.

Quanto ao controlo do VIS, importa igualmente salientar que as actividades de controlo das autoridades nacionais de controlo e da AEPD deverão em certa medida ser coordenadas, para garantir um nível suficiente de coerência e de eficácia global. Existe, de facto, a necessidade de uma implementação harmonizada do regulamento, e de trabalhar em prol de uma abordagem comum de problemas comuns. Além disso, no que diz respeito à segurança, convém acrescentar que o nível de segurança do VIS será — em última análise — determinado pelo nível de segurança do seu elo mais fraco. A este respeito, também a cooperação entre a AEPD e as autoridades nacionais tem de ser estruturada e reforçada. O artigo 35.º deverá assim conter uma disposição nesse sentido, que preveja que a AEPD convocará uma reunião com todas as autoridades nacionais de controlo, pelo menos uma vez por ano.

3.12. **Implementação**

O n.º 2 da proposta prevê: «As medidas necessárias à implementação técnica das funcionalidades referidas no n.º 1 serão adoptadas em conformidade com o procedimento previsto no n.º 2 do artigo 39.º.» O artigo 39.º faz referência a um comité que deverá assistir a Comissão, que foi criado em Dezembro de 2001 ([1]) e tem sido utilizado em diversos instrumentos.

A implementação técnica das funcionalidades do VIS (interacções com as autoridades competentes e formato uniforme dos vistos) apresenta alguns impactos críticos potenciais na protecção dos dados. Por exemplo, as escolhas quanto a implantar ou não uma micropastilha no visto que terá impacto na forma como a base de dados central será usada, bem como o padrão do formato usado para intercambiar os dados biométricos orientarão ou delinearão a correspondente política de protecção de dados ([2]).

Esta selecção de tecnologias terá um impacto determinante na correcta implementação dos princípios da finalidade e da proporcionalidade, e deverá por conseguinte ser controlada. Assim sendo, as escolhas tecnológicas com impacto significativo na protecção dos dados deverão ser feitas de preferência através de um regulamento, segundo o procedimento de co-decisão. Só então poderá ser dado o necessário controlo político. Em todos os outros casos com impacto na protecção dos dados, deverá ser dada à AEPD a possibilidade de prestar aconselhamento sobre as escolhas feitas por este comité.

3.13. **Interoperabilidade**

A interoperabilidade é um pré-requisito crítico e vital para a eficiência de sistemas informáticos de grande escala como o VIS, 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 uma política comum de vistos através da implementação do mesmo padrão processual a todos os elementos constitutivos desta política. No entanto, é fundamental distinguir entre dois níveis de interoperabilidade:

— a interoperabilidade entre os Estados-Membros da UE é altamente desejável; com efeito, os pedidos de visto enviados pelas autoridades de um Estado-Membro têm de ser interoperáveis com os que são enviadas por qualquer das autoridades de outro Estado-Membro.

([1]) Regulamento (CE) n.º 2424/2001 do Conselho, de 6 de Dezembro de 2001 relativo ao desenvolvimento da segunda geração do Sistema de Informação de Schengen (SIS II).

([2]) A proposta de regulamento do Conselho que altera o Regulamento (CE) n.º 1683/95 (formato uniforme para os vistos) também incluía um artigo semelhante.

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

Entre as salvaguardas disponíveis utilizadas para limitar a finalidade do sistema e prevenir a «deformação do sistema», a utilização de diferentes padrões tecnológicos pode contribuir para essa limitação. Além disso, qualquer forma de interacção entre dois sistemas diferentes deverá ser exaustivamente documentada. A interoperabilidade nunca deverá levar a uma situação em que uma autoridade não habilitada a aceder a certos dados ou a fazer uso deles possa obter esse acesso através de outro sistema de informação.

Neste contexto, a AEPD gostaria de remeter para a Declaração do Conselho de 25 de Março de 2004 relativa à Luta contra o Terrorismo, na qual se solicita à Comissão que apresente propostas destinadas a reforçar a interoperabilidade e as sinergias entre os sistemas de informação (SIS, VIS e Eurodac).

A AEPD gostaria ainda de remeter para o debate em curso sobre qual o organismo a quem poderia ser confiada a gestão dos diferentes sistemas de grande escala no futuro (ver igualmente ponto 3.8 do parecer).

A AEPD gostaria de destacar 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 deverá ser submetida.

4. **CONCLUSÕES**

4.1. **Tópicos gerais**

1. A AEPD reconhece que os progressos no desenvolvimento de uma política de vistos requer um intercâmbio eficaz de dados pertinentes. Um dos mecanismos que pode garantir um fluxo regular de informação é o VIS. A AEPD tomou cuidadosamente nota das provas apresentadas na AIE. Embora essas provas não sejam inteiramente concludentes, parece haver razões suficientes para justificar a criação do VIS com o propósito de aperfeiçoar a política comum de vistos.

   No entanto, este novo instrumento deverá ser limitado à recolha e ao intercâmbio de dados, na medida em que essa recolha ou intercâmbio seja necessário para o desenvolvimento de uma política comum de vistos e seja proporcional a este objectivo.

2. A criação do VIS pode ter consequências positivas para outros interesses públicos legítimos, mas tal não altera a sua finalidade. Por conseguinte, todos os elementos do VIS têm de ser instrumentos necessários e proporcionados para atingir o objectivo político atrás referido. Além disso:

   — O acesso de rotina pelas autoridades de aplicação da lei não estaria de acordo com essa finalidade.

   — A AEPD recomenda que esta distinção entre «finalidade» e «benefícios» seja melhor explicitada no texto do n.º 2 do artigo 1.º.

   — A interoperabilidade com outros sistemas não pode ser implementada em violação do princípio de limitação da finalidade.

3. A AEPD reconhece as vantagens da utilização da biometria, mas destaca o considerável impacto da utilização de tais dados e sugere a inserção de salvaguardas rigorosas para a utilização de dados biométricos. Além disso, a imperfeição técnica das impressões digitais requer o desenvolvimento de procedimentos de recuperação de folhas e a sua inclusão nesta proposta.

4. O presente parecer deverá ser referido no preâmbulo do regulamento antes dos considerandos («Tendo em conta o parecer …»).

4.2. **Tópicos específicos**

5. No que diz respeito aos motivos de recusa do visto: deverá ser incluído no texto da proposta uma referência ao artigo 29.º da Directiva 2004/58/CE, para assegurar que uma «ameaça à saúde pública» é entendida à luz dessa disposição.

6. Os dados relativos aos membros de um grupo têm um significado especial na proposta: deverá portanto ser dada uma definição precisa e exaustiva de «membros do grupo».

7. Não há provas de que a escolha política efectuada nesta proposta quanto ao prazo relativo à retenção dos dados não seja razoável ou venha a ter consequências inaceitáveis, desde que todos os mecanismos de correcção adequados estejam a funcionar.

   Além disso, deverá ser explicitado na proposta que os dados pessoais têm de ser inteiramente reavaliados para cada novo pedido de visto.

8. No que diz respeito aos controlos de vistos nas fronteiras externas: o artigo 16.º da proposta deverá ser alterado uma vez que o acesso à base de dados central do VIS seria nestes casos desproporcionada. O acesso apenas à micropastilha protegida, pelas autoridades competentes para a realização dos controlos de vistos, é suficiente.

   Além disso, se a verificação da identidade tiver sido bem sucedida, não é de todo claro que os restantes dados sejam ainda necessários.

9. No que diz respeito à utilização dos dados para efeitos de identificação e regresso dos imigrantes clandestinos, e para os procedimentos de asilo: o termo «fotografias» deverá ser suprimido da primeira parte dos artigos 17.º, 18.º e 19.º e mantido na segunda parte.

10. No que diz respeito às responsabilidades da Comissão e dos Estados-Membros: o n.º 2 do artigo 23.º deverá ser suprimido.

11. Deverão ser aditadas à proposta disposições sobre (auto-) auditoria permanente das medidas de segurança. O âmbito do artigo 40.º deverá ser alargado à monitorização e à avaliação da legalidade do tratamento. Além disso:

   — Tem de ser elaborada e mantida permanentemente actualizada pelos Estados-Membros uma lista completa das identidades dos utilizadores. O mesmo vale para a Comissão: a alínea b) do n.º 2 do artigo 22.º deverá pois ser completada no mesmo sentido.

   — O artigo 28.º da proposta descreve as condições e os fins que obrigam a que sejam mantidos registos de todas as operações de tratamento de dados. Tais registos não serão apenas armazenados para monitorização do controlo dos dados e garantia da sua segurança mas também para a realização de auto-auditorias periódicas do VIS.

12. No que diz respeito aos direitos da pessoa em causa:

   — O artigo 30.º deverá ser alterado para assegurar que as pessoas em causa sejam igualmente informadas sobre o período de retenção aplicável aos seus dados.

   — A alínea e) do n.º 1 do artigo 30.º deverá referir «o direito de acesso e o direito de rectificação ou supressão desses dados».

   — O n.º 1 do artigo 31.º deve explicitar que certas comunicações podem ser solicitadas em qualquer Estado-Membro.

13. No que diz respeito ao controlo:

— O artigo 34.º deverá ser alterado a fim de deixar claro que as autoridades nacionais de controlo supervisionam a legalidade do tratamento dos dados pessoais pelo Estado-Membro, incluindo a sua transmissão para e da Interface Nacional do VIS.

— O artigo 35.º deverá assim conter uma disposição que estipule que a AEPD convocará uma reunião com todas as autoridades nacionais de controlo pelo menos uma vez por ano.

14. No que diz respeito à implementação:

— As escolhas tecnológicas com impacto significativo na protecção de dados deverão de preferência ser feitas através de regulamento, segundo o procedimento de co-decisão.

— Nos outros casos, deverá ser dada a possibilidade à AEPD de prestar aconselhamento sobre as escolhas feitas pelo comité previstas na proposta.

Feito em Bruxelas, em 23 de Março de 2005.

Peter HUSTINX

Autoridade Europeia para a Protecção de Dados