Parecer 11/2024 sobre a utilização do reconhecimento facial para racionalizar o fluxo de passageiros nos aeroportos (compatibilidade com o artigo 5.º, n.º 1, alíneas e) e f), e os artigos 25.º e 32.º do RGPD)

Versão 1.1

Adotado em 23 de maio de 2024

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Adotado

Versão 1.1	28 de maio de 2024	Correção gramatical no resumo (páginas 3 e 4) e nos n.os 77 e 90 do parecer
Versão 1.0	23 de maio de 2024	Adoção do parecer

Resumo

A autoridade de controlo francesa solicitou ao Comité Europeu para a Proteção de Dados que emitisse um parecer sobre a utilização da tecnologia de reconhecimento facial pelos operadores aeroportuários e companhias aéreas para a autenticação ou identificação de passageiros com base na biometria, a fim de racionalizar o fluxo de passageiros nos aeroportos.

A título preliminar, o Comité recorda que a utilização de dados biométricos e, em especial, da tecnologia de reconhecimento facial implica riscos acrescidos para os direitos e liberdades dos titulares dos dados. Está relacionada com o tratamento de dados biométricos, aos quais é concedida proteção especial ao abrigo do artigo 9.º do RGPD. Antes de utilizarem essas tecnologias, mesmo que sejam consideradas particularmente eficazes, os responsáveis pelo tratamento devem avaliar o impacto nos direitos e liberdades fundamentais dos titulares dos dados e ponderar se podem utilizar meios menos intrusivos para alcançar a finalidade legítima do tratamento que efetuam.

O âmbito do presente parecer, de acordo com o pedido, limita-se à compatibilidade do tratamento com o **artigo 5.º, n.º 1, alíneas e) e f), e os artigos 25.º e 32.º do RGPD**, com a **finalidade específica de racionalizar o fluxo de passageiros nos aeroportos** em quatro pontos de controlo específicos, a saber, os pontos de controlo de segurança, os locais de entrega de bagagem, o embarque e o acesso às salas de espera. O presente parecer não inclui uma análise total e completa do cumprimento do RGPD por parte do responsável ou responsáveis pelo tratamento em questão em cada caso, bem como por parte do(s) seu(s) subcontratante(s), se for caso disso. Por conseguinte, o presente parecer não prejudica uma análise jurídica e técnica caso a caso baseada no tratamento previsto e nas circunstâncias de um determinado responsável pelo tratamento. Além disso, a análise da base jurídica aplicável não se enquadra no âmbito das questões submetidas ao Comité no pedido, pelo que o presente parecer não examina a validade do consentimento para esse tratamento, em conformidade com os artigos 6.º, 7.º e 9.º do RGPD. Ademais, o presente parecer não prejudica as restrições à utilização de dados biométricos previstas no direito dos Estados-Membros.

No presente parecer, o Comité avalia a conformidade do tratamento com as disposições do RGPD acima referidas no contexto de **quatro cenários específicos**.

O **primeiro cenário** implica o armazenamento de um modelo biométrico inscrito na posse da pessoa singular, por exemplo, no seu dispositivo individual, sob o seu controlo exclusivo, a fim de autenticar (comparação 1:1) o passageiro ao passar pelos pontos de controlo aeroportuários acima referidos.

O Comité conclui que se pode considerar que as medidas escolhidas respeitam o princípio da necessidade se o responsável pelo tratamento puder demonstrar que não existem soluções alternativas menos intrusivas que possam alcançar o mesmo objetivo de forma igualmente eficaz. Além disso, o caráter intrusivo do tratamento pode ser compensado pela participação ativa dos passageiros, uma vez que o seu modelo biométrico é armazenado apenas num dispositivo em sua posse, por exemplo, no seu dispositivo individual, sob o seu controlo exclusivo, e que os seus dados são apagados pouco tempo após a conclusão da operação de correspondência. Nesta base, o Comité conclui que o tratamento previsto no primeiro cenário **pode ser considerado, em princípio, compatível com artigo 5.º, n.º 1, alínea f), e os artigos 25.º e 32.º do RGPD**, sob reserva da aplicação de garantias adequadas.

O Comité identificou garantias mínimas que devem ser aplicadas para uma solução semelhante à do primeiro cenário.

O **segundo cenário** consiste no armazenamento centralizado, no aeroporto, de um modelo biométrico inscrito em forma encriptada com uma chave ou segredo apenas na posse do passageiro. Tal permite a autenticação dos passageiros (comparação 1:1) à medida que passam pelos pontos de controlo aeroportuários acima referidos. A inscrição é válida por um determinado período, que, por exemplo, pode ser até um ano entre o embarque no último voo e a data de validade do passaporte.

O Comité conclui que se pode considerar que o tratamento respeita o princípio da necessidade se o responsável pelo tratamento puder demonstrar que não existem soluções alternativas menos intrusivas que possam alcançar o mesmo objetivo de forma igualmente eficaz. Além disso, o caráter intrusivo do tratamento pode ser compensado pela participação ativa do passageiro, uma vez que este detém sob o seu controlo exclusivo a chave ou segredo dos seus dados biométricos encriptados. Partindo do princípio de que o responsável pelo tratamento aplica garantias adequadas, os riscos de segurança decorrentes da utilização de uma base de dados centralizada neste cenário podem ser atenuados e o impacto negativo nos direitos e liberdades fundamentais dos titulares dos dados pode ser considerado proporcional ao benefício esperado. No que diz respeito ao princípio da limitação da conservação, não foram fornecidas ao Comité informações para fundamentar esse longo prazo de conservação. A fim de alcançar a compatibilidade com o artigo 5.º, n.º 1, alínea e), do RGPD neste cenário, os responsáveis pelo tratamento devem poder justificar por que razão o prazo de conservação previsto é necessário para a finalidade em questão em casos específicos. O Comité recomenda que os responsáveis pelo tratamento prevejam o prazo de conservação mais curto possível, oferecendo simultaneamente aos passageiros a opção de fixar o prazo de conservação que preferirem. Nesta base, o Comité conclui que o tratamento previsto no cenário 2 **pode ser considerado, em princípio, compatível com artigo 5.º, n.º 1, alíneas e) e f), e os artigos 25.º e 32.º do RGPD**, sob reserva da aplicação de garantias adequadas.

O Comité identificou garantias mínimas que devem ser aplicadas para uma solução semelhante à do segundo cenário.

O **terceiro cenário** implica o armazenamento centralizado de um modelo biométrico inscrito em forma encriptada no aeroporto sob o controlo do operador aeroportuário. Tal permite a identificação dos passageiros (comparação 1:N) à medida que passam pelos pontos de controlo aeroportuários acima referidos. Neste cenário, o prazo de conservação é normalmente de 48 horas e os dados são apagados após a descolagem do avião.

Uma vez que os dados de identificação e biométricos são armazenados numa base de dados central, uma situação que ponha em causa a confidencialidade da base de dados pode posteriormente implicar o acesso a todo o conjunto de dados e permitir a identificação não autorizada ou ilícita de passageiros noutros ambientes. A arquitetura de armazenamento centralizado sob o controlo do operador aeroportuário também implica uma maior perda de controlo dos passageiros sobre os seus dados. O Comité considera que é possível alcançar um resultado semelhante em termos de racionalização do fluxo de passageiros nos aeroportos de forma menos intrusiva e que o impacto negativo nos direitos e liberdades fundamentais dos titulares dos dados que resultaria de uma violação de dados numa base de dados biométrica centralizada parece ser superior ao benefício esperado resultante do tratamento. Por conseguinte, o tratamento não pode respeitar os princípios da necessidade e da proporcionalidade. Nesta base, o Comité conclui que o tratamento previsto no terceiro cenário **não pode ser compatível com o artigo 25.º do RGPD**. Além disso, **não cumpriria o disposto no artigo 5.º, n.º 1, alínea f), e no artigo 32.º do RGPD** se um responsável pelo tratamento se limitasse às medidas descritas neste cenário.

O **quarto cenário** implica o armazenamento centralizado de um modelo biométrico inscrito em forma encriptada na nuvem sob o controlo da companhia aérea ou do seu prestador de serviços de computação em nuvem. Tal permite a identificação dos passageiros (comparação 1:N) à medida que passam pelos pontos de controlo aeroportuários acima referidos. Neste cenário, o prazo de conservação pode eventualmente vigorar enquanto o cliente for titular de uma conta junto da companhia aérea.

Uma vez que os dados de identificação e biométricos se encontram numa base de dados central na nuvem, várias entidades podem ter acesso a esses dados, incluindo, eventualmente, prestadores de serviços fora do EEE. Os dados do passageiro são desencriptados quando estão a ser utilizados e as chaves estão sob o controlo da companhia aérea ou dos seus subcontratantes, o que pode aumentar a superfície de exposição em termos de segurança. Essa arquitetura de armazenamento centralizado também implica uma maior perda de controlo dos passageiros sobre os seus dados. Além disso, os dados podem ser armazenados durante um período significativo, o que os expõe a riscos mais elevados de violação da segurança e parece ir além do estritamente necessário e proporcionado para as finalidades do tratamento, a menos que sejam tomadas outras medidas evidentes para atenuar os riscos para as pessoas singulares.

O Comité considera que é possível alcançar um resultado semelhante em termos de racionalização do fluxo de passageiros nos aeroportos de forma menos intrusiva e que o impacto negativo nos direitos e liberdades fundamentais dos titulares dos dados que poderia resultar de uma violação de dados numa base de dados biométrica centralizada parece ser superior ao benefício esperado resultante do tratamento. Por conseguinte, o tratamento não pode respeitar os princípios da necessidade e da proporcionalidade. Nesta base, o Comité conclui que o tratamento previsto no quarto cenário **não pode ser compatível com o artigo 25.º do RGPD**. Além disso, **não cumpriria o disposto no artigo 5.º, n.º 1, alínea e), do RGPD**, com base nas informações de que o Comité dispõe, e **não cumpriria o disposto no artigo 5.º, n.º 1, alínea f), e no artigo 32.º do RGPD** se um responsável pelo tratamento se limitasse às medidas descritas neste cenário.

Índice

O Comité Europeu para a Proteção de Dados,

Tendo em conta o artigo 63.º e o artigo 64.º, n.º 2, do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (a seguir designado por «**RGPD**»),

Tendo em conta o Acordo EEE, nomeadamente o anexo XI e o Protocolo n.º 37, com a redação que lhe foi dada pela Decisão n.º 154/2018 do Comité Misto do EEE, de 6 de julho de 2018[1],

Tendo em conta o artigo 10.º e o artigo 22.º do Regulamento Interno (a seguir designado por «**Regulamento Interno do CEPD**») do Comité Europeu para a Proteção de Dados (a seguir designado por «**Comité**» ou «**CEPD**»),

Considerando o seguinte:

(1) O Comité tem como principal função assegurar a aplicação coerente do RGPD em todo o Espaço Económico Europeu (a seguir designado por «**EEE**»). De acordo com o artigo 64.º, n.º 2, do RGPD, as autoridades de controlo (a seguir designadas por «**AC**»), o presidente do Comité ou a Comissão Europeia podem solicitar que o Comité analise qualquer assunto de aplicação geral ou que produza efeitos em mais do que um Estado-Membro do EEE, com vista a obter um parecer.

(2) O parecer do Comité deve ser adotado em conformidade com o artigo 64.º, n.º 3, do RGPD em conjugação com o artigo 10.º, n.º 2, do Regulamento Interno do CEPD no prazo de oito semanas após a presidente e a AC competente decidirem que o processo está concluído. Por decisão da presidente, este prazo pode ser prorrogado por mais seis semanas, tendo em conta a complexidade do tema.

Adotou o seguinte parecer:

1 INTRODUÇÃO

1.1 Resumo dos factos

1. Em 16 de fevereiro de 2024, a autoridade de controlo francesa (a seguir designada por «**AC FR**») solicitou ao Comité que emitisse um parecer sobre a compatibilidade com o artigo 5.º, n.º 1, alíneas e) e f), e os artigos 25.º e 32.º do RGPD, da utilização da tecnologia de reconhecimento facial pelos operadores aeroportuários e companhias aéreas para a autenticação ou identificação de passageiros com base na biometria[2], a fim de racionalizar o fluxo de passageiros, nos pontos de controlo de segurança[3], nos locais de entrega de bagagem, no embarque e no acesso às salas de espera dos

[1] As referências a «**Estados-Membros**» no presente parecer devem ser entendidas como referências a «Estados do EEE». As referências à «União» ou «UE» no presente parecer devem ser entendidas como referências ao «EEE».

[2] No contexto do presente parecer, entende-se por «**passageiro**» um titular de dados cujos dados pessoais são tratados para a finalidade específica nele descrita. No presente parecer, os termos «passageiro» e «pessoa singular» são utilizados indistintamente.

[3] Para efeitos do presente parecer, entende-se por «**pontos de controlo de segurança dos aeroportos**» os controlos de segurança efetuados sob a responsabilidade do operador aeroportuário a que os passageiros têm de ser submetidos para passarem do átrio de partidas para a zona de embarque ou para a porta de embarque.

aeroportos (excluindo o controlo nas fronteiras e os controlos efetuados por lojas francas) («**pedido**»). A AC FR anexou ao seu pedido uma descrição dos casos típicos de utilização (anexo I).

2. No seu pedido, a AC FR observa que os modelos que estão atualmente a ser testados em vários aeroportos da UE variam de um Estado-Membro para outro, criando assim um risco de divergência entre as interpretações das AC e o risco de se produzirem efeitos diferentes sobre os direitos e liberdades fundamentais dos titulares dos dados na UE[4].

3. O Comité considera que, para dar uma resposta ao pedido da AC francesa, é necessário responder às seguintes perguntas:

4. **Pergunta 1**:

1.1. A utilização da tecnologia de reconhecimento facial para autenticação com base na biometria **com a finalidade específica de racionalizar o fluxo de passageiros nos aeroportos** (pontos de controlo de segurança, locais de entrega de bagagem, embarque e acesso às salas de espera) pode ser compatível com **o artigo 5.º, n.º 1, alínea f), e os artigos 25.º e 32.º do RGPD** no caso de uma arquitetura de armazenamento em que o modelo biométrico de cada passageiro só é armazenado **em dispositivos na posse da pessoa singular**, por exemplo, localmente, no seu dispositivo individual, sob o seu controlo exclusivo?

1.2. Se esse tratamento for considerado compatível com as disposições acima referidas, que garantias mínimas adequadas seriam necessárias, à luz dos artigos 25.º e 32.º do RGPD?

Pergunta 2:

2.1. A utilização da tecnologia de reconhecimento facial para autenticação ou identificação com base na biometria **com a finalidade específica de racionalizar o fluxo de passageiros nos aeroportos** (pontos de controlo de segurança, locais de entrega de bagagem, embarque e acesso às salas de espera) pode ser compatível com **o artigo 5.º, n.º 1, alíneas e) e f), e os artigos 25.º e 32.º do RGPD** no caso de uma arquitetura de armazenamento **centralizado**, em que o modelo biométrico de cada passageiro é armazenado numa base de dados central:

2.1.1. Numa base de dados central do aeroporto, sob o controlo do operador aeroportuário, em forma encriptada, com uma chave ou segredo mantido exclusivamente na posse da pessoa singular (por exemplo, no seu telemóvel), para autenticação?

2.1.2. Se esse tratamento for considerado compatível, que garantias mínimas adequadas seriam necessárias, à luz dos artigos 25.º e 32.º do RGPD?

2.2.1. Numa base de dados central do aeroporto, sob o controlo do operador aeroportuário, em forma encriptada, com as chaves na posse do operador aeroportuário, para identificação?

2.2.2. Se esse tratamento for considerado compatível, que garantias mínimas adequadas seriam necessárias, à luz dos artigos 25.º e 32.º do RGPD?

[4] Pedido, p. 1.

2.3.1. Na nuvem, sob o controlo da companhia aérea ou do seu prestador de serviços (subcontratante), em forma encriptada, com as chaves na posse da companhia aérea ou do seu prestador de serviços, para identificação?

2.3.2. Se esse tratamento for considerado compatível, que garantias mínimas adequadas seriam necessárias, à luz dos artigos 25.º e 32.º do RGPD?

5. Depois de a AC FR, em 16 de fevereiro de 2024, e a presidente do Comité, em 23 de fevereiro de 2024, terem considerado que o processo estava concluído, este foi distribuído pelo Secretariado em 23 de fevereiro de 2024. A presidente do CEPD decidiu, em conformidade com o artigo 64.º, n.º 3, do RGPD, em conjugação com o artigo 10.º, n.º 2, do Regulamento Interno do CEPD, prorrogar por mais seis semanas o prazo para a adoção, que é por defeito de oito semanas, devido à complexidade do assunto em apreço.

1.2 Admissibilidade do pedido de parecer nos termos do artigo 64.º, n.º 2, do RGPD

6. O artigo 64.º, n.º 2, do RGPD dispõe que, nomeadamente, as AC podem solicitar que o Comité analise qualquer assunto de aplicação geral ou que produza efeitos em mais do que um Estado-Membro, com vista a obter um parecer.

7. O Comité considera que o pedido apresentado pela AC FR sobre a compatibilidade da utilização da tecnologia de reconhecimento facial para autenticação ou identificação com base na biometria com a finalidade específica de racionalizar o fluxo de passageiros nos aeroportos diz respeito a questões que produzem «efeitos em mais do que um Estado-Membro», uma vez que, tal como explicado no pedido[5], existem atualmente vários projetos em fase de implantação nos aeroportos dos Estados-Membros, prevendo-se que essa utilização aumente nos próximos anos. Os modelos que estão atualmente a ser testados por diferentes aeroportos e companhias aéreas variam significativamente de um Estado-Membro para outro, existindo assim o risco de, do ponto de vista da proteção de dados, produzirem efeitos divergentes em mais do que um Estado-Membro.

8. Além disso, o Comité considera que o pedido apresentado pela AC FR tem consequências importantes para a aplicação dos princípios estabelecidos no artigo 5.º, n.º 1, alíneas e) e f), do RGPD e dos requisitos aplicáveis aos responsáveis pelo tratamento nos termos do artigo 25.º do RGPD, bem como dos requisitos aplicáveis aos responsáveis pelo tratamento e aos subcontratantes nos termos do artigo 32.º do RGPD. Por conseguinte, o pedido em causa diz respeito a um «assunto de aplicação geral» na aceção do artigo 64.º, n.º 2, do RGPD, uma vez que se refere à interpretação coerente dos princípios da limitação da conservação (artigo 5.º, n.º 1, alínea e), do RGPD) e da integridade e confidencialidade (artigo 5.º, n.º 1, alínea f), do RGPD), bem como dos conceitos de proteção de dados desde a conceção e por defeito (artigo 25.º do RGPD) e segurança dos dados (artigo 32.º do RGPD), a fim de assegurar, nomeadamente, a aplicação coerente dessas disposições no EEE.

9. Quaisquer eventuais posições divergentes entre os Estados-Membros sobre a interpretação do artigo 5.º, n.º 1, alíneas e) e f), e dos artigos 25.º e 32.º do RGPD aumentariam o risco de os operadores aeroportuários e as companhias aéreas desenvolverem projetos de reconhecimento facial de forma não coerente. Uma vez que a AC FR demonstrou a clara necessidade de uma interpretação coerente

[5] Pedido, p. 3.

destas disposições em relação à tecnologia de reconhecimento facial para autenticação ou identificação de passageiros com base na biometria, a fim de racionalizar o fluxo de passageiros nos aeroportos[6], o Comité considera que o pedido é fundamentado, em conformidade com o artigo 10.º, n.º 3, do Regulamento Interno do CEPD.

10. Nos termos do artigo 64.º, n.º 3, do RGPD, o CEPD não emite um parecer quando já antes tenha emitido um parecer sobre o mesmo assunto[7]. O CEPD ainda não respondeu às questões decorrentes do pedido. Embora as Diretrizes 3/2019 do CEPD relativas aos dispositivos de vídeo[8] já forneçam alguns elementos úteis sobre as medidas de segurança que devem ser aplicadas ao tratamento de dados biométricos, não abordam todos os aspetos relativos às questões suscitadas no pedido. Além disso, as diretrizes disponíveis do CEPD, incluindo as Diretrizes 3/2019 relativas aos dispositivos de vídeo, não fornecem orientações específicas sobre possíveis elementos a verificar em relação ao armazenamento centralizado ou descentralizado de dados biométricos para identificar ou autenticar os passageiros, a fim de racionalizar o fluxo de passageiros nos aeroportos, nem sobre a compatibilidade desse tratamento com o artigo 5.º, n.º 1, alíneas e) e f), e os artigos 25.º e 32.º do RGPD.

11. Por estas razões, o Comité considera que o pedido é admissível e que as questões nele suscitadas devem ser analisadas num parecer adotado nos termos do artigo 64.º, n.º 2, do RGPD.

2 ÂMBITO E CONTEXTO DO PARECER

2.1 Âmbito do parecer

12. O presente parecer diz apenas respeito à compatibilidade com o artigo 5.º, n.º 1, alíneas e) e f), e os artigos 25.º e 32.º do RGPD da utilização da tecnologia de reconhecimento facial para a autenticação ou identificação de passageiros com base na biometria por parte dos operadores aeroportuários e das companhias aéreas, **com a finalidade específica de racionalizar o fluxo de passageiros nos aeroportos**, nomeadamente nos pontos de controlo de segurança, nos locais de entrega de bagagem, no embarque e no acesso às salas de espera, de acordo com o pedido.

13. No que diz respeito ao **âmbito do presente parecer**, o Comité esclarece o seguinte:

    1) O tratamento de dados pessoais no quadro dos controlos nas fronteiras e dos controlos efetuados por lojas francas não é abrangido pelo âmbito do presente parecer, uma vez que é realizado por outros responsáveis pelo tratamento que não são operadores aeroportuários nem companhias aéreas.

    2) A utilização da tecnologia de reconhecimento facial, mesmo que baseada nos cenários descritos na secção 3.2 *infra*, para quaisquer outras finalidades (como a aplicação da lei) ou por quaisquer outras partes, ainda que para fins semelhantes, não é abrangida pelo âmbito do presente parecer.

---

[6] Pedido, pp. 1-3.
[7] Artigo 64.º, n.º 3, do RGPD e artigo 10.º, n.º 4, do Regulamento Interno do CEPD.
[8] Diretrizes 3/2019 sobre tratamento de dados pessoais através de dispositivos de vídeo, versão 2.0, adotadas em 29 de janeiro de 2020 (a seguir designadas por «**Diretrizes 3/2019 do CEPD relativas aos dispositivos de vídeo**»).

3) O presente parecer analisa apenas o tratamento de dados pessoais dos passageiros e não abrange outros tipos de titulares de dados, como o pessoal dos operadores aeroportuários ou das companhias aéreas.

4) O presente parecer analisa o pedido apresentado pela AC FR, em relação à compatibilidade das arquiteturas de armazenamento dos modelos biométricos dos passageiros com o artigo 5.º, n.º 1, alíneas e) e f), e os artigos 25.º e 32.º do RGPD. A este respeito, o presente parecer não inclui uma análise total e completa do cumprimento do RGPD por parte do responsável ou responsáveis pelo tratamento em questão em cada caso, bem como por parte do(s) seu(s) subcontratante(s), se for caso disso. Este aspeto é particularmente importante tendo em conta que estas tecnologias implicam riscos acrescidos associados ao tratamento das categorias especiais de dados em conformidade com o artigo 9.º do RGPD. Por conseguinte, o presente parecer não prejudica uma avaliação de outras disposições do RGPD no que diz respeito à utilização de tecnologias de reconhecimento facial, incluindo no setor específico abordado pelo pedido, nem uma análise jurídica e técnica caso a caso baseada no tratamento previsto e nas circunstâncias de um determinado responsável pelo tratamento.

5) O presente parecer não analisa o tratamento de dados pessoais das crianças e não prejudica quaisquer requisitos específicos aplicáveis a esse respeito.

6) O presente parecer não prejudica os requisitos legais e outras restrições à utilização de dados biométricos decorrentes das legislações nacionais dos Estados-Membros[9].

7) Qualquer conclusão do presente parecer é formulada sem prejuízo de outras evoluções tecnológicas.

8) O presente parecer analisa quatro cenários, cujas características específicas são descritas na secção 3.2 *infra*. Não aborda outros cenários, mesmo que o tratamento tenha as mesmas finalidades.

14. No seu pedido, a AC FR indicou que o tratamento dos dados biométricos dos passageiros para efeitos de racionalização do fluxo de passageiros nos aeroportos se basearia no pressuposto de que as pessoas consentiam nesse tratamento, o que poderia constituir a base jurídica ao abrigo do RGPD[10]. **No entanto, a análise da base jurídica aplicável não se enquadra no âmbito das questões submetidas ao CEPD no pedido, pelo que o presente parecer não examina a validade do consentimento para esse tratamento, em conformidade com os artigos 6.º, 7.º e 9.º do RGPD.**

[9] Por exemplo, o artigo 9.º, n.º 4, do RGPD permite que os Estados-Membros mantenham ou imponham novas condições, incluindo limitações, no que respeita ao tratamento de dados biométricos.
[10] Pedido, anexo I.

15. Todavia, o CEPD observa, em termos gerais, que, se os responsáveis pelo tratamento em causa recorressem a esta base jurídica, teriam de obter um consentimento explícito válido[11] das pessoas singulares que pretendem utilizar esses serviços. Esse consentimento explícito teria de ser uma manifestação de vontade, livre, específica e informada[12] e o cumprimento dessas condições seria analisado caso a caso. Isto significa, nomeadamente, o seguinte:

1) As pessoas teriam de poder retirar facilmente esse consentimento a qualquer momento e sem serem prejudicadas[13].

2) Para que o consentimento seja dado livremente, a utilização de tecnologias baseadas na biometria só pode ter lugar numa base voluntária, uma vez que as pessoas singulares devem poder escolher livremente se utilizam ou não estes serviços, sem quaisquer prejuízos (por exemplo, atrasos significativamente mais longos para os passageiros que não dão o seu consentimento[14]), incentivos, custos suplementares ou vantagens adicionais em contrapartida[15].

3) Seria igualmente necessário obter o consentimento explícito das pessoas singulares cujos dados biométricos são tratados, mesmo que não se tenham inscrito para serem identificadas ou autenticadas por esses meios. Por outras palavras, é essencial que as pessoas singulares que não tenham consentido explicitamente no reconhecimento facial para as finalidades previstas não sejam sujeitas ao reconhecimento ótico do seu rosto por câmaras. Tal pode ser alcançado, por exemplo, dedicando corredores específicos ao reconhecimento facial e proporcionando uma sinalização adequada e uma separação física com os fluxos de controlo não biométricos, a fim de permitir uma identificação clara desses corredores.

4) Sem prejuízo de o consentimento ser ou não a base jurídica aplicável a esse tratamento, os princípios do tratamento consagrados no artigo 5.º do RGPD no que diz respeito à necessidade e à proporcionalidade continuam a ser aplicáveis mesmo que as pessoas singulares tenham dado o seu consentimento explícito para a utilização dos seus dados biométricos[16].

---

[11] Nos termos do artigo 4.º, ponto 14, e do artigo 9.º, n.º 1, do RGPD, bem como do artigo 9.º, n.º 2, alínea a), do mesmo regulamento, o tratamento de dados biométricos para identificar uma pessoa de forma inequívoca só é permitido se o titular dos dados tiver dado o seu consentimento explícito para o tratamento desses dados pessoais para uma ou mais finalidades específicas, exceto se o direito da União ou de um Estado-Membro previr que a proibição a que se refere o artigo 9.º, n.º 1, do RGPD não pode ser anulada pelo titular dos dados. Ver igualmente considerandos 51, 52 e 53 do RGPD.

[12] Artigo 4.º, ponto 11, e artigo 7.º do RGPD.

[13] Artigo 7.º, n.º 4, do RGPD; ver igualmente considerando 50 do RGPD.

[14] Tal pode incluir considerações como, por exemplo, a conceção de um sistema para evitar criar pressão social sobre os passageiros que não querem dar o seu consentimento, evitando que a sua escolha tenha um impacto negativo noutros passageiros.

[15] Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679, versão 1.1, adotadas em 4 de maio de 2020 (a seguir designadas por «**Diretrizes 05/2020 do CEPD relativas ao consentimento**»), n.os 46 e 48.

[16] *Idem*, n.º 5.

16. O pedido especifica[17] que os operadores aeroportuários atuariam como responsáveis pelo tratamento nos pontos de controlo de segurança dos aeroportos, ao passo que as companhias aéreas assumiriam esse papel no que diz respeito aos locais de entrega de bagagem, ao embarque e ao acesso às salas de espera. Por conseguinte, o Comité observa que diferentes intervenientes podem participar no tratamento descrito no pedido e não avaliou a aplicação das funções de responsável (conjunto) pelo tratamento e/ou subcontratante nos cenários descritos na secção 3.2 do presente parecer. Em cada caso, é necessário identificar os intervenientes em causa e definir claramente as suas responsabilidades, a fim de cumprir os requisitos do RGPD[18].

17. Além disso, o Comité observa que, atualmente, não existe um requisito legal uniforme na UE sobre a forma como os operadores aeroportuários e as companhias aéreas devem identificar os passageiros e verificar se o nome no cartão de embarque do passageiro corresponde ao nome constante do seu documento de identificação em todos os pontos de controlo acima mencionados[19]. Assim, tais requisitos estão sujeitos a legislações nacionais que podem variar de um Estado-Membro para outro. Em alguns Estados-Membros, essa verificação pode ser exigida para alguns pontos de controlo (por exemplo, os locais de entrega de bagagem ou o embarque), enquanto noutros não são atualmente exigidos controlos desse tipo[20]. A existência de obrigações legais de verificação da identidade dos passageiros tem um impacto direto nas diferentes práticas dos aeroportos.

18. Por conseguinte, nestas situações **em que não é exigida a verificação da identidade dos passageiros com um documento de identidade oficial, não deve ser efetuada qualquer verificação com base na biometria, uma vez que tal resultaria num tratamento excessivo de dados, ou seja, no tratamento de dados adicionais em comparação com a situação atual, e iria além do necessário para a finalidade em causa, em violação do princípio da minimização dos dados estabelecido no artigo 5.º, n.º 1, alínea c), do RGPD.** Esta consideração deve ser tida em conta no âmbito da análise de todos os cenários descritos na secção 3.2 do presente parecer.

2.2 Conceitos essenciais

19. Para se poder falar de dados biométricos nos termos do artigo 4.º, ponto 14, do RGPD[21], o tratamento de dados em bruto, como as características físicas, fisiológicas ou comportamentais de uma pessoa

[17] Pedido, anexo I.
[18] Em conformidade com o artigo 4.º, pontos 7 e 8, o artigo 5.º, n.º 2, e os artigos 24.º, 26.º, 28.º e 29.º do RGPD. Ver também as Orientações 07/2020 do CEPD sobre os conceitos de responsável pelo tratamento e subcontratante no RGPD, versão 2.1, adotadas em 7 de julho de 2021.
[19] O regulamento pertinente a nível da UE é o Regulamento de Execução (UE) 2015/1998 da Comissão, de 5 de novembro de 2015, que estabelece as medidas de execução das normas de base comuns sobre a segurança da aviação. No entanto, esse regulamento não aborda os controlos dos documentos de identidade oficiais nos pontos de controlo nos aeroportos, e os Estados-Membros têm o poder discricionário de regulamentar esta questão a nível nacional.
[20] O que significa que, atualmente, não é efetuada qualquer verificação ou apenas é verificada a existência do cartão de embarque. Por exemplo, com base no Protocolo relativo à isenção dos nacionais da Dinamarca, da Finlândia, da Noruega e da Suécia da obrigação de possuir um passaporte ou uma autorização de residência enquanto residirem num país escandinavo diferente do seu, de 22 de maio de 1954, os cidadãos da Noruega, da Dinamarca, da Finlândia e da Suécia estão isentos, desde 1 de julho de 1954, da obrigação de possuir um passaporte ou outra identificação de viagem quando viajam entre esses países.
[21] Ver igualmente considerandos 51, 52 e 53 do RGPD.

singular, deve implicar uma medição dessas características, uma vez que os dados biométricos resultam dessas medições[22].

20. Utilizando a imagem do rosto de uma pessoa (uma fotografia ou um vídeo), designada por «**amostra**» biométrica, é possível extrair uma representação digital de características distintas desse rosto (designada por «**modelo**»)[23]. Além disso, o Comité recorda que «[u]m modelo biométrico é uma representação digital das características únicas que foram extraídas de uma amostra biométrica e que podem ser armazenadas numa base de dados biométrica»[24] que permitem ou confirmam a identificação inequívoca de uma pessoa singular. Além disso, este modelo biométrico «deverá ser único e específico para cada pessoa e é, em princípio, constante ao longo do tempo»[25]. Normalmente, num processo de comparação destinado a identificar ou autenticar uma pessoa através do reconhecimento facial, um modelo biométrico recebido é comparado com objetos armazenados para verificar ou procurar uma correspondência numa base de dados[26].

21. A tecnologia de reconhecimento facial pode desempenhar duas funções distintas: autenticação[27] e identificação[28]. Embora estas duas funções sejam diferentes, ambas se baseiam no tratamento de dados biométricos relacionados com uma pessoa singular identificada ou identificável[29] e, por conseguinte, constituem um tratamento de categorias especiais de dados pessoais ao abrigo do artigo 9.º do RGPD[30].

22. Em especial:

---

[22] Diretrizes 3/2019 do CEPD relativas aos dispositivos de vídeo, n.º 74.

[23] Orientações 05/2022 sobre a utilização da tecnologia de reconhecimento facial no domínio da aplicação da lei, versão 2.0, adotadas em 26 de abril de 2023 (a seguir designadas por «**Orientações 05/2022 do CEPD relativas ao reconhecimento facial na aplicação da lei**»), n.ºs 7 e 8.

[24] *Idem*, n.º 9.

[25] *Idem*.

[26] Orientações 05/2022 do CEPD relativas ao reconhecimento facial na aplicação da lei, n.ºs 10 e 11; ver também a norma internacional ISO/IEC 2382-37, 2022-03, disponível em: https://standards.iso.org/ittf/PubliclyAvailableStandards/c073514_ISO_IEC%202382-37_2022(E).zip [consultado pela última vez em 23 de maio de 2024] (a seguir designada por «**ISO/IEC 2382-37**»).

[27] O Comité observa que o futuro regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial) (ainda não publicado no Jornal Oficial) define também, no artigo 3.º, ponto 36, a «verificação biométrica» como «a verificação automatizada, "um para um", incluindo a autenticação, da identidade de pessoas singulares por meio da comparação dos seus dados biométricos com dados biométricos previamente fornecidos» [ver Resolução legislativa do Parlamento Europeu, de 13 de março de 2024, sobre a proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da União (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))].

[28] De igual modo, o artigo 3.º, ponto 35, do Regulamento Inteligência Artificial define «identificação biométrica» como «o reconhecimento automatizado de características humanas físicas, fisiológicas, comportamentais ou psicológicas para efeitos de determinação da identidade de uma pessoa singular, comparando os dados biométricos dessa pessoa com os dados biométricos de pessoas armazenados numa base de dados».

[29] ISO/IEC 2382-37.

[30] Artigo 4.º, ponto 14, do RGPD, e Orientações 05/2022 do CEPD relativas ao reconhecimento facial na aplicação da lei, n.º 12.

A **autenticação** visa confirmar uma alegação biométrica através de comparação. É também designada por verificação «um para um».

A **identificação** visa consultar uma base de dados de inscrições biométricas para obter identificadores atribuíveis a uma única pessoa. É também designada por identificação «um entre muitos».

23. Em ambos os casos (ou seja, identificação e autenticação), as técnicas de reconhecimento facial baseiam-se numa correspondência estimada entre modelos, ou seja, o que está a ser comparado e a(s) base(s) de referência. Deste ponto de vista, são probabilísticas: a comparação deduz uma maior ou menor probabilidade de a pessoa em questão ser efetivamente a pessoa a autenticar ou a identificar; se esta probabilidade exceder um determinado limiar no sistema, definido pelo utilizador ou pelo programador do sistema, este assumirá que existe uma correspondência a identificar ou autenticar[31].

[31] Orientações 05/2022 do CEPD relativas ao reconhecimento facial na aplicação da lei, n.º 11. Ver também ISO/IEC 2382-37.

3 QUANTO AO MÉRITO DO PEDIDO

3.1 Observações gerais

24. A presente secção analisa as questões apresentadas no n.º 4 *supra*. Neste contexto, o Comité analisará, relativamente à pergunta 1, a compatibilidade com o artigo 5.º, n.º 1, alínea f), e os artigos 25.º e 32.º do RGPD, e, relativamente à pergunta 2, a compatibilidade com o artigo 5.º, n.º 1, alíneas e) e f), e os artigos 25.º e 32.º do RGPD.

25. Para o efeito, o Comité analisará quatro cenários diferentes[32], cujas características específicas são descritas na secção 3.2 *infra*.

26. A título preliminar, o Comité recorda que a utilização de dados biométricos e, em especial, da tecnologia de reconhecimento facial implica riscos acrescidos para os direitos e liberdades dos titulares dos dados. Em primeiro lugar, o tratamento em causa diz respeito a dados biométricos aos quais é concedida proteção especial ao abrigo do artigo 9.º do RGPD. Nomeadamente, os dados biométricos alteram irreversivelmente a relação entre o corpo e a identidade, ao permitirem que as características do corpo humano sejam lidas por uma máquina e sujeitas a utilização posterior[33]. Além disso, a utilização da tecnologia de reconhecimento facial pode conduzir a riscos associados a falsos negativos, desequilíbrios e discriminação[34], e a potencial utilização abusiva de dados biométricos pode ter consequências graves para as pessoas, como a fraude ou a usurpação de identidade[35]. Note-se igualmente que, quando o reconhecimento facial é efetuado à distância e sem a participação ativa do titular dos dados, as pessoas singulares podem estar ainda menos cientes desse tratamento e dos riscos associados. Por último, é importante salientar que as características em que se baseiam os dados biométricos podem, de um modo geral, ser consideradas permanentes e devem ser tratadas como não revogáveis, especialmente no contexto do reconhecimento facial[36].

27. Por conseguinte, tendo em conta o que precede, antes de utilizarem essas tecnologias, mesmo que sejam consideradas particularmente eficazes, os responsáveis pelo tratamento devem avaliar o

[32] Os quatro cenários analisados pelo Comité baseiam-se nos casos de utilização apresentados no anexo I do pedido. A AC FR esclareceu que os casos de utilização constantes do anexo I do pedido são exemplos de execução inseridos num cenário e utilizados para fins ilustrativos.

[33] Parecer 3/2012 do Grupo do Artigo 29.º sobre a evolução das tecnologias biométricas, adotado em 27 de abril de 2012, WP193 (a seguir designado por «**Parecer 3/2012 do Grupo do Artigo 29.º relativo às tecnologias biométricas**»), p. 4. Importa salientar que este parecer se refere à Diretiva 95/46/CE, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados («Diretiva Proteção de Dados»). O RGPD alargou o âmbito das categorias especiais de dados e, ao contrário da Diretiva Proteção de Dados, estabelece que os dados biométricos são categorias especiais de dados (artigo 9.º do RGPD).

[34] *Guidelines on facial recognition* (Diretrizes sobre o reconhecimento facial), Comité Consultivo da Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, junho de 2021, p. 15; ver também as Orientações 05/2022 do CEPD relativas ao reconhecimento facial na aplicação da lei, n.º 27.

[35] Parecer 3/2012 do Grupo do Artigo 29.º relativo às tecnologias biométricas, p. 34.

[36] Orientações 05/2022 do CEPD relativas ao reconhecimento facial na aplicação da lei, n.º 104.

impacto nos direitos e liberdades fundamentais dos titulares dos dados e ponderar se podem utilizar meios menos intrusivos para alcançar a finalidade legítima do tratamento que efetuam[37].

28. O Comité recorda igualmente que o direito à proteção de dados pessoais não é absoluto e deve ser equilibrado com outros direitos fundamentais protegidos pela Carta, em conformidade com o princípio da proporcionalidade[38].

29. O artigo 25.º, n.º 1, do RGPD refere-se aos «princípios da proteção de dados» enumerados no artigo 5.º do mesmo regulamento[39] e exige que sejam aplicados «com eficácia» desde a conceção[40]. Tal inclui expressamente o princípio da minimização dos dados previsto no artigo 5.º, n.º 1, alínea c), do RGPD[41], que exige que os dados pessoais sejam «[a]dequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados», dando expressão ao princípio da proporcionalidade[42]. Além disso, o artigo 25.º, n.º 2, do RGPD especifica a obrigação de «minimização dos dados por defeito», declarando que se aplica à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade[43].

30. No entanto, o artigo 25.º do RGPD não exige que os responsáveis pelo tratamento apliquem quaisquer medidas técnicas e organizativas específicas, mas que as medidas e garantias escolhidas sejam específicas do contexto e dos riscos para os direitos e liberdades do titular dos dados decorrentes do tratamento[44]. Do mesmo modo, o artigo 32.º do RGPD, relativo à segurança do tratamento, exige que

---

[37] Considerando 39 do RGPD. Ver também as Diretrizes 3/2019 do CEPD relativas aos dispositivos de vídeo, n.º 73.

[38] Considerando 4 do RGPD. Ver também, a este respeito, o Acórdão do Tribunal de Justiça de 22 de junho de 2021, Latvijas Republikas Saeima, C-439/19, ECLI:EU:C:2021:504 (a seguir designado por «C-439/19 Latvijas Republikas Saeima»), n.os 98, 110 e 113. Além disso, o princípio da proporcionalidade, enquanto princípio geral do direito da União, exige que os meios postos em prática por um ato da União sejam aptos a realizar o objetivo prosseguido e não vão além do que é necessário para o alcançar [ver Acórdão do Tribunal de Justiça de 9 de novembro de 2010, Volker und Markus Schecke e Eifert, C-92/09 e C-93/09, ECLI:EU:C:2010:662 (a seguir designado por «C-92/09 e C-93/09 Volker und Schecke»), n.º 74, e jurisprudência aí referida].

[39] Orientações 4/2019 do CEPD relativas ao artigo 25.º – Proteção de Dados desde a Conceção e por Defeito, versão 2.0, adotadas em 20 de outubro de 2020 (a seguir designadas por «**Orientações 4/2019 do CEPD relativas à proteção de dados desde a conceção e por defeito**»), n.º 11.

[40] O artigo 25.º, n.º 1, do RGPD estabelece o seguinte: «Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados.» Ver também as Orientações 4/2019 do CEPD relativas ao artigo 25.º – Proteção de Dados desde a Conceção e por Defeito, n.º 13.

[41] Do mesmo modo, o considerando 39 do RGPD estabelece que os dados pessoais só devem ser tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios.

[42] C-439/19 Latvijas Republikas Saeima, n.º 98; Acórdão do Tribunal de Justiça de 11 de dezembro de 2019, Asociaţia de Proprietari bloc M5A-ScaraA, C-708/18, ECLI:EU:C:2019:1064 (a seguir designado por «C-708/18 M5A-ScaraA»), n.º 48.

[43] Orientações 4/2019 do CEPD relativas ao artigo 25.º – Proteção de Dados desde a Conceção e por Defeito, n.º 48.

[44] Orientações 4/2019 do CEPD relativas ao artigo 25.º – Proteção de Dados desde a Conceção e por Defeito, n.º 14.

os responsáveis pelo tratamento e os subcontratantes apliquem medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco para os direitos e liberdades das pessoas singulares.

31. É importante salientar que, mesmo que os passageiros consentissem explicitamente na utilização dos seus dados biométricos a fim de racionalizar o fluxo de passageiros nos aeroportos, os princípios da necessidade e da proporcionalidade do tratamento consagrados no RGPD continuam a ser aplicáveis e têm de ser respeitados[45].

32. No que diz respeito ao **princípio da necessidade**, o Comité examinará se o tratamento proposto é necessário para atingir o objetivo prosseguido e se o mesmo objetivo pode ser alcançado de forma eficaz por outros meios menos intrusivos para os direitos e liberdades fundamentais do titular dos dados[46]. No que diz respeito ao **princípio da proporcionalidade**, o Comité avaliará se o impacto negativo nos direitos e liberdades fundamentais dos titulares dos dados é proporcional a qualquer benefício esperado. Se o benefício for relativamente reduzido, esse impacto poderá não ser proporcionado[47].

33. Em todo o caso, mesmo que o Comité considere que um dos cenários a seguir analisados poderia cumprir os requisitos do artigo 5.º, n.º 1, alíneas e) e f), e dos artigos 25.º e 32.º do RGPD, cabe ao responsável pelo tratamento demonstrar esse cumprimento com elementos factuais em cada caso. Essa demonstração deve incluir a ponderação de cenários alternativos.

3.2 Quanto à compatibilidade com o artigo 5.º, n.º 1, alíneas e) e f), e os artigos 25.º e 32.º do RGPD

3.2.1 Cenário 1: armazenamento do modelo biométrico inscrito apenas na posse da pessoa singular, para autenticação

34. A presente secção analisa a compatibilidade com o artigo 5.º, n.º 1, alínea f), e os artigos 25.º e 32.º do RGPD do armazenamento do modelo biométrico dos passageiros apenas num dispositivo na posse da pessoa singular, por exemplo no seu dispositivo individual[48], sob o seu controlo exclusivo[49], para autenticação[50] («**cenário 1**»). A presente secção analisa igualmente as garantias adequadas para o cenário 1, à luz dos artigos 25.º e 32.º do RGPD.

Descrição do cenário

35. No cenário 1, o modelo biométrico inscrito de cada passageiro, desde que este tenha consentido nesse tipo de tratamento, só é armazenado num dispositivo na posse da pessoa singular, por exemplo, num

[45] Diretrizes 5/2020 do CEPD relativas ao consentimento na aceção do Regulamento (UE) 2016/679, n.º 5.
[46] C-439/19 Latvijas Republikas Saeima, n.os 110 e 113; Acórdão do Tribunal de Justiça (Grande Secção) de 4 de julho de 2023, Meta v. Bundeskartellamt, C-252/21, ECLI:EU:C:2023:537, n.º 108.
[47] C-708/18 M5A-ScaraA, n.os 52 a 56, C-92/09 e C-93/09 Volker und Schecke, n.º 87, C-439/19 Latvijas Republikas Saeima, n.os 98, 110 e 113. Ver também o Parecer 3/2012 do Grupo do Artigo 29.º relativo às tecnologias biométricas, p. 9.
[48] Em alternativa, o passageiro poderia imprimir e conservar o seu modelo biométrico em papel.
[49] Tal não prejudica a responsabilidade global do responsável pelo tratamento.
[50] Como exemplificado pelo caso de utilização 1 constante do anexo I do pedido.

seu dispositivo individual, e sob o seu controlo exclusivo. Os passageiros são autenticados (comparação 1:1) quando passam por pontos de controlo específicos no aeroporto.

36. A inscrição é efetuada pelo operador aeroportuário à distância, através da respetiva aplicação[51], ou nos terminais dos aeroportos com um nível de garantia de identidade adequado (por exemplo, nível de garantia adequado eIDAS[52]). Essa inscrição consiste no registo, no dispositivo do passageiro, de um modelo biométrico e dos dados de identificação[53] (a seguir designados por «**DI**») necessários para o tratamento. A inscrição ocorre apenas uma vez e tem um período de validade específico (por exemplo, em consonância com o período de validade do passaporte do passageiro). Nem os DI dos passageiros nem os seus dados biométricos são conservados pelo operador aeroportuário após o processo de inscrição.

37. No que diz respeito, em especial, ao armazenamento, os DI e o modelo biométrico do passageiro são armazenados localmente, no dispositivo de cada passageiro (por exemplo, na aplicação móvel do operador aeroportuário ou numa aplicação de carteira digital). O dispositivo pode depois ser utilizado para transmitir ou consultar os DI e o modelo biométrico dos passageiros, incluindo eventualmente informações sobre o voo e/ou o cartão de embarque. Por exemplo, esta informação é encriptada com uma chave detida apenas pelo operador aeroportuário, eventualmente codificada sob a forma de um código QR, que pode ser impresso em papel ou exibido no ecrã do dispositivo do passageiro. Neste caso, o passageiro apresentaria este código QR em módulos de controlo específicos no aeroporto, equipados com um leitor de códigos QR e uma câmara.

38. Em termos de segurança, durante a correspondência, os códigos QR são desencriptados com uma chave detida pelo operador aeroportuário, que é o único capaz de realizar essa desencriptação. Os dados biométricos dos passageiros são conservados apenas durante um período muito curto e apagados após a conclusão da operação de correspondência. Note-se que as medidas de segurança em matéria de armazenamento dependem, em parte, da segurança do dispositivo do passageiro.

Avaliação do CEPD

39. O cenário 1 descreve medidas técnicas e organizativas concebidas para garantir um nível de segurança adequado aos riscos para os titulares dos dados, tal como exigido no artigo 5.º, n.º 1, alínea f), e no artigo 32.º do RGPD. Os passageiros são autenticados (comparação 1:1) quando passam por pontos de controlo específicos no aeroporto. Neste cenário, a principal operação de correspondência é efetuada num ambiente controlado[54], em que os passageiros participam ativamente e têm mais

[51] O CEPD observa que poderão ser previstas formas alternativas para essa inscrição no futuro e que a inscrição poderá eventualmente ser efetuada sem uma aplicação específica de um operador aeroportuário, por exemplo, através da interação com a carteira digital de um utilizador.

[52] Um quadro em matéria de identificação eletrónica e de serviços de confiança (a seguir designado por «**eIDAS**») com base no Regulamento (UE) 2024/1183 do Parlamento Europeu e do Conselho, de 11 de abril de 2024, que altera o Regulamento (UE) n.º 910/2014 no respeitante à criação do Regime Europeu para a Identidade Digital.

[53] Para efeitos do presente parecer, os dados de identificação referem-se a dados como o apelido, o nome próprio, a data de nascimento, etc., cuja exatidão foi verificada relativamente a um documento de identidade ou passaporte.

[54] «Ambiente não controlado» refere-se à utilização do reconhecimento facial para efeitos de identificação sem a participação ativa dos titulares dos dados e em que o modelo de cada rosto que entra na área de monitorização é comparado com modelos provenientes de uma secção transversal ampla da população conservada numa base de dados; ver as Orientações 05/2022 do CEPD relativas ao reconhecimento facial na aplicação da lei, n.º 17.

controlo sobre os seus dados. Em especial, apenas seriam controlados os passageiros que consentissem nesse tratamento e, uma vez que tal ocorreria em módulos específicos, não seriam recolhidos dados biométricos de outros passageiros que não dessem o mesmo consentimento. Além disso, os passageiros que tenham dado o seu consentimento têm a possibilidade de interromper o tratamento em qualquer momento, apagando os dados do seu dispositivo.

40. A utilização do reconhecimento facial com base num modelo biométrico armazenado apenas em dispositivos na posse da pessoa singular, por exemplo num dispositivo individual mantido pelo mesmo, sob o seu controlo exclusivo, utilizado para autenticação em pontos de controlo específicos através de uma interface específica, apresenta, em determinadas condições, menos riscos em comparação com a utilização de dados biométricos que os armazena numa base de dados centralizada[55]. Esse armazenamento localizado, quando acompanhado de garantias adequadas[56], reduz a gravidade das violações de dados pessoais em comparação com o armazenamento centralizado, no que diz respeito ao número de pessoas afetadas, e garante que o acesso ao modelo biométrico implica uma participação ativa do titular dos dados.

41. Além disso, a correspondência pode ser efetuada localmente no aeroporto, comparando o modelo biométrico, por exemplo contido no código QR, com o resultado do modelo calculado com base na amostra biométrica captada pela câmara do módulo de controlo. O responsável pelo tratamento que efetua um controlo específico (nomeadamente um operador aeroportuário ou uma companhia aérea, consoante o controlo seja efetuado nos pontos de controlo de segurança, nos locais de entrega de bagagem, no embarque e no acesso às salas de espera) conhece e utiliza apenas o resultado da correspondência. Além disso, o facto de as informações necessárias para a correspondência (por exemplo, o código QR) terem de ser fornecidas pela pessoa singular resulta num segundo fator[57] que reforça a segurança da autenticação.

42. No que diz respeito à compatibilidade com o artigo 25.º do RGPD e tendo em vista, em especial, o cumprimento do requisito de minimização dos dados, importa garantir que o tratamento respeita o princípio da necessidade. No cenário 1, poderá considerar-se que as medidas escolhidas respeitam o princípio da necessidade em relação ao objetivo prosseguido (ou seja, racionalizar o fluxo de passageiros) se, dependendo das circunstâncias do tratamento, o responsável pelo tratamento puder demonstrar que não existem soluções alternativas menos intrusivas que possam alcançar o mesmo objetivo de forma igualmente eficaz. Por exemplo, o responsável pelo tratamento pode ser capaz de demonstrar que, mesmo que os passageiros tenham de mostrar o seu dispositivo, o cenário 1 acelera o processo de verificação em comparação com a situação atual, que inclui uma verificação humana da correspondência entre o nome no cartão de embarque e o documento de identidade do passageiro[58]. Nomeadamente, tal não poderia ser demonstrado se não existissem atualmente controlos para verificar a identidade dos passageiros com base no seu documento de identidade oficial (ver, a este respeito, o n.º 18 *supra*).

[55] Orientações 05/2022 do CEPD relativas ao reconhecimento facial na aplicação da lei, n.º 17.
[56] Tal como referido a partir do ponto 46 *infra*.
[57] Por exemplo, atenua o risco de mistificação da identidade. Ver também a garantia C.1.2 *infra*.
[58] É possível também argumentar que o controlo biométrico pode ser menos propenso a erros do que um controlo humano.

43. Além disso, os modelos biométricos não são conservados pelo operador aeroportuário após a inscrição e o prazo de conservação dos dados biométricos pelo responsável pelo tratamento que efetua o controlo é muito curto, uma vez que esses dados são apagados logo que a operação de correspondência é concluída. Assim, as medidas escolhidas no cenário 1 parecem limitar a extensão do tratamento e o prazo de conservação dos dados pessoais.

44. No que diz respeito ao princípio da proporcionalidade, o caráter intrusivo desse tratamento pode ser compensado pela participação ativa dos passageiros, uma vez que os seus dados biométricos se manteriam exclusivamente na sua posse. Além disso, tendo em conta as medidas acima descritas e partindo do princípio de que o responsável pelo tratamento aplica as garantias exigidas pelo tratamento em questão, a aplicação de medidas adequadas poderá garantir um nível de segurança adequado ao risco. Nesse caso, o impacto negativo nos direitos e liberdades fundamentais dos titulares dos dados pode ser considerado proporcional ao benefício esperado.

45. Por conseguinte, tendo em conta o que precede, em resposta à pergunta 1.1, o Comité conclui que esse tratamento **pode ser considerado, em princípio, compatível com o artigo 5.º, n.º 1, alínea f), e os artigos 25.º e 32.º do RGPD, sob reserva de garantias adequadas**.

Garantias adequadas

46. Neste tipo de cenário, em resposta à pergunta 1.2, o CEPD considera que devem ser aplicadas, pelo menos, as garantias a seguir descritas. Podem ser utilizadas outras garantias, para além das descritas no presente parecer, para alcançar os mesmos objetivos de segurança e de proteção de dados, e as mesmas podem ser lícitas, desde que garantam o cumprimento do quadro jurídico aplicável.

47. Nota: o que se segue é uma visão geral não exaustiva das possíveis garantias adequadas que devem ser aplicadas por um responsável pelo tratamento numa solução semelhante à do cenário 1. A sua adequação nos termos dos artigos 25.º e 32.º do RGPD dependerá de uma análise caso a caso. Todos os responsáveis pelo tratamento terão de assegurar que realizam a sua própria avaliação de impacto sobre a proteção de dados (a seguir designada por «AIPD»)[59], e as suas soluções específicas poderão exigir medidas adicionais não incluídas no presente parecer.

A. Aspetos gerais

A.1 Avaliação de impacto sobre o tratamento de dados

A.1.1 Realizar uma AIPD, em conformidade com os requisitos do artigo 35.º do RGPD, sempre que o responsável pelo tratamento preveja realizar uma nova operação de tratamento que envolva um tipo de tratamento suscetível de implicar um elevado risco. É provável que seja esse o caso no cenário 1, uma vez que envolve o tratamento de dados biométricos em grande escala[60]. Avaliar a adequação da aplicação de um sistema de reconhecimento facial, incluindo

[59] Artigo 35.º do RGPD.

[60] Artigo 35.º, n.º 3, do RGPD, e Orientações do Grupo de Trabalho do Artigo 29.º relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679, adotadas em 13 de outubro de 2017, WP248rev.01, aprovadas pelo CEPD.

a sua necessidade e proporcionalidade em relação aos objetivos prosseguidos[61], durante a fase inicial de conceção e revê-la ao longo de todo o ciclo de vida do desenvolvimento do produto;

A.1.2 Consultar a autoridade de controlo competente caso o tratamento continue a resultar num risco elevado, apesar das medidas tomadas pelo responsável pelo tratamento para atenuar o risco[62].

A.2 Direitos e garantias dos titulares dos dados que podem ser aplicados pelos responsáveis pelo tratamento

A.2.1 Garantias para corrigir casos de falsos negativos. Atenuar o risco de desequilíbrios em função da idade, do género e da raça avaliando «regularmente se os algoritmos estão a funcionar em consonância com as finalidades e ajustá-los para atenuar desequilíbrios detetados e garantir a lealdade no tratamento»[63], por exemplo, aplicando a supervisão e intervenção humanas, a fim de atenuar eventuais desequilíbrios e impedir a estigmatização ou a definição de perfis dos passageiros;

A.2.2 Assegurar que qualquer tratamento de dados pessoais é transparente e que as pessoas conhecem e controlam a forma como os seus dados são tratados para cada operação de tratamento[64];

A.2.3 Assegurar a existência de medidas para assegurar o respeito do princípio da limitação da finalidade, de modo que os dados não sejam utilizados para outros fins, como a segurança ou a formação;

A.2.4 Evitar a captação de fotografias ou vídeos, mesmo que não sejam gravados e tratados, de pessoas que não consentem no reconhecimento facial, através de medidas adequadas (como a utilização de uma profundidade de campo e de uma área de captação adequadas para evitar captar imagens de outros passageiros em fundo ou em redor, introduzindo filas específicas claramente identificadas para reconhecimento facial);

A.2.5 Sempre que os mesmos módulos possam ser utilizados por passageiros que tenham ou não consentindo no reconhecimento facial, ou quando passageiros que não tenham consentido no reconhecimento facial possam surgir no campo de visão enquanto o sistema não é utilizado, aguardar uma ação positiva por parte de um passageiro que tenha dado o seu consentimento antes de iniciar a captação de fotografias ou vídeos;

---

[61] Artigo 35.º, n.º 7, alínea b), do RGPD.
[62] Artigo 36.º, n.º 1, do RGPD.
[63] Orientações 4/2019 do CEPD relativas ao artigo 25.º – Proteção de Dados desde a Conceção e por Defeito, nota de rodapé 60, n.º 70.
[64] Orientações 4/2019 do CEPD relativas ao artigo 25.º – Proteção de Dados desde a Conceção e por Defeito, n.º 68, e considerando 7 do RGPD.

A.2.6 Possibilidade de o titular dos dados, em qualquer momento, proceder ao apagamento de dados que estejam exclusivamente na sua posse (modelo biométrico[65]), nomeadamente os armazenados numa aplicação móvel ou numa carteira digital[66];

A.2.7 Existência de alternativas viáveis ou de soluções de salvaguarda (nomeadamente para os passageiros que não consentiriam na utilização dos seus dados biométricos, para os passageiros que não poderiam utilizar essas soluções ou para os passageiros que são objeto de rejeições falsas), a fim de garantir também que os passageiros que não dão o seu consentimento não sejam prejudicados[67];

A.2.8 Se for utilizada uma aplicação, esta deve ser cuidadosamente concebida e configurada para não recolher dados desnecessários e de forma a evitar a utilização de conjuntos de desenvolvimento de *software* («SDK») de terceiros que recolham dados para outras finalidades.

A.3 Responsabilidade

A.3.1 Avaliar se existem códigos de conduta ou procedimentos de certificação pertinentes para ajudar a demonstrar a conformidade com a segurança do tratamento prevista no artigo 32.º do RGPD[68]. Verificar a adequação das medidas ao tratamento específico em questão. As normas[69], boas práticas e códigos de conduta reconhecidos por associações e outros organismos representativos de categorias de responsáveis pelo tratamento podem ser úteis na determinação de medidas adequadas;

A.3.2 Assegurar a realização de controlos de segurança básicos do dispositivo do utilizador, a fim de permitir a fase de inscrição, embora o passageiro também tenha um papel a desempenhar na proteção dos seus dados, uma vez que estes são conservados no seu dispositivo. A secção C.2 «Infraestruturas e redes» apresenta exemplos dessas verificações e controlos técnicos.

B. Aspetos organizativos:

B.1 Política e conformidade

[65] As referências ao modelo biométrico nas garantias para o cenário 1 correspondem a referências à chave ou segredo no cenário 2.
[66] Note-se que esta garantia aplica-se apenas ao cenário 1.
[67] Diretrizes 3/2019 do CEPD relativas aos dispositivos de vídeo, n.º 86.
[68] Artigo 32.º, n.º 3, do RGPD, e Orientações 4/2019 do CEPD relativas ao artigo 25.º – Proteção de Dados desde a Conceção e por Defeito, n.º 10.
[69] Ver, por exemplo, ISO/IEC 2382-37.

B.1.1. Assegurar a existência de controlos internos de acesso[70] com regras para os administradores;

B.1.2 Sempre que o serviço de reconhecimento facial possa ser prestado por uma das partes envolvidas no tratamento sem dados de identificação ou biométricos, ou ambos, que tenham de ser tratados pelas outras partes envolvidas, proibir o fluxo de dados nessas outras partes. Por exemplo, uma companhia aérea não precisa de acesso técnico aos dados biométricos quando se baseia na infraestrutura comum do aeroporto, mesmo que essa companhia aérea atue como responsável pelo tratamento ao abrigo do RGPD;

B.1.3 Definir uma política de encriptação e gestão de chaves[71], nomeadamente para o tratamento de DI e dados biométricos;

B.1.4 Assegurar a conformidade com o capítulo V do RGPD. Por exemplo, para assegurar transferências conformes se o responsável pelo tratamento utilizar um serviço à distância, baseado num país terceiro, durante o processo de inscrição;

B.1.5 Quando são utilizados subcontratantes, assegurar a existência de um contrato de subcontratação de tratamento de dados[72] em conformidade com o artigo 28.º, n.º 3, do RGPD;

B.1.6 Assegurar a existência de procedimentos para gerir a supervisão e a intervenção humanas, em especial para fazer face a problemas relacionados com rejeições falsas e questões técnicas ou relativas à facilidade de utilização.

B.2 Formação e testes

B.2.1. Assegurar que o pessoal recebe formação adequada;

B.2.2 Aplicar «[u]m processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento»[73].

B.2.3. Aplicar um processo para assegurar que o tratamento do modelo biométrico do passageiro[74] para autenticação é tecnicamente eficaz e suficientemente exato;

---

[70] Diretrizes 4/2020 do CEPD sobre a utilização de dados de localização e meios de rastreio de contactos no contexto do surto de COVID-19, adotadas em 21 de abril de 2020 (a seguir designadas por «**Diretrizes 4/2020 do CEPD sobre dados de localização e meios de rastreio de contactos**»), SEC-10, p. 19.
[71] Diretrizes 3/2019 do CEPD relativas aos dispositivos de vídeo, n.º 89.
[72] Artigo 28.º, n.º 3, do RGPD.
[73] Artigo 32.º, n.º 1, alínea d), do RGPD.
[74] As referências ao modelo biométrico nas garantias para o cenário 1 correspondem a referências à chave ou segredo no cenário 2.

B.2.4. Assegurar que as amostras biométricas recolhidas tanto no momento da inscrição como no ponto de controlo têm qualidade suficiente para a realização de um tratamento biométrico fiável.

C. Aspetos técnicos:

C.1 Acesso

C.1.1 Aplicar garantias durante a fase de inscrição para assegurar um processo de inscrição em *bootstrapping* com uma identidade verificada. Por exemplo, para reforçar a avaliação da autenticação multifatorial das identidades dos utilizadores, podem ser aplicadas etapas, desde ligações únicas protegidas por senha para ativar a aplicação até mecanismos locais de desbloqueio do dispositivo;

C.1.2 Aplicar garantias para fazer face a casos de falsos positivos e ataques baseados na aparência e prevenir fraudes[75];

C.1.3 Proibir qualquer acesso externo aos DI e aos dados biométricos[76];

C.1.4 Assegurar que o tratamento é efetuado localmente nas fases de inscrição, transmissão e correspondência. O ponto de correspondência deve encontrar-se o mais próximo possível do dispositivo da pessoa singular. Permitir a correspondência de modelos no dispositivo individual pode exigir uma interação com prestadores de serviços localizados fora do aeroporto e implicar a utilização de recursos da rede pública, o que tem como desvantagem o facto de afetar a disponibilidade do modelo e a sua transmissão a entidades externas;

C.1.5 Autenticar um utilizador para adicionar um novo voo e gerar um novo código QR encriptado;

C.1.6 Aplicar medidas para fazer face a situações em que um passageiro pode perder o acesso ao seu código QR.

C.2 Infraestruturas e redes

C.2.1 Subordinar o funcionamento da aplicação/carteira digital à atualização do sistema operativo («SO») e à ativação da autenticação para acesso ao dispositivo, nomeadamente através do apagamento automático de DI e dados biométricos se o SO estiver desatualizado e representar riscos de segurança;

[75] Relatório da ENISA intitulado *Digital Identity: Leveraging the SSI Concept to Build Trust* (Identidade digital: aproveitar o conceito de identidade autossoberana para reforçar a confiança), janeiro de 2022.
[76] Diretrizes 3/2019 do CEPD relativas aos dispositivos de vídeo, n.º 89.

C.2.2 Isolar as unidades de correspondência (ou seja, os módulos) da rede durante o funcionamento e tomar todas as outras medidas necessárias para garantir a segurança;

C.2.3 Realizar as correspondências biométricas no dispositivo do passageiro ou no módulo (computação periférica);

C.2.4 Soluções para fazer face às vulnerabilidades de segurança dos dispositivos individuais dos passageiros, incluindo a encriptação para (no mínimo) dados biométricos e de identificação inativos;

C.2.5 Utilizar o armazenamento seguro para (pelo menos) dados biométricos exclusivamente na posse do utilizador[77], por exemplo utilizando um enclave seguro num telemóvel inteligente;

C.2.6 Salvaguardas de segurança para garantir a segurança física das instalações, incluindo o terminal biométrico do aeroporto. Garantir um elevado nível de segurança dos elementos da arquitetura que tratam DI e dados biométricos (por exemplo, computação, fluxo de dados, armazenamento transitório ou a longo prazo).

C.3 Segurança e gestão dos dados de controlo de identidade do utilizador

C.3.1 Compartimentar os dados durante a transmissão e o armazenamento em, pelo menos, três grupos diferentes, tais como: DI, dados biométricos e dados de voo[78]. Assegurar que os dados estão adequadamente encriptados entre a transmissão e o armazenamento;

C.3.2 Introduzir medidas técnicas para garantir que, no posto de controlo, apenas são tratados e verificados os dados que podem ser objeto de um tratamento lícito em pontos de controlo específicos;

C.3.3 Assegurar a eficácia do apagamento de dados[79] através de um procedimento de apagamento seguro (por exemplo, memória principal, cache, eventuais cópias de segurança) e avaliar em que momentos se deve automatizar o apagamento dos dados. Os prazos de conservação dos dados devem ser rigorosamente aplicados através de rotinas automáticas, sem necessidade de uma ação suplementar por parte da pessoa singular[80];

C.3.4 Assegurar a autenticidade e a integridade dos dados (por exemplo, assinatura)[81];

[77] As referências ao modelo biométrico nas garantias para o cenário 1 correspondem a referências à chave ou segredo no cenário 2.
[78] Diretrizes 3/2019 do CEPD relativas aos dispositivos de vídeo, n.º 89.
[79] Diretrizes 3/2019 do CEPD relativas aos dispositivos de vídeo, n.º 89.
[80] Orientações 4/2019 do CEPD relativas ao artigo 25.º – Proteção de Dados desde a Conceção e por Defeito, n.º 82.
[81] Diretrizes 3/2019 do CEPD relativas aos dispositivos de vídeo, n.º 89.

C.3.5 Conservar os dados biométricos dos passageiros no ponto de inscrição e no ponto de controlo apenas durante um período muito curto e apagá-los logo que o passageiro passe pelo ponto de controlo;

C.3.6 Se for utilizada uma aplicação para a inscrição, pôr em prática normas de segurança para aplicações móveis durante o desenvolvimento das mesmas, bem como testes de segurança realizados por terceiros;

C.3.7 Assegurar a aplicação de medidas de segurança durante a fase de inscrição no aeroporto, a fim de preservar a confidencialidade e a integridade dos dados biométricos dos passageiros. Por exemplo, se o código QR for impresso pelo terminal, não deve ser exibido nesse local, para evitar que um interveniente mal-intencionado tire uma fotografia. Nos casos de transmissão de curto alcance, a transmissão deve contar com a participação ativa do utilizador e ser realizada através de um canal que garanta a proximidade;

C.3.8 Os dados que estejam exclusivamente na posse da pessoa singular[82] devem ser conservados em armazenamento seguro no dispositivo e quaisquer eventuais vulnerabilidades relacionadas com os sistemas operativos do dispositivo devem ser objeto das correções de segurança adequadas. No caso de um código QR impresso, a pessoa singular deve ser informada da natureza particularmente sensível dos dados que o código contém e das ações que o mesmo permite executar;

C.3.9 Assegurar que a inscrição é efetuada de acordo com técnicas adequadas de prova de identidade à distância[83].

3.2.2 Cenário 2: armazenamento centralizado de um modelo biométrico inscrito em forma encriptada no aeroporto e com uma chave ou segredo exclusivamente na posse dos passageiros, para autenticação

48. A presente secção analisa a compatibilidade com o artigo 5.º, n.º 1, alíneas e) e f), e os artigos 25.º e 32.º do RGPD do armazenamento centralizado, para autenticação, dos modelos biométricos dos passageiros inscritos numa base de dados centralizada, em forma encriptada e com uma chave ou segredo exclusivamente na posse do passageiro[84] («**cenário 2**»). A presente secção analisa igualmente as garantias adequadas para o cenário 2, à luz dos artigos 25.º e 32.º do RGPD.

Descrição do cenário

49. No cenário 2, a inscrição é feita apenas uma vez, com um determinado período de validade (por exemplo, um ano desde o último voo até ao termo da validade do passaporte), e pode ser realizada à

[82] As referências ao modelo biométrico nas garantias para o cenário 1 correspondem a referências à chave ou segredo no cenário 2.
[83] Ver relatório da ENISA intitulado *Remote ID Proofing: Analysis of methods to carry out identity proofing remotely* (Prova de ID à distância: análise dos métodos para a realização da prova de identidade à distância), março de 2021.
[84] Como exemplificado pelo caso de utilização 2 constante do anexo I do pedido.

distância, com um nível de garantia de identidade adequado (por exemplo, nível de garantia adequado eIDAS) ou em terminais de aeroportos. A inscrição é controlada pelo operador aeroportuário e consiste na geração de DI e dados biométricos encriptados com uma chave ou segredo.

50. A base de dados é armazenada nas instalações do aeroporto, sob o controlo do operador aeroportuário. As chaves ou segredos de encriptação específicos são armazenados apenas no dispositivo da pessoa singular (por exemplo, na aplicação móvel do operador aeroportuário). A aplicação pode gerar um código QR que contém a chave ou segredo, e esse código pode ser impresso em papel ou exibido no ecrã do dispositivo[85]. Além disso, o operador aeroportuário aplica um segundo nível de encriptação[86], com chaves controladas por esse operador.

51. Os passageiros são autenticados (comparação 1:1) quando passam por pontos de controlo específicos no aeroporto. Os passageiros que optam por passar pelos pontos de controlo biométricos mostram o seu código QR num módulo de controlo específico equipado com um leitor de códigos QR e uma câmara. O índice do passageiro é enviado para a base de dados para solicitar o modelo encriptado, que é descarregado e verificado localmente no módulo e/ou no dispositivo do utilizador. O responsável pelo tratamento do ponto de controlo conhece e utiliza apenas o resultado da correspondência[87].

52. Neste cenário, não existem fluxos de DI e dados biométricos entre aeroportos, como também não há interligação nem interoperabilidade entre as bases de dados centralizadas.

Avaliação do CEPD

53. No cenário 2, os modelos biométricos inscritos dos passageiros são armazenados de forma centralizada, mas de forma encriptada e com uma chave ou segredo exclusivamente na posse dos passageiros. No cenário 2, os passageiros são autenticados (comparação 1:1).

54. Este cenário pressupõe que é possível alcançar o objetivo de racionalizar o fluxo de passageiros (ou seja, aumentar a velocidade dos controlos) utilizando um sistema centralizado. O CEPD observou anteriormente que essa solução podia ser considerada uma alternativa viável ao armazenamento descentralizado dos modelos biométricos inscritos[88] (tal como descrito no cenário 1) se existissem necessidades objetivas e fossem utilizadas garantias adequadas (ver garantias descritas no n.º 60 *infra*).

55. Em termos de considerações de segurança, os dados de cada pessoa singular são encriptados com a chave específica conservada apenas pela pessoa singular e sob o seu controlo exclusivo. Além disso, o facto de as informações necessárias para a correspondência (ou seja, o segredo ou chave) terem de ser fornecidas pela pessoa singular resulta num segundo fator[89] que reforça a segurança da

[85] A AC FR esclareceu igualmente que poderão existir outras soluções técnicas para enviar as informações necessárias, nomeadamente através da utilização de um protocolo de comunicação de curto alcance.
[86] A própria chave ou segredo (na posse da pessoa singular) é encriptada com outra chave detida pelo operador aeroportuário.
[87] A AC FR esclareceu que este período de armazenamento é ilustrativo e pode ser considerado aceitável, uma vez que a chave é mantida na posse da pessoa singular e pode ser escolhida na fase de inscrição. No entanto, importa notar que esse prazo de conservação pode ser ajustado.
[88] Diretrizes 3/2019 do CEPD relativas aos dispositivos de vídeo, n.º 88.
[89] Por exemplo, atenua o risco de mistificação da identidade. Ver também a garantia C.1.2.

autenticação. Além disso, o operador aeroportuário aplica um segundo nível de encriptação, com chaves controladas por esse operador. No cenário 2, o índice da pessoa singular é enviado para a base de dados central, a fim de obter os dados biométricos associados a essa pessoa. Estes dados são depois enviados (encriptados) para um computador localizado no ponto de controlo, onde são desencriptados a fim de efetuar a correspondência, e o responsável pelo tratamento do ponto de controlo conhece e utiliza apenas o resultado da correspondência. Por conseguinte, desde que a chave ou segredo da pessoa seja conservada no computador localizado no ponto de controlo e que apenas seja enviado um índice do passageiro para a base de dados central para recuperar o modelo biométrico encriptado, essas medidas de segurança podem ser consideradas compatíveis com o artigo 5.º, n.º 1, alínea f), e o artigo 32.º do RGPD.

56. No que diz respeito à compatibilidade com o artigo 25.º do RGPD e tendo em vista, em especial, o cumprimento do requisito de minimização dos dados, importa garantir que o tratamento respeita o princípio da necessidade. No cenário 2, poderá considerar-se que as medidas escolhidas respeitam o princípio da necessidade em relação ao objetivo prosseguido (ou seja, racionalizar o fluxo de passageiros nos aeroportos) se, dependendo das circunstâncias do tratamento, o responsável pelo tratamento puder demonstrar que não existem soluções alternativas menos intrusivas que possam alcançar o mesmo objetivo de forma igualmente eficaz. No cenário 2, os passageiros continuariam a ter de mostrar o seu dispositivo[90]. No entanto, o responsável pelo tratamento pode ser capaz de demonstrar que o cenário 2 acelera o processo de verificação em comparação com a situação atual, que inclui uma verificação humana da correspondência entre o nome no cartão de embarque e o documento de identidade do passageiro[91], ou em comparação com o cenário 1. Nomeadamente, tal não poderia ser demonstrado se não existissem atualmente controlos para verificar a identidade dos passageiros com base no seu documento de identidade oficial (ver, a este respeito, o n.º 18 *supra*).

57. No que diz respeito ao princípio da proporcionalidade, o caráter intrusivo desse tratamento pode ser compensado pela participação ativa dos passageiros, que mantêm o controlo exclusivo da chave dos seus dados encriptados. Além disso, afigura-se possível, através da utilização de garantias adequadas, atenuar os riscos de segurança decorrentes do armazenamento dos dados biométricos dos passageiros numa base de dados centralizada com a chave exclusivamente na posse dos passageiros (ver garantias abordadas no n.º 60 *infra*). Por conseguinte, partindo do princípio de que o responsável pelo tratamento aplica as garantias exigidas pelo tratamento em questão, os riscos para as pessoas singulares podem ser atenuados e o impacto negativo nos direitos e liberdades fundamentais dos titulares dos dados pode ser considerado proporcional ao benefício esperado. É evidente que, em cada caso, cumpre garantir que apenas os dados necessários para a finalidade em causa sejam tratados e que apenas os passageiros que tenham dado o seu consentimento sejam controlados, para que não exista o risco de serem recolhidos dados biométricos de outros passageiros que não deram o seu consentimento.

58. No pedido, afirma-se a título de exemplo que, no cenário 2, o prazo de conservação dos dados encriptados na base de dados pode ser normalmente de um ano entre o último voo efetuado pela

[90] A AC FR esclareceu igualmente que podiam existir outras opções para apresentar um modelo, por exemplo, impresso em papel. Além disso, o CEPD reconhece que, no futuro, poderá prever-se a utilização de uma tecnologia alternativa, por exemplo, baseada num sistema de comunicação de campo próximo.

[91] É possível também argumentar que o controlo biométrico pode ser menos propenso a erros do que um controlo humano.

pessoa singular e o termo da validade do passaporte. O pedido não contém informações para fundamentar um prazo tão longo com base em razões objetivas, embora se possa presumir que esse prazo de conservação vise uma maior conveniência em voos futuros. No que diz respeito ao prazo de conservação, a fim de alcançar a compatibilidade com o artigo 5.º, n.º 1, alínea e), do RGPD neste cenário, os responsáveis pelo tratamento devem poder justificar por que motivo esse prazo de conservação é necessário para a finalidade em questão em casos específicos. O Comité recomenda aos responsáveis pelo tratamento que prevejam o prazo de conservação mais curto possível, tendo igualmente em conta os passageiros que voam muito raramente, e que ofereçam aos titulares dos dados a possibilidade de fixarem o prazo de conservação que preferirem.

59. À luz destas considerações, em resposta à pergunta 2.1.1, o Comité conclui que esse tratamento **pode ser considerado, em princípio, compatível com o artigo 5.º, n.º 1, alíneas e) e f), e os artigos 25.º e 32.º do RGPD, sob reserva de garantias adequadas**.

Garantias adequadas

60. Neste tipo de cenário, em resposta à pergunta 2.1.2, o Comité considera que, **para além das garantias enumeradas no cenário 1**, devem ser aplicadas, pelo menos, as garantias a seguir descritas. Podem ser utilizadas outras garantias, para além das descritas no presente parecer, para alcançar os mesmos objetivos de segurança e de proteção de dados, e as mesmas podem ser lícitas, desde que garantam o cumprimento dos quadros jurídicos aplicáveis.

61. Nota: *o que se segue é uma visão geral não exaustiva das possíveis garantias adequadas que podem ser aplicadas por um responsável pelo tratamento numa solução semelhante à do cenário 2. A sua adequação nos termos dos artigos 25.º e 32.º do RGPD dependerá de uma análise caso a caso. Todos os responsáveis pelo tratamento terão de assegurar que realizam a sua própria AIPD, e as suas soluções específicas poderão exigir medidas adicionais não incluídas no presente parecer.*

D. Aspetos gerais

D.1 Direitos e garantias dos titulares dos dados que podem ser aplicados pelos responsáveis pelo tratamento

D.1.1 Assegurar que o passageiro tem controlo sobre os prazos de conservação de todos os seus dados. Os prazos de conservação devem limitar-se ao necessário para a finalidade específica. Deve ser fixado um prazo máximo na sequência de uma análise exaustiva de fatores como a validade do documento de identificação. Os titulares dos dados devem ter a possibilidade de fixar o prazo de conservação que preferirem, que poderá ser mais curto do que o prazo de conservação por defeito;

D.1.2 Possibilidade de o titular dos dados, em qualquer momento, solicitar o apagamento de dados que estejam exclusivamente na sua posse (chave ou segredo), nomeadamente os conservados numa aplicação móvel ou numa carteira digital[92];

[92] Note-se que esta garantia aplica-se apenas ao cenário 2.

D.1.3 Assegurar que a localização da base de dados central permite uma supervisão eficaz por parte da autoridade de controlo competente.

E. Aspetos organizativos:

E.1 Política e conformidade

E.1.1 A confiança no servidor central deve ser limitada. Assegurar que a gestão do servidor central segue regras de governação claramente definidas e inclui todas as medidas necessárias para garantir a sua segurança[93].

F. Aspetos técnicos:

F.1 Acesso

F.1.1 Manter registos dos utilizadores com acesso a dados pessoais, em especial DI e dados biométricos, e dos momentos em que estes foram consultados;

F.2 Infraestruturas e redes

F.2.1 Proteger adequadamente a base de dados central, incluindo contra ataques baseados na disponibilidade;

F.2.2 Assegurar que não existe ligação Internet à base de dados central, aos módulos de inscrição e às unidades de correspondência. O funcionamento e a manutenção deste sistema (por exemplo, cópias de segurança, correções, monitorização, etc.) devem ser realizados localmente nas instalações do aeroporto.

F.3 Segurança e gestão dos dados

F.3.1 Aplicar técnicas criptográficas de última geração para proteger os intercâmbios entre a aplicação e o servidor centralizado[94];

F.3.2 Manter a chave ou segredo individual ao nível em que será utilizada para desencriptar (designadamente no módulo) e utilizar o índice apenas para recuperar o modelo biométrico correspondente inscrito na base de dados central;

F.3.3 Assegurar que o intercâmbio da chave ou segredo entre o dispositivo do utilizador e o módulo protege a comunicação contra qualquer possível interceção ou transmissão a terceiros;

[93] Diretrizes 4/2020 do CEPD sobre dados de localização e meios de rastreio de contactos, PRIV-5, p. 20.
[94] Diretrizes 4/2020 do CEPD sobre dados de localização e meios de rastreio de contactos, SEC-4, p. 18: «Entre os exemplos de técnicas que podem ser utilizadas incluem-se, por exemplo: a cifragem simétrica e assimétrica, funções de dispersão, o teste de pertença a uma associação privada, a intersecção de conjuntos privados, filtros de Bloom, recuperação de informações privadas, cifragem homomórfica, etc.»

F.3.4 Indexar o modelo biométrico quando armazenado na base de dados central para permitir a autenticação 1:1 e garantir que é único e está relacionado com a pessoa. Assegurar que o índice não revela nenhuma das informações de identificação do passageiro e não está correlacionado com a chave de encriptação;

F.3.5 Autenticar e encriptar adequadamente qualquer transmissão entre a base de dados central e os pontos de controlo e colocá-la em redes isoladas;

F.3.6 Evitar ligações bidirecionais entre conjuntos de dados (DI e dados biométricos, bem como dados de voo) e manter apenas as ligações unidirecionais pertinentes na base de dados. Por exemplo, apenas as ligações unidirecionais do índice aos DI, do índice aos dados biométricos encriptados e do índice aos dados de voo;

F.3.7 Assegurar mecanismos de continuidade operacional, por exemplo dispondo de sistemas de armazenamento de cópias de segurança adequados;

F.3.8 Assegurar que o módulo não mantém registos dos modelos encriptados ou não encriptados.

3.2.3 Armazenamento centralizado dos modelos biométricos inscritos para identificação

62. A presente secção analisa a compatibilidade com o artigo 5.º, n.º 1, alíneas e) e f), e os artigos 25.º e 32.º do RGPD do armazenamento centralizado, para identificação, dos modelos biométricos inscritos dos passageiros, em que esses modelos não estão encriptados com uma chave ou segredo exclusivamente na posse dos passageiros, em dois casos de utilização: 1) quando esses modelos são armazenados numa base de dados no aeroporto, sob o controlo do operador aeroportuário[95] («**cenário 3.1**»), e 2) quando esses modelos são armazenados na nuvem, sob o controlo da companhia aérea[96] («**cenário 3.2**»).

63. O Comité considera que a utilização de dados biométricos para efeitos de **identificação** em grandes bases de dados centrais interfere com os direitos fundamentais dos titulares dos dados e pode ter consequências graves para os titulares dos dados[97]. Além disso, a utilização de dados biométricos deve também ser analisada em relação à finalidade para a qual são tratados, à luz dos princípios da necessidade e da proporcionalidade[98].

[95] Como exemplificado pelo caso de utilização 3A constante do anexo I do pedido.
[96] Como exemplificado pelo caso de utilização 3B constante do anexo I do pedido.
[97] Ver, por exemplo, o Parecer 3/2012 do Grupo do Artigo 29.º relativo às tecnologias biométricas, p. 9. Ver também o n.º 26 *supra*.
[98] Considerando 4 do RGPD. Ver também o Parecer 3/2012 do Grupo do Artigo 29.º relativo às tecnologias biométricas, p. 9.

3.2.3.1 *Cenário 3.1: armazenamento centralizado numa base de dados no aeroporto, sob o controlo do operador aeroportuário*

Descrição do cenário

64. No cenário 3.1, o modelo biométrico inscrito dos passageiros é armazenado numa base de dados central nas instalações do aeroporto e sob o controlo do operador aeroportuário em forma encriptada. Em especial, os dados dos passageiros são compartimentados, o que significa que os seus dados de identificação, o modelo biométrico inscrito e as informações de voo são armazenados em três bases de dados diferentes. Esses dados são encriptados com diferentes chaves, tanto durante o armazenamento como quando são transmitidos aos servidores que efetuam a correspondência, onde são depois desencriptados pelo operador aeroportuário.

65. Os passageiros devem inscrever-se para cada voo, num curto espaço de tempo antes da partida (por exemplo, 48 horas). Essa inscrição pode ser efetuada à distância ou nos terminais dos aeroportos com um nível de garantia de identidade adequado (por exemplo, nível de garantia adequado eIDAS). Em alternativa, a inscrição pode revestir a mesma forma descrita no cenário 1, caso em que os passageiros têm de transferir os seus dados das suas carteiras digitais para o sistema do aeroporto no prazo de 48 horas antes da partida.

66. Também neste cenário, os passageiros apresentam-se perante um módulo de controlo específico equipado com uma câmara. A sua amostra biométrica é depois enviada para um servidor central do aeroporto, que tentará estabelecer a correspondência entre os dados e a base de dados biométrica central. Tal permite identificar o passageiro e verificar se está ou não registado para um voo de partida (ou para o embarque em caso de controlo no embarque). Dependendo do ponto de controlo, é possível minimizar os dados devolvidos ao responsável pelo tratamento do ponto de controlo que os solicita, por exemplo, através de uma «resposta sim/não» ou do próprio resultado da correspondência, se necessário. Neste caso, o responsável pelo tratamento do ponto de controlo recebe e utiliza apenas o resultado do pedido.

67. Em especial, neste cenário, os passageiros são identificados (comparação 1:N), sendo N o número de passageiros previsto no aeroporto num período de vários dias. Além disso, as correspondências biométricas só são efetuadas quando cada passageiro se apresenta em pontos de controlo predefinidos no aeroporto de partida, mas o próprio tratamento de dados é efetuado num servidor central ligado à base de dados central. Neste cenário, o prazo de conservação é normalmente de 48 horas e os dados são apagados após a descolagem do avião.

Avaliação do CEPD

68. Tal como acima referido, o tratamento de dados biométricos implica riscos acrescidos para os direitos e liberdades dos titulares dos dados[99]. Por conseguinte, qualquer falha na segurança dos dados pode ter consequências particularmente graves para os titulares dos dados[100]. Os responsáveis pelo tratamento são obrigados a atenuar eficazmente esses riscos. Uma vez que, neste cenário, toda a

[99] Ver n.º 26 *supra*.

[100] *Guidelines on facial recognition* (Diretrizes sobre o reconhecimento facial), Comité Consultivo da Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, junho de 2021, p. 22.

arquitetura está totalmente centralizada, os passageiros perdem mais controlo sobre os seus dados. Além disso, pode aumentar o risco de os dados acabarem por ser tratados para outras finalidades que não o controlo do fluxo de passageiros.

69. À luz do princípio e dos requisitos em matéria de segurança (artigo 5.º, n.º 1, alínea f), e artigo 32.º do RGPD), deve considerar-se que o armazenamento de DI e de dados biométricos em bases de dados centrais, ainda que separadas, pode proporcionar valiosos pontos de ataque, e que uma violação da confidencialidade dessa base de dados pode posteriormente implicar o acesso a todo o conjunto de dados. Consequentemente, uma eventual violação dos modelos de reconhecimento facial e dos DI conexos pode permitir a identificação não autorizada ou ilícita dos titulares dos dados noutros ambientes. Pode também, dependendo dos métodos utilizados para a identificação biométrica, ameaçar a posterior utilização segura de modelos de reconhecimento facial como identificador. Nesse caso, não é possível atenuar os efeitos da violação, ao contrário do que acontece com outro tipo de credenciais (por exemplo, nome do utilizador, senha) que podem ser alteradas[101].

70. Além disso, a elevada quantidade e qualidade dos DI e dos dados biométricos detidos pelo responsável pelo tratamento torna-os um alvo muito valioso para um atacante, o que aumenta a probabilidade de riscos de segurança. Acresce que as violações de dados podem ter um maior impacto, uma vez que, devido ao armazenamento de dados numa localização centralizada, poderá ser mais fácil para os atacantes acederem a dados pessoais relativos a vários passageiros. Por conseguinte, uma eventual violação poderia expor um grande número de titulares de dados a riscos de elevada gravidade, por exemplo, a usurpação de identidade em grande escala, que são extremamente difíceis de atenuar.

71. Por conseguinte, no que diz respeito à compatibilidade com o artigo 5.º, n.º 1, alínea f), e o artigo 32.º do RGPD, as medidas previstas no cenário 3.1[102], tendo em conta as técnicas mais avançadas, são insuficientes para garantir um nível de segurança adequado ao risco. Nesta base, o tratamento no âmbito do cenário 3.1 não cumpriria o disposto no artigo 5.º, n.º 1, alínea f), e no artigo 32.º do RGPD se um responsável pelo tratamento se limitasse às medidas nele descritas.

72. À luz do princípio do artigo 5.º, n.º 1, alínea e), do RGPD, neste cenário, o prazo de conservação de dados biométricos na base de dados central é normalmente de 48 horas. Esta limitação da conservação parece reduzir significativamente os riscos associados a violações de dados pessoais. No entanto, o prazo de conservação dos dados não é um fator decisivo, em si mesmo, para a compatibilidade global da referida arquitetura, uma vez que esses prazos de conservação podem estar sujeitos a alterações por parte dos responsáveis pelo tratamento. Em todo o caso, as medidas propostas têm de cumprir os requisitos da proteção de dados desde a conceção e por defeito, nos termos do artigo 25.º do RGPD.

73. Ao contrário dos cenários 1 e 2, em que os passageiros são autenticados, no cenário 3.1 os passageiros são identificados (comparação 1:N), sendo N o número de passageiros previsto no aeroporto, num período de vários dias, que deram o seu consentimento para esse tratamento ao passar por pontos de controlo específicos no aeroporto. Tal implica a pesquisa de passageiros numa base de dados central, através do tratamento de cada amostra biométrica captada para verificar se corresponde a uma pessoa conhecida do sistema. Ao contrário do que sucede no cenário 2, no cenário 3.1 as chaves

[101] Ver, a este respeito, o Parecer 3/2012 do Grupo do Artigo 29.º relativo às tecnologias biométricas, p. 39.
[102] Conforme descrito nos n.os 64 a 67 *supra*.

não são mantidas apenas na posse dos passageiros. Por conseguinte, neste cenário, os passageiros têm muito menos controlo sobre os seus dados biométricos. Assim, o tratamento proposto no âmbito do cenário 3.1 não pode ser compatível com os requisitos da proteção de dados desde a conceção e por defeito previstos no artigo 25.º do RGPD.

74. À luz do artigo 25.º do RGPD, os responsáveis pelo tratamento devem ter em consideração os tipos, as categorias e o nível de pormenor dos dados pessoais necessários para efeitos do tratamento[103]. As suas escolhas em termos de conceção devem ter em conta os riscos acrescidos para os princípios da minimização dos dados, da integridade e confidencialidade e da limitação da conservação ao recolherem grandes quantidades de dados pessoais pormenorizados e compará-los com os riscos reduzidos da recolha de menos informações e/ou de informações menos pormenorizadas sobre os titulares dos dados. Em todo o caso, a configuração por defeito não deve incluir a recolha de dados pessoais que não sejam necessários para a finalidade específica do tratamento. Por outras palavras, se determinadas categorias de dados pessoais forem desnecessárias ou se não forem necessários dados pormenorizados por serem suficientes dados menos granulares, não devem ser recolhidos quaisquer dados pessoais excedentários. No caso em apreço, se outra forma de execução do tratamento puder alcançar o mesmo objetivo e estiver disponível de acordo com os termos descritos no cenário 3.1, não é necessário utilizar a tecnologia de reconhecimento facial.

75. No que diz respeito ao artigo 25.º do RGPD, um elemento fundamental da proteção de dados desde a conceção e por defeito é a autonomia do titular dos dados. Em especial, os titulares dos dados devem beneficiar do mais elevado grau de autonomia possível para determinar a utilização dos seus dados pessoais, bem como em relação ao âmbito e às condições dessa utilização ou tratamento[104]. No cenário 1, o titular dos dados teria autonomia e controlo no que respeita à utilização, divulgação e apagamento dos seus modelos biométricos e, no cenário 2, manteria algum controlo sobre a divulgação do seu próprio modelo biométrico, uma vez que a chave ou segredo de encriptação ficaria em sua posse. No entanto, no cenário 3.1, o titular dos dados depende totalmente das escolhas do responsável pelo tratamento no que diz respeito ao tratamento dos seus dados biométricos e, por conseguinte, não tem qualquer controlo direto sobre a utilização do seu modelo biométrico.

76. No que diz respeito à compatibilidade com o artigo 25.º do RGPD e tendo em vista, em especial, o cumprimento do requisito de minimização dos dados, o tratamento previsto no cenário 3.1 não pode respeitar o princípio da necessidade. O Comité considera que é possível alcançar um resultado semelhante em termos de racionalização do fluxo de passageiros nos aeroportos de forma menos intrusiva para a privacidade. Por exemplo, é possível alcançar esse resultado sem a utilização de dados biométricos (embora, nesse caso, a experiência do utilizador seja diferente, uma vez que poderá demorar mais tempo a mostrar o seu cartão de embarque e, se necessário, os documentos oficiais de identificação). Além disso, outras soluções, nomeadamente as que se baseiam no armazenamento dos dados biométricos numa carteira local no dispositivo da pessoa singular ou as que exigem a encriptação dos dados com uma chave específica armazenada nesse dispositivo, permitem alcançar os objetivos de uma forma menos intrusiva para a privacidade.

---

[103] Orientações 4/2019 do CEPD relativas à proteção de dados desde a conceção e por defeito, n.º 49.

[104] Orientações 4/2019 do CEPD relativas à proteção de dados desde a conceção e por defeito, n.º 70. O considerando 7 do RGPD clarifica igualmente que «[a]s pessoas singulares deverão poder controlar a utilização que é feita dos seus dados pessoais».

77. No que diz respeito ao princípio da proporcionalidade, o tratamento previsto no cenário 3.1 criaria riscos para os direitos dos titulares dos dados, que, tendo em conta as técnicas mais avançadas, não seriam atenuados pelas garantias previstas. O risco de impacto negativo nos direitos e liberdades fundamentais dos titulares dos dados que poderia resultar de uma violação de dados numa base de dados centralizada de dados biométricos de um grande número de pessoas singulares parece ser superior ao benefício esperado resultante do tratamento, uma vez que esse benefício, ou seja, um ligeiro aumento da conveniência e da rapidez dos controlos, é relativamente reduzido. Por conseguinte, não pode justificar o elevado nível de ingerência dessas medidas nos direitos e liberdades fundamentais das pessoas singulares, e o tratamento previsto no cenário 3.1 não respeita o princípio da proporcionalidade.

78. À luz destas considerações, em resposta à pergunta 2.2.1, o Comité conclui que, quando o tratamento é efetuado com a finalidade específica de racionalizar o fluxo de passageiros nos aeroportos, o tratamento previsto no cenário 3.1:

- **não pode ser compatível com o artigo 25.º do RGPD**;
- **não cumpriria o disposto no artigo 5.º, n.º 1, alínea f), e no artigo 32.º do RGPD** se um responsável pelo tratamento se limitasse às medidas descritas no cenário 3.1.

3.2.3.2 Cenário 3.2: armazenamento centralizado em nuvem, sob o controlo da companhia aérea

Descrição do cenário

79. No cenário 3.2, o modelo biométrico inscrito dos passageiros é armazenado na nuvem, sob o controlo da companhia aérea ou do seu prestador de serviços de computação em nuvem (subcontratante). No pedido, especifica-se que o prestador de serviços de computação em nuvem estaria localizado no EEE[105]. Neste caso, os dados dos passageiros estão encriptados, mas são desencriptados quando estão a ser utilizados (por exemplo, quando a operação de correspondência é realizada) e as chaves são controladas pela companhia aérea ou pelo seu subcontratante que presta os serviços de computação em nuvem. Os dados biométricos dos passageiros são utilizados para a identificação dos passageiros (comparação 1:N), podendo N atingir o número total de clientes da companhia aérea[106].

80. À semelhança dos cenários 1, 2 e 3.1, também neste caso é necessária a inscrição prévia dos passageiros. No entanto, no cenário 3.2, a inscrição dos passageiros é feita uma vez, mantendo-se enquanto o cliente for titular de uma conta junto da companhia aérea. A inscrição é feita à distância, com um nível de garantia de identidade adequado (por exemplo, nível de garantia adequado eIDAS) ou nos terminais dos aeroportos. As correspondências biométricas só são efetuadas quando os passageiros se apresentam em pontos de controlo predefinidos no aeroporto, mas o tratamento de dados propriamente dito é efetuado na nuvem.

81. No aeroporto, os passageiros passam por módulos de controlo específicos, equipados com uma câmara. Os dados biométricos dos passageiros são enviados através de um pedido para um servidor em nuvem de uma companhia aérea, onde é efetuada a comparação destes dados com a base de dados central. Tal permite identificar o passageiro e verificar se está ou não registado para um voo de partida (ou para o embarque em caso de controlo no embarque).

82. É possível que os resultados da comparação sejam disponibilizados a vários operadores aeroportuários que disponibilizam a uma companhia aérea um terminal específico ou o acesso à infraestrutura comum do sistema de informação de um aeroporto. Dependendo do ponto de controlo, é possível minimizar os dados devolvidos ao responsável pelo tratamento do ponto de controlo que os solicita, por exemplo, através de uma «resposta sim/não» ou do próprio resultado da correspondência, se necessário. Neste caso, o responsável pelo tratamento do ponto de controlo conhece e utiliza apenas o resultado do pedido.

83. O prazo de conservação do modelo é definido pela companhia aérea e pode eventualmente vigorar enquanto o cliente for titular de uma conta junto da companhia aérea.

Avaliação do CEPD

[105] A AC FR esclareceu que o exemplo é ilustrativo e que também poderia ser contemplado o recurso a prestadores de serviços de computação em nuvem localizados no EEE. Além disso, poderiam também ser previstas outras soluções de armazenamento (por exemplo, sem utilizar a computação em nuvem).
[106] A AC FR esclareceu que o exemplo é ilustrativo e que existe uma solução em que os dados biométricos são transferidos antes de cada voo.

84. As considerações já expressas pelo Conselho em relação ao cenário 3.1[107] também se aplicam a este cenário.

85. No que diz respeito ao princípio e aos requisitos em matéria de segurança (artigo 5.º, n.º 1, alínea f), e artigo 32.º do RGPD), o tratamento no cenário 3.2 é efetuado na nuvem e várias entidades podem ter acesso a esses dados, incluindo, eventualmente, prestadores de serviços fora do EEE, mesmo quando os dados são conservados neste último[108]. Essa arquitetura implica riscos potenciais no que se refere às transferências de dados pessoais para países terceiros. Além disso, embora os dados dos passageiros estejam encriptados, são desencriptados quando estão a ser utilizados (nomeadamente quando a operação de correspondência é realizada), sendo as chaves controladas pela companhia aérea ou pelo seu subcontratante que presta os serviços de computação em nuvem. Esse armazenamento pode conduzir a um novo aumento da superfície de exposição em termos de segurança.

86. Por conseguinte, no que diz respeito à compatibilidade com o artigo 5.º, n.º 1, alínea f), e o artigo 32.º do RGPD, as medidas previstas no cenário 3.2[109], tendo em conta as técnicas mais avançadas, são insuficientes para garantir um nível de segurança adequado ao risco. Nesta base, o tratamento no âmbito do cenário 3.2 não cumpriria o disposto no artigo 5.º, n.º 1, alínea f), e no artigo 32.º do RGPD se um responsável pelo tratamento se limitasse às medidas nele descritas.

87. Além disso, de acordo com o cenário 3.2[110], os dados poderiam ser armazenados durante um prazo significativo (que poderia eventualmente vigorar enquanto o cliente fosse titular de uma conta junto da companhia aérea). Essa duração da conservação expõe os dados a riscos mais elevados de violação da sua confidencialidade e integridade e parece ir além do estritamente necessário e proporcionado para as finalidades do tratamento. O Comité observa que o prazo de conservação dos dados não é um fator decisivo, em si mesmo, para a compatibilidade global da referida arquitetura com o RGPD, uma vez que pode estar sujeito a alterações por parte dos responsáveis pelo tratamento de dados. No entanto, com base nas informações de que o Comité dispõe e que constam da descrição do cenário 3.2, não existe uma justificação suficiente para este longo prazo de conservação nem estão previstas medidas evidentes para atenuar os riscos para as pessoas singulares. Com base no que precede, o prazo de conservação proposto não se limitaria ao necessário, em conformidade com o princípio da limitação da conservação previsto no artigo 5.º, n.º 1, alínea e), do RGPD.

88. Em todo o caso, as medidas propostas no cenário 3.2 não podem cumprir os requisitos em matéria de proteção de dados desde a conceção e por defeito previstos no artigo 25.º do RGPD. No cenário 3.2, os modelos biométricos inscritos dos passageiros são armazenados na nuvem, sob o controlo da companhia aérea ou do seu prestador de serviços de computação em nuvem (subcontratante). Tal como acima descrito, várias entidades poderiam ter acesso a esses dados. Além disso, os dados biométricos dos passageiros são utilizados para a identificação dos passageiros (comparação 1:N), podendo N atingir o número total de utilizadores/clientes da companhia aérea. Este método implica procurar uma pessoa num grupo de pessoas singulares na base de dados central, tratando cada rosto

[107] N.os 68 a 77 *supra*.
[108] CEPD, *2022 Coordinated Enforcement Action – Use of cloud-based services by the public sector* (Ação coordenada de supervisão de 2022 – Utilização de serviços de computação em nuvem pelo setor público), 17 de janeiro de 2023, p. 19.
[109] Ver n.os 79 a 83 *supra*.
[110] Ver n.º 83 *supra*.

captado para verificar se corresponde a uma pessoa conhecida do sistema. Ao contrário do que sucede no cenário 3.1, no cenário 3.2 a comparação poderia ser efetuada numa escala muito maior, uma vez que, neste caso, o critério é o número total de clientes da companhia aérea, enquanto o cenário 3.1 incluía apenas o número de passageiros previsto num período de vários dias.

89. Além disso, no que diz respeito à compatibilidade com o artigo 25.º do RGPD e tendo em vista, em especial, o cumprimento do requisito de minimização dos dados, o tratamento previsto no cenário 3.2 não pode respeitar o princípio da necessidade. O Comité considera que seria possível alcançar um resultado semelhante em termos de racionalização do fluxo de passageiros nos aeroportos através de outras medidas menos intrusivas, por exemplo, sem a utilização de dados biométricos, embora, nesse caso, a experiência do utilizador fosse diferente, uma vez que poderia demorar mais tempo a mostrar o seu documento de identificação e o seu cartão de embarque. Além disso, outras soluções, nomeadamente as que se baseiam no armazenamento dos dados biométricos numa carteira local no dispositivo da pessoa singular ou as que exigem a encriptação dos dados com uma chave específica armazenada nesse dispositivo, permitem ao responsável pelo tratamento alcançar os objetivos de uma forma menos intrusiva para a privacidade.

90. No que diz respeito ao princípio da proporcionalidade, o tratamento previsto no cenário 3.2 criaria riscos para os direitos dos titulares dos dados, que não seriam atenuados pelas garantias previstas. O impacto negativo nos direitos e liberdades fundamentais dos titulares dos dados que resultaria de uma violação de dados numa base de dados centralizada de dados biométricos de um grande número de pessoas singulares parece ser superior ao benefício esperado resultante do tratamento, uma vez que esse benefício, ou seja, um ligeiro aumento da conveniência e da rapidez dos controlos, é relativamente reduzido. Por conseguinte, não pode justificar o elevado nível de ingerência dessas medidas nos direitos e liberdades fundamentais das pessoas singulares, e o tratamento previsto no cenário 3.2 não pode ser considerado proporcionado.

91. À luz destas considerações, em resposta à pergunta 2.3.1, o Comité conclui que, quando o tratamento é efetuado com a finalidade específica de racionalizar o fluxo de passageiros nos aeroportos, o tratamento previsto no cenário 3.2:

- **não pode ser compatível com o artigo 25.º do RGPD**;
- **não cumpriria o disposto no artigo 5.º, n.º 1, alínea f), e no artigo 32.º do RGPD** se um responsável pelo tratamento se limitasse às medidas descritas no cenário 3.2;
- **não cumpriria o disposto no artigo 5.º, n.º 1, alínea e), do RGPD**, uma vez que, com base nas informações de que o Comité dispõe, não existe uma justificação suficiente para o prazo de conservação previsto no cenário 3.2. A fim de respeitar o princípio da limitação da conservação previsto no artigo 5.º, n.º 1, alínea e), do RGPD, o responsável pelo tratamento teria de demonstrar que os dados pessoais são conservados apenas durante o período necessário para as finalidades para as quais são tratados.

4 CONCLUSÕES

92. No que diz respeito à pergunta 1.1, com base no pedido de parecer da AC FR, em relação aos requisitos do artigo 5.º, n.º 1, alínea f), e dos artigo 25.º e 32.º do RGPD, e com base na análise acima exposta, o Comité conclui o seguinte:

93. a utilização da tecnologia de reconhecimento facial para autenticação com base na biometria com a finalidade específica de racionalizar o fluxo de passageiros nos aeroportos (pontos de controlo de segurança, locais de entrega de bagagem, embarque e acesso às salas de espera) pode ser considerada, em princípio, compatível com os princípios da integridade e da confidencialidade previstos no artigo 5.º, n.º 1, alínea f), e nos artigos 25.º e 32.º do RGPD, no caso de uma arquitetura de armazenamento em que o modelo biométrico inscrito de cada passageiro é armazenado localmente no seu dispositivo individual e sob o seu controlo exclusivo, sob reserva das garantias adequadas, tal como descrito no n.º 46 *supra*.

94. No que diz respeito à pergunta 2.1.1, com base no pedido de parecer da AC FR, em relação aos requisitos do artigo 5.º, n.º 1, alíneas e) e f), e dos artigos 25.º e 32.º do RGPD, e com base na análise acima exposta, o Comité conclui o seguinte:

95. a utilização da tecnologia de reconhecimento facial para autenticação com base na biometria com a finalidade específica de racionalizar o fluxo de passageiros nos aeroportos (pontos de controlo de segurança, locais de entrega de bagagem, embarque e acesso às salas de espera) pode ser considerada, em princípio, compatível com o princípio da limitação da conservação previsto no artigo 5.º, n.º 1, alínea e), e com os princípios da integridade e da confidencialidade previstos no artigo 5.º, n.º 1, alínea f), e nos artigos 25.º e 32.º do RGPD, no caso de uma arquitetura de armazenamento centralizado em que o modelo biométrico inscrito de cada passageiro é armazenado numa base de dados central no aeroporto, sob o controlo do operador aeroportuário, em forma encriptada, com uma chave ou segredo exclusivamente na posse da pessoa singular, sob reserva das garantias adequadas, tal como descrito no n.º 60 *supra*.

96. No que diz respeito à pergunta 2.2.1, com base no pedido de parecer da AC FR, em relação aos requisitos do artigo 5.º, n.º 1, alíneas e) e f), e dos artigos 25.º e 32.º do RGPD, e com base na análise acima exposta, o Comité conclui o seguinte:

97. a utilização da tecnologia de reconhecimento facial para identificação com base na biometria com a finalidade específica de racionalizar o fluxo de passageiros nos aeroportos (pontos de controlo de segurança, locais de entrega de bagagem, embarque e acesso às salas de espera), no caso de uma arquitetura de armazenamento centralizado em que os modelos biométricos inscritos dos passageiros não são encriptados com uma chave ou segredo exclusivamente na posse de cada passageiro e em que esses modelos são armazenados numa base de dados no aeroporto (sob o controlo do operador aeroportuário), não pode ser compatível com o artigo 25.º do RGPD. Além disso, esse tratamento não respeitaria o princípio da integridade e da confidencialidade nos termos do artigo 5.º, n.º 1, alínea f), e do artigo 32.º do RGPD se um responsável pelo tratamento se limitasse às medidas descritas no cenário 3.1.

98. No que diz respeito à pergunta 2.3.1, com base no pedido de parecer da AC FR, em relação aos requisitos do artigo 5.º, n.º 1, alíneas e) e f), e dos artigos 25.º e 32.º do RGPD, e com base na análise acima exposta, o Comité conclui o seguinte:

99. a utilização da tecnologia de reconhecimento facial para identificação com base na biometria com a finalidade específica de racionalizar o fluxo de passageiros nos aeroportos (pontos de controlo de segurança, locais de entrega de bagagem, embarque e acesso às salas de espera), no caso de uma arquitetura de armazenamento centralizado em que os modelos biométricos inscritos dos passageiros não são encriptados com uma chave ou segredo exclusivamente na posse de cada passageiro e em que esses modelos são armazenados na nuvem (sob o controlo da companhia aérea), não pode ser compatível com o artigo 25.º do RGPD. Além disso, esse tratamento não respeitaria os princípios da

integridade e da confidencialidade nos termos do artigo 5.º, n.º 1, alínea f), e do artigo 32.º do RGPD se um responsável pelo tratamento se limitasse às medidas descritas no cenário 3.2. Por último, com base na descrição do cenário 3.2 e nas informações de que o Comité dispõe, o tratamento não respeitaria o princípio da limitação da conservação previsto no artigo 5.º, n.º 1, alínea e), do RGPD.

Pelo Comité Europeu para a Proteção de Dados

A Presidente

(Anu Talus)