Conselho da
União Europeia

Bruxelas, 14 de dezembro de 2017
(OR. en)

15119/17

Dossiê interinstitucional:
2017/0351 (COD)

COSI 336	**VISA 458**
FRONT 507	**FAUXDOC 73**
ASIM 142	**COPEN 419**
DAPIX 430	**JAI 1212**
ENFOPOL 622	**CT 164**
ENFOCUSTOM 285	**CSCI 79**
SIRIS 217	**SAP 28**
SCHENGEN 88	**COMIX 840**
DATAPROTECT 220	

NOTA DE ENVIO

de:	Secretário-Geral da Comissão Europeia, assinado por Jordi AYET PUIGARNAU, Diretor
data de receção:	12 de dezembro de 2017
para:	Jeppe TRANHOLM-MIKKELSEN, Secretário-Geral do Conselho da União Europeia
n.° doc. Com.:	COM(2017) 793 final
Assunto:	Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo à criação de um quadro para a interoperabilidade entre os sistemas de informação da UE (fronteiras e vistos) e que altera a Decisão 2004/512/CE do Conselho, o Regulamento (CE) n.º 767/2008, a Decisão 2008/633/JAI do Conselho, o Regulamento (UE) 2016/399 e o Regulamento (UE) 2017/2226

Envia-se em anexo, à atenção das delegações, o documento COM(2017) 793 final.

Anexo: COM(2017) 793 final

COMISSÃO
EUROPEIA

Estrasburgo, 12.12.2017
COM(2017) 793 final

2017/0351 (COD)

Proposta de

REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO

relativo à criação de um quadro para a interoperabilidade entre os sistemas de informação da UE (fronteiras e vistos) e que altera a Decisão 2004/512/CE do Conselho, o Regulamento (CE) n.º 767/2008, a Decisão 2008/633/JAI do Conselho, o Regulamento (UE) 2016/399 e o Regulamento (UE) 2017/2226

{SWD(2017) 473 final} - {SWD(2017) 474 final}

EXPOSIÇÃO DE MOTIVOS

1. CONTEXTO DA PROPOSTA

• Contexto da proposta

Nos últimos três anos, a UE registou um aumento da passagem irregular das suas fronteiras e uma ameaça crescente e permanente à segurança interna, conforme demonstrado pela série de ataques terroristas de que foi alvo. Os cidadãos da UE esperam que os controlos de pessoas nas fronteiras externas e os controlos no espaço Schengen sejam eficazes, a fim de permitirem uma gestão eficaz da migração e de contribuírem para a segurança interna. Estes desafios chamaram ainda mais a atenção para a necessidade urgente de unir e reforçar, de forma abrangente, os instrumentos de informação da UE no que toca a gestão de fronteiras, migração e segurança.

A gestão da informação da UE pode e deve ser mais eficaz e eficiente, no pleno respeito pelos direitos fundamentais, nomeadamente, o direito à proteção dos dados pessoais, a fim de melhor proteger as fronteiras externas da UE, melhorar a gestão da migração e reforçar a segurança interna, em benefício de todos os cidadãos. Existem já alguns sistemas de informação a nível da UE, e estão a ser desenvolvidos mais sistemas, para fornecer aos guardas de fronteira, funcionários dos serviços de imigração e membros da polícia, informações relevantes sobre as pessoas. Para que esse apoio seja eficaz, as informações fornecidas pelos sistemas de informação da UE têm de ser completas, exatas e fiáveis. No entanto, existem lacunas estruturais na arquitetura de gestão da informação da UE. As autoridades nacionais enfrentam uma paisagem complexa de sistemas de informação regidos de formas diferentes. Além disso, a arquitetura de gestão de dados aplicada aos controlos nas fronteiras e à segurança está fragmentada, na medida em que as informações são armazenadas separadamente em sistemas sem ligação entre si. Esta situação dá origem a ângulos mortos. Consequentemente, **os vários sistemas de informação a nível da UE não são atualmente interoperáveis**, ou seja, não é possível fazer intercâmbio de dados nem partilhar informações a fim de que as autoridades e funcionários competentes disponham das informações de que necessitam, onde e quando delas necessitam. A interoperabilidade dos sistemas de informação a nível da UE pode contribuir significativamente para eliminar os atuais ângulos mortos, que permitem que pessoas, incluindo suspeitos de terrorismo, estejam registadas com nomes diferentes em diversas bases de dados sem ligação entre elas.

Em abril de 2016, a Comissão apresentou uma **Comunicação sobre *Sistemas de informação mais sólidos e mais inteligentes para controlar as fronteiras e garantir a segurança***[1] que aborda uma série de lacunas estruturais relacionadas com os sistemas de informação[2]. A Comunicação de abril de 2016 teve como objetivo dar início a um debate sobre o modo como os sistemas de informação da União Europeia podem reforçar a gestão das fronteiras e da migração, bem como a segurança interna. Por seu lado, o **Conselho** também reconheceu a necessidade urgente de se atuar neste domínio. Em junho de 2016, aprovou um **roteiro para intensificar o intercâmbio e a gestão de informações**, incluindo soluções de

[1] COM(2016) 205 de 6 de abril de 2016.

[2] 1) Funcionalidades insuficientes nalguns dos sistemas de informação existentes; 2) lacunas de informação na arquitetura de gestão de dados da UE; 3) uma paisagem complexa de sistemas de informação regidos de formas diferentes; e 4) uma arquitetura de gestão de dados fragmentada aplicada aos controlos nas fronteiras e à segurança, na qual as informações são armazenadas separadamente em sistemas sem ligação entre si, o que dá origem a ângulos mortos.

interoperabilidade no domínio da Justiça e Assuntos Internos[3]. O roteiro teve como objetivo dar apoio operacional às investigações e fornecer rapidamente aos profissionais no terreno, tais como agentes da polícia, guardas de fronteira, procuradores públicos, funcionários dos serviços de imigração e outros, informações de elevada qualidade, abrangentes e atuais, tendo em vista uma cooperação e atuação eficazes. O **Parlamento Europeu** instou também a ações neste domínio. Na sua resolução de julho de 2016[4] sobre o programa de trabalho da Comissão para 2017, o Parlamento Europeu apelou a *«propostas com vista a melhorar e desenvolver os sistemas de informação existentes, colmatar lacunas de informação e a avançar rumo à interoperabilidade, bem como propostas de partilha obrigatória de informações a nível da UE, acompanhado das necessárias salvaguardas em matéria de proteção de dados»*. O discurso do Presidente Juncker sobre o estado da União proferido em setembro de 2016[5] e as conclusões do Conselho Europeu de dezembro de 2016[6] insistiram na importância de colmatar as atuais lacunas em matéria de gestão de dados e de melhorar a interoperabilidade dos sistemas de informação existentes.

Em junho de 2016, no seguimento da Comunicação de abril de 2016, a Comissão criou um **grupo de peritos de alto nível em matéria de sistemas de informação e interoperabilidade**[7] para dar resposta aos desafios jurídicos, técnicos e operacionais de melhorar a interoperabilidade entre os sistemas centrais da UE para controlar fronteiras e garantir a segurança, incluindo a sua necessidade, viabilidade técnica, proporcionalidade e implicações a nível da proteção de dados. O **relatório final** do grupo de peritos de alto nível foi publicado em maio de 2017[8]. Delineou uma série de recomendações destinadas a reforçar e a desenvolver os sistemas de informação da UE e a sua interoperabilidade. A Agência dos Direitos Fundamentais da UE, a Autoridade Europeia para a Proteção de Dados e o Coordenador da UE da Luta Antiterrorista participaram ativamente nos trabalhos do grupo de peritos. Cada entidade apresentou declarações de apoio, ao mesmo tempo que reconheceu a necessidade de, no seguimento deste tema, se dedicar uma especial atenção às questões mais amplas relacionadas com os direitos fundamentais e de proteção de dados. Estiveram presentes enquanto observadores representantes do Secretariado da Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos do Parlamento Europeu e do Secretariado-Geral do Conselho. O grupo de peritos de alto nível concluiu que é **necessário e tecnicamente viável trabalhar rumo a soluções práticas de interoperabilidade** e que estas podem, em princípio, gerar ganhos operacionais e ser estabelecidas em conformidade com as exigências em matéria de proteção de dados.

Com base no relatório e nas recomendações do grupo de peritos, a Comissão apresentou, no *Sétimo relatório sobre os progressos alcançados rumo à criação de uma União da Segurança genuína e eficaz,*[9] uma **nova abordagem para a gestão dos dados** para controlar as fronteiras, garantir a segurança e gerir a migração, segundo a qual todos os sistemas de informação centralizados a nível da UE que asseguram a gestão da segurança, das fronteiras e da migração serão interoperáveis, no pleno respeito dos direitos fundamentais. A Comissão

---

3 Roteiro de 6 de junho de 2016 para intensificar o intercâmbio e a gestão de informações, incluindo soluções de interoperabilidade no domínio da Justiça e Assuntos Internos – 9368/1/16 REV 1.

4 Resolução do Parlamento Europeu, de 6 de julho de 2016, sobre as prioridades estratégicas para o Programa de Trabalho da Comissão para 2017 (2016/2773(RSP).

5 Estado da União de 2016 (14.9.2016), https://ec.europa.eu/commission/state-union-2016_en.

6 Conclusões do Conselho Europeu (15.12.2016), http://www.consilium.europa.eu/en/meetings/european-council/2016/12/20161215-euco-conclusions-final_pdf/.

7 Decisão da Comissão de 17 de junho de 2016 que institui o Grupo de Peritos de Alto Nível em matéria de sistemas de informação e interoperabilidade – 2016/C 257/03.

8 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

9 COM(2017) 261 final.

anunciou a sua intenção de prosseguir os trabalhos no sentido de criar um portal europeu de pesquisa que permita a consulta simultânea de todos os sistemas da UE relevantes nos domínios da gestão da segurança, das fronteiras e da migração, eventualmente, com regras mais simplificadas para o acesso das autoridades policiais, e de desenvolver para estes sistemas um serviço partilhado de correspondências biométricas (possivelmente com uma funcionalidade de indicadores de respostas positivas[10]) e um repositório comum de dados de identificação. Anunciou a sua intenção de apresentar, o mais rapidamente possível, uma proposta legislativa em matéria de interoperabilidade.

As conclusões do Conselho Europeu de junho de 2017[11] reiteraram a necessidade de agir. Com base nas conclusões de junho de 2017[12] do Conselho (Justiça e Assuntos Internos), o Conselho Europeu convidou a Comissão a preparar, o mais rapidamente possível, projetos de legislação para adotar as recomendações formuladas pelo grupo de peritos de alto nível. Esta iniciativa responde também ao apelo do Conselho no sentido de um quadro global para o acesso das autoridades policiais às diferentes bases de dados no domínio da justiça e dos assuntos internos, com vista a assegurar uma maior simplificação, coerência, eficácia e atenção às necessidades operacionais[13]. A fim de reforçar os esforços no sentido de tornar a União Europeia uma sociedade mais segura, no pleno respeito dos direitos fundamentais, a Comissão anunciou, no contexto do seu Programa de Trabalho para 2018[14], uma proposta relativa à interoperabilidade dos sistemas de informação a apresentar até ao final de 2017.

- **Objetivos da proposta**

Os objetivos gerais desta iniciativa têm origem nos objetivos consagrados no Tratado, nomeadamente, melhorar a gestão das fronteiras externas do espaço Schengen e contribuir para a segurança interna da União Europeia. Decorrem ainda de decisões políticas da Comissão e de Conclusões pertinentes do Conselho (Europeu). Estes objetivos são desenvolvidos de forma mais aprofundada na Agenda Europeia da Migração e nas comunicações subsequentes, incluindo na Comunicação sobre a preservação e o reforço de Schengen[15], na Agenda Europeia para a Segurança[16] e nos relatórios da Comissão sobre o trabalho e os progressos alcançados rumo a uma União da Segurança genuína e eficaz[17].

Embora os objetivos da presente proposta tenham por base, em especial, a Comunicação de abril de 2016 e as conclusões do grupo de peritos de alto nível, eles estão intrinsecamente ligados ao acima exposto.

Os objetivos específicos da presente proposta consistem em:

---

[10] Novo princípio da «privacidade desde a conceção» que restringe o acesso a todos os dados, limitando-o a uma simples notificação de «resposta positiva/negativa», indicando a presença (ou ausência) de dados.

[11] Conclusões do Conselho Europeu, 22-23 de junho de 2017.

[12] Resultados da 3546.ª reunião do Conselho sobre Justiça e Assuntos Internos, 8 e 9 de junho de 2017, 10136/17.

[13] Após ter dado mandato à Presidência do Conselho para dar início a negociações interinstitucionais sobre o Sistema de Entrada/Saída da UE em 2 de março de 2017, o Comité de Representantes Permanentes do Conselho (Coreper), acordou um projeto de declaração do Conselho convidando a Comissão a propor um quadro global para o acesso das autoridades policiais às diferentes bases de dados no domínio da justiça e dos assuntos internos, com vista a assegurar uma maior simplificação, coerência, eficácia e atenção às necessidades operacionais (ata sumária 7177/17, 21.3.2017).

[14] COM(2017) 650 final.

[15] COM(2017)570 final.

[16] COM(2015)185 final.

[17] COM(2016)230 final.

(1) Assegurar que os utilizadores finais, nomeadamente os guardas de fronteira, agentes com funções coercivas, agentes dos serviços de imigração e autoridades judiciais têm **acesso rápido, contínuo, sistemático e controlado** às informações de que necessitam para desempenhar as suas funções;

(2) Encontrar uma solução para **detetar identidades múltiplas** ligadas ao mesmo conjunto de dados biométricos, com o duplo objetivo de garantir a identificação correta das pessoas de boa-fé e **combater a fraude de identidade**;

(3) Facilitar os **controlos de identidade de nacionais de países terceiros**, no território de um Estado-Membro, por parte das autoridades policiais; e

(4) Facilitar e **agilizar o acesso das autoridades de aplicação da lei** aos sistemas de informação com finalidades não coercivas a nível da UE, sempre que tal for necessário para efeitos de prevenção, investigação, deteção ou repressão de formas graves de criminalidade e terrorismo.

Para além destes objetivos operacionais principais, a presente proposta contribuirá igualmente para:

- facilitar a **aplicação, por parte dos Estados-Membros,** dos aspetos técnicos e operacionais dos sistemas de informação atuais e futuros;
- reforçar e simplificar as **condições de segurança e de proteção dos dados** que regem os respetivos sistemas; e
- melhorar e harmonizar os requisitos de **qualidade dos dados** dos respetivos sistemas.

Por último, a presente proposta inclui disposições para a criação e gestão do formato de mensagem universal (UMF) como uma norma da UE para o desenvolvimento dos sistemas de informação no domínio da justiça e dos assuntos internos, e a criação de um repositório central para a elaboração de relatórios e estatísticas.

- **Âmbito de aplicação da proposta**

Juntamente com a sua proposta conexa apresentada no mesmo dia, a presente proposta sobre interoperabilidade foca os sistemas de informação da UE no domínio da gestão da segurança, das fronteiras e da migração, que são geridos a nível central. Três destes sistemas já existem, um encontra-se em desenvolvimento, e os outros dois estão na fase das propostas em debate entre os colegisladores. Cada sistema possui os seus próprios objetivos, finalidades, bases jurídicas, regras, grupos de utilizadores e contexto institucional.

Os três sistemas de informação centralizados existentes até à data são os seguintes:

- o **Sistema de Informação Schengen (SIS)** com um amplo espetro de indicações sobre pessoas (recusas de entrada ou permanência, mandado de detenção da UE, pessoas desaparecidas, assistência nos processos judiciais, vigilância discreta ou

controlo específico) e objetos (incluindo documentos de identidade ou de viagem extraviados, roubados e invalidados)[18];

- o sistema **Eurodac**, com os dados de impressões digitais dos requerentes de asilo e nacionais de países terceiros que atravessaram as fronteiras externas de forma irregular ou que se encontram em situação irregular num Estado-Membro; e

- o **Sistema de Informação sobre Vistos (VIS)**, com dados relativos aos vistos de curta duração.

Para além dos sistemas já existentes, a Comissão propôs, em 2016-2017, três novos sistemas de informação centralizados da UE:

- o **Sistema de Entrada/Saída (SES)**, cuja base jurídica foi recentemente acordada, que substituirá o atual sistema de carimbar manualmente os passaportes e registará por via eletrónica o nome, o tipo de documento de viagem, os dados biométricos e a data e o local de entrada e de saída dos nacionais de países terceiros que visitam o espaço Schengen para uma estada de curta duração;

- o **Sistema Europeu de Informação e Autorização de Viagem (ETIAS)** proposto, que, uma vez adotado, seria um sistema amplamente automatizado que recolheria e verificaria a informação apresentada pelos nacionais de países terceiros isentos da obrigação de visto antes de estes viajarem para o espaço Schengen; e

- o **Sistema Europeu de Informação sobre os Registos Criminais de nacionais de países terceiros (sistema ECRIS-TCN)** proposto, que seria um sistema eletrónico de intercâmbio de informações sobre condenações anteriores proferidas contra nacionais de países terceiros por tribunais penais na UE.

Estes seis sistemas são complementares e, com a exceção do Sistema de Informação Schengen (SIS), exclusivamente focados em nacionais de países terceiros. Os sistemas apoiam as autoridades nacionais na gestão de fronteiras, migração, processamentos de vistos e asilo, e na luta contra a criminalidade e o terrorismo. O último objetivo aplica-se, em especial, ao SIS, que é o instrumento de partilha de informações policiais mais amplamente utilizado hoje em dia.

Para além destes sistemas de informação, geridos de forma centralizada a nível da UE, o âmbito de aplicação da presente proposta inclui também a base de dados da **Interpol** relativa a documentos de viagem roubados e extraviados (SLTD), que, em conformidade com as disposições do Código das Fronteiras Schengen é sistematicamente consultada nas fronteiras externas da UE, e a base de dados da Interpol relativa a documentos de viagem associados a notificações (TDAWN). Abrange igualmente os dados da **Europol**, na medida em que tal seja relevante para o funcionamento do sistema ETIAS proposto, e para ajudar os Estados-Membros durante a consulta de dados sobre formas graves de criminalidade e terrorismo.

Os sistemas de informação nacionais e os sistemas de informação da UE descentralizados estão fora do âmbito de aplicação da presente iniciativa. Desde que se justifique a sua necessidade, os sistemas descentralizados, como é o caso dos que são operados nos termos do quadro do Prüm,[19] da Diretiva relativa ao Registo de Identificação dos Passageiros (PNR)[20] e

[18] A proposta de regulamento, de dezembro de 2016, da Comissão sobre o SIS propõe o alargamento da mesma a fim de incluir as decisões em matéria de regresso e controlos de verificação.

[19] http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1508936184412&uri=CELEX:32008D06 15.

da Diretiva relativa a Informações Prévias sobre Passageiros[21], podem, numa fase posterior, ser ligados a um ou mais dos componentes propostos na presente iniciativa[22].

Para respeitar a distinção entre questões que constituem uma evolução do acervo de Schengen no que diz respeito a fronteiras e vistos, por um lado, e outros sistemas que dizem respeito ao acervo de Schengen em matéria de cooperação policial ou que não estão relacionados com o acervo de Schengen, por outro, a presente proposta trata do acesso ao Sistema de Informação sobre Vistos, ao Sistema de Informação Schengen, conforme presentemente regulado pelo Regulamento (CE) n.º 1987/2006, ao Sistema de Entrada-Saída e ao Sistema Europeu de Informação e Autorização de Viagem.

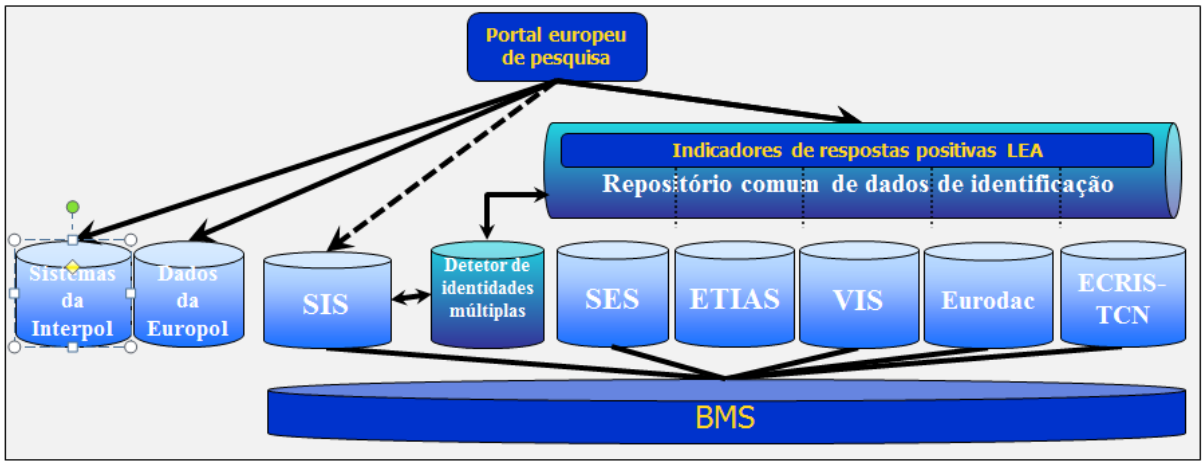
- **Componentes técnicos necessários para alcançar a interoperabilidade**

A fim de alcançar os objetivos da presente proposta, é necessário criar quatro componentes de interoperabilidade:

- O portal europeu de pesquisa – ESP
- Um serviço partilhado de correspondências biométricas – BMS
- Um repositório comum de dados de identificação – CIR
- Um detetor de identidades múltiplas – MID

Cada um destes componentes é descrito em pormenor no documento de trabalho dos serviços da Comissão sobre a avaliação de impacto que acompanha a presente proposta.

Os quatro componentes combinados levam à seguinte solução de interoperabilidade:



[20] http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1508936384641&uri=CELEX:32016L06 81.

[21] Diretiva 2004/82/CE do Conselho, de 29 de abril de 2004, relativa à obrigação de comunicação de dados dos passageiros pelas transportadoras.

[22] Do mesmo modo, no que respeita aos sistemas aduaneiros, nas suas conclusões de junho de 2017, o Conselho convidou a Comissão a realizar um estudo de viabilidade para explorar mais aprofundadamente os aspetos técnicos, operacionais e jurídicos da interoperabilidade dos sistemas de gestão de segurança e de fronteiras com os sistemas aduaneiros, e a apresentar as suas conclusões para debate no Conselho até ao final de 2018.

Os objetivos e o funcionamento destes quatro componentes podem resumir-se do seguinte modo:

1) O **portal europeu de pesquisa (ESP)** é o componente que permitiria consultar vários sistemas em simultâneo (SIS Central, Eurodac, VIS, o futuro SES e os sistemas ETIAS e ECRIS-TCN propostos, bem como os sistemas da Interpol e os dados da Europol pertinentes), utilizando dados de identificação (biográficos e biométricos). Este portal asseguraria aos utilizadores dos sistemas de informação da UE um acesso rápido, contínuo, eficiente, sistemático e controlado a todas as informações de que necessitam para desempenhar as suas funções.

   Uma consulta feita através do portal europeu de pesquisa permitiria obter, numa questão de segundos, informações provenientes dos diferentes sistemas aos quais o utilizador tem acesso legítimo. Consoante o objetivo da consulta, e os direitos de acesso correspondentes, o ESP teria configurações específicas.

   O ESP não processa dados novos e não armazena dados; funcionaria como um «balcão único» ou «intermediário de mensagens» para consultar os vários sistemas centrais e extrair as informações necessárias de forma integrada, respeitando integralmente as exigências em matéria de controlo de acessos e de proteção de dados dos sistemas subjacentes. O ESP facilitaria a utilização correta e autorizada de cada um dos atuais sistemas de informação da UE, e tornaria mais fácil e menos oneroso para os Estados-Membros consultar e utilizar os sistemas, em conformidade com os instrumentos jurídicos que regem estes sistemas.

2) O **serviço partilhado de correspondências biométricas (BMS)** permitiria consultar e comparar os dados biométricos (impressões digitais e imagens faciais) existentes nos vários sistemas centrais (em especial, o SIS, o Eurodac, o VIS, o futuro SES e o sistema ECRIS-TCN proposto). O ETIAS proposto não irá conter dados biométricos e, como tal, não seria ligado ao BMS.

   Enquanto cada um dos atuais sistemas centrais (SIS, Eurodac, VIS) dispõe atualmente de um motor de busca próprio dedicado para dados biométricos[23], um serviço partilhado de correspondências biométricas forneceria uma plataforma comum onde os dados seriam consultados e comparados em simultâneo. O BMS traria benefícios substanciais em termos de segurança, custos, manutenção e funcionamento, na medida em que se apoiaria num único componente tecnológico em vez de em cinco componentes diferentes. Os dados biométricos (impressões digitais e imagens faciais) estão conservados em exclusivo nos sistemas subjacentes. O BMS criaria e teria uma representação matemática das amostras biométricas (um modelo), mas eliminaria os dados reais, que desta forma permanecem armazenados num local, uma única vez.

   O BMS seria um fator essencial para ajudar a detetar ligações entre conjuntos de dados e identidades diferentes assumidas pela mesma pessoa em sistemas centrais diferentes. Sem um BMS, nenhum dos outros três componentes funcionará.

[23] Estes motores de busca biométrica são referidos tecnicamente como Sistema Automático de Identificação Dactiloscópica (AFIS) ou Sistema Automático de Identificação Biométrica (ABIS).

3) O **repositório comum de dados de identificação (CIR)** seria o componente partilhado para armazenar dados de identificação biográficos[24] e biométricos de nacionais de países terceiros registados no Eurodac, no VIS, no futuro SES e nos sistemas ETIAS ECRIS-TCN propostos Cada um destes cinco sistemas centrais regista ou registará dados biográficos sobre determinadas pessoas por motivos específicos. Isto não seria alterado. Os dados de identificação pertinentes seriam armazenados no CIR, mas continuariam a «pertencer» aos respetivos sistemas subjacentes que os registaram.

O CIR não iria conter dados do SIS. A complexa arquitetura técnica do SIS contendo cópias nacionais, cópias nacionais parciais e eventuais sistemas de correspondências biométricas nacionais tornaria o CIR muito complexo ao ponto de deixar de ser técnica e financeiramente viável.

O principal objetivo do CIR é facilitar a identificação biográfica de um nacional de um país terceiro. Esta opção proporcionaria uma maior rapidez das operações, uma maior eficiência e economias de escala. A criação do CIR é necessária para permitir um controlo eficaz da identidade de nacionais de países terceiros, incluindo no território de um Estado-Membro. Além disso, adicionando uma «funcionalidade de indicadores de respostas positivas» ao CIR, seria possível verificar a presença (ou ausência) de dados em qualquer dos sistemas abrangidos pelo CIR através de uma simples notificação de resposta positiva/negativa. Desta forma, o CIR contribuiria também para agilizar o acesso das autoridades de aplicação da lei a sistemas de informação com finalidades não coercivas, mantendo simultaneamente uma importante garantia de proteção de dados (ver a secção sobre a abordagem em duas fases para acesso das autoridades de aplicação da lei, infra).

Dos cinco sistemas que o CIR deverá abranger, o futuro SES e os sistemas ETIAS e ECRIS-TCN propostos são sistemas novos que têm ainda de ser desenvolvidos. O atual sistema Eurodac não dispõe de dados biográficos; este alargamento será desenvolvido depois da adoção da nova base jurídica do Eurodac. O VIS atual contém dados biográficos, mas as interações necessárias entre o VIS e o futuro SES exigirão uma atualização do VIS existente, pelo que a criação do CIR chegaria, assim, no momento certo. Não implicaria, de modo algum, a duplicação de dados existentes. Tecnicamente, o CIR seria desenvolvido com base na plataforma do SES/ETIAS.

4) O **detetor de identidades múltiplas – MID** verificaria se os dados de identificação pesquisados existem em mais do que um dos sistemas ligados ao detetor. O MID abrange os sistemas que armazenam dados de identificação no CIR (o Eurodac, o VIS, o futuro SES e os sistemas ETIAS e ECRIS-TCN propostos), bem como o SIS. O MID permitiria detetar identidades múltiplas ligadas ao mesmo conjunto de dados biométricos, com o duplo objetivo de garantir a identificação correta das pessoas de boa-fé e combater a fraude de identidade.

O MID permitiria determinar que nomes diferentes pertencem à mesma identidade. Trata-se de uma inovação necessária para lidar de forma eficaz com a utilização fraudulenta de identidades, que constitui uma grave violação da segurança. O MID mostraria apenas os registos de identidades biográficas que têm uma ligação em sistemas centrais diferentes. Estas ligações seriam detetadas utilizando o serviço partilhado de correspondências biométricas com base em dados biométricos, e teriam de ser confirmadas ou rejeitadas

[24] Os dados biográficos que constam no documento de viagem incluem: apelido, nome próprio, sexo, data de nascimento, número do documento de viagem. Não incluem moradas, nomes antigos, dados biométricos, etc.

pela autoridade que registou os dados no sistema de informação que levou à criação da ligação. Para ajudar os utilizadores autorizados do MID nesta tarefa, o sistema teria de rotular as ligações identificadas em quatro categorias:

- Ligação amarela – identidades biográficas potencialmente diferentes relativas à mesma pessoa
- Ligação branca – confirmação de que as diferentes identidades biográficas pertencem à mesma pessoa de boa-fé
- Ligação verde – confirmação de que diferentes pessoas de boa-fé partilham a mesma identidade biográfica
- Ligação vermelha – suspeita de que uma mesma pessoa está a utilizar identidades biográficas diferentes de forma ilícita.

A presente proposta descreve os procedimentos que seriam instituídos para lidar com estas diferentes categorias. A identidade das pessoas de boa-fé afetadas deve ser esclarecida o mais rapidamente possível, transformando a ligação amarela numa ligação verde ou branca confirmada, de modo a garantir que não serão confrontadas com situações desagradáveis desnecessárias. Se, por outro lado, a avaliação confirmar a existência de uma ligação vermelha, ou uma mudança de uma ligação amarela para uma vermelha, é necessário tomar as medidas adequadas.

- **Abordagem em duas fases ao acesso para fins de aplicação da lei, conforme previsto pelo repositório comum de dados de identificação**

A aplicação da lei é definida como um objetivo secundário ou acessório do Eurodac, do VIS, do futuro SES e do ETIAS proposto. Como tal, a possibilidade de aceder a dados armazenados nestes sistemas para efeitos de aplicação da lei é limitado. As autoridades de aplicação da lei só podem consultar diretamente esses sistemas de informação com finalidades não coercivas para efeitos de prevenção, investigação, deteção ou repressão do terrorismo e de outras infrações penais graves. Além disso, os respetivos sistemas são regidos por diferentes condições e garantias de acesso, e algumas dessas regras_poderão dificultar a rapidez_da utilização legítima dos sistemas por estas autoridades. De um modo mais geral, o princípio da pesquisa prévia restringe a possibilidade de as autoridades dos Estados-Membros consultarem os sistemas para efeitos de aplicação da lei justificados e pode, por conseguinte, resultar na perda de oportunidades para revelar informações necessárias.

Na sua Comunicação de abril de 2016, a Comissão reconheceu a necessidade de otimizar os instrumentos existentes para efeitos de aplicação da lei, respeitando, simultaneamente, os requisitos em matéria de proteção de dados. Esta necessidade foi confirmada e reiterada pelos Estados-Membros e pelas agências competentes no âmbito do grupo de peritos de alto nível.

Tendo em conta o que precede, ao criar o CIR com uma chamada «funcionalidade de indicadores de respostas positivas», a presente proposta introduz a possibilidade de aceder ao SES, ao VIS, ao ETIAS e ao Eurodac utilizando uma **abordagem em duas fases à consulta de dados**. Esta abordagem em duas fases não alteraria o facto de que a aplicação da lei constitui um objetivo estritamente acessório destes sistemas e deve, por conseguinte, obedecer a regras de acesso estritas.

O primeiro passo do funcionário responsável pela aplicação da lei seria iniciar uma consulta sobre uma pessoa específica utilizando os dados de identificação, o documento de viagem ou os dados biométricos dessa pessoa para verificar se as informações sobre a pessoa pesquisada estão armazenadas no CIR. Se esses dados existirem, o funcionário receberá **uma resposta indicando quais são os sistemas de informação da UE que contêm dados** sobre esta pessoa (o **indicador de resposta positiva**). O funcionário não teria acesso efetivo a quaisquer dados em qualquer um dos sistemas subjacentes.

O segundo passo do funcionário seria, eventualmente, solicitar o acesso individual a cada sistema identificado como contendo dados, para obter o processo completo sobre a pessoa pesquisada, **em conformidade com as regras e os procedimentos em vigor, estabelecidos por cada um dos sistemas em causa**. Neste segundo passo, o acesso permaneceria sujeito a autorização prévia de uma autoridade designada e continuaria a exigir uma ID de utilizador específica e o início de sessão.

Esta nova abordagem seria também mais vantajosa para as autoridades de aplicação da lei, devido à **existência de ligações potenciais** no MID. O MID ajudaria o CIR a identificar as ligações existentes, o que contribui para tornar a pesquisa ainda mais precisa. O MID seria capaz de indicar se a pessoa é **conhecida sob diferentes identidades** nos diferentes sistemas de informação.

A abordagem em duas fases à consulta de dados é particularmente útil nos casos em que **se desconhece** quem é o suspeito, o autor ou presumível vítima de uma infração terrorista ou outra infração penal grave. Com efeito, nesses casos, o CIR permitiria identificar o sistema de informação que conhece a pessoa, numa única pesquisa. Deste modo, as atuais condições de pesquisas prévias em bases de dados nacionais e de uma pesquisa prévia no sistema automático de identificação dactiloscópica de outros Estados-Membros ao abrigo da Decisão 2008/615/JAI («Controlo Prüm») tornam-se redundantes.

A nova abordagem em duas fases à consulta só **entraria em vigor quando** os **componentes de interoperabilidade necessários estivessem plenamente operacionais**.

- **Elementos adicionais da presente proposta para apoiar os componentes de interoperabilidade**

1) Para além dos componentes supramencionados, o presente projeto de regulamento inclui também a proposta para criar um **repositório central para a elaboração de relatórios e estatísticas (CRRS)**. Este repositório é necessário para permitir a criação e a partilha de relatórios com dados estatísticos (anónimos) para fins políticos, operacionais e de qualidade dos dados. A atual prática de recolher dados estatísticos apenas nos sistemas de informação individuais é prejudicial para a segurança dos dados e o seu desempenho, e não permite o cruzamento de dados entre os sistemas.

   O CRRS proporcionaria um repositório separado e dedicado para estatísticas anónimas extraídas do SIS, do VIS, do Eurodac, do futuro SES, dos sistemas ETIAS e ECRIS-TCN propostos, do repositório comum de dados de identificação, do detetor de identidades múltiplas e do serviço partilhado de correspondências biométricas. O repositório preveria a possibilidade de partilhar relatórios de forma segura (conforme regulado pelos respetivos instrumentos jurídicos) com os Estados-Membros, a Comissão (incluindo o Eurostat) e as agências da UE.

   O desenvolvimento de um repositório central em vez de repositórios separados para cada sistema teria um custo inferior e implicaria menos esforços para a sua criação,

funcionamento e manutenção. Contribuiria também para um nível mais alto de segurança de dados, na medida em que o armazenamento dos dados e o controlo dos acessos seriam geridos num único repositório.

2) O presente projeto de regulamento propõe igualmente criar o **formato de mensagem universal (UMF)** como a norma a utilizar a nível da UE para organizar interações entre múltiplos sistemas de forma interoperativa, incluindo os sistemas desenvolvidos e geridos pela eu-LISA. A utilização da norma pela Europol e pela Interpol também seria incentivada.

   A norma UMF introduz uma linguagem técnica comum e unificada para descrever e ligar elementos de dados, em particular os elementos respeitantes às pessoas e documentos (de viagem). A utilização do UMF durante o desenvolvimento de novos sistemas de informação garante uma integração e interoperabilidade mais fáceis com outros sistemas, em particular para os Estados-Membros que precisam de criar interfaces para comunicar com estes novos sistemas. A este respeito, a utilização obrigatória do UMF durante o desenvolvimento de novos sistemas pode ser considerada uma condição prévia necessária para a introdução dos componentes de interoperabilidade propostos no presente regulamento.

   A fim de assegurar a plena implantação em toda a UE da norma UMF, é proposta uma estrutura de governação adequada. A Comissão seria responsável por criar e desenvolver a norma UMF, no quadro de um processo de exame com os Estados-Membros. Os Estados associados a Schengen, as agências da UE e os organismos internacionais que participam nos projetos UMF (como a eu-LISA, Europol e Interpol) também irão estar envolvidos. A estrutura de governação proposta é essencial para o UMF a fim de prolongar e alargar a norma, garantindo simultaneamente uma máxima utilizabilidade e aplicabilidade.

3) O presente projeto de regulamento introduz também os conceitos de **mecanismos automatizados de controlo da qualidade de dados** e indicadores de qualidade comuns, e a necessidade de os Estados-Membros assegurarem dados da mais alta qualidade na alimentação e utilização dos sistemas. Se os dados não forem da mais alta qualidade, pode haver consequências, não só porque não se consegue identificar pessoas procuradas, mas também porque afeta os direitos fundamentais de pessoas inocentes. A fim de ultrapassar os problemas que podem decorrer da introdução de dados por operadores humanos, as regras de validação automática podem impedir os operadores de cometer erros. O objetivo seria identificar automaticamente dados aparentemente incorretos ou incoerentes, de modo que o Estado-Membro de origem pudesse verificar os dados e tomar as medidas necessárias para corrigir os erros. Isto seria complementado com relatórios regulares sobre a qualidade dos dados produzidos pela eu-LISA.

- **Consequências para outros instrumentos jurídicos**

Juntamente com a sua proposta conexa, este projeto de regulamento introduz inovações que irão exigir a introdução de alterações noutros instrumentos jurídicos:

- Regulamento (UE) n.º 2016/399 (Código das Fronteiras Schengen)
- Regulamento (UE) n.º 2017/2226 (Regulamento SES)
- Regulamento (CE) n.º 767/2008 (Regulamento VIS)

- Decisão 2004/512/CE do Conselho (Decisão VIS)
- Decisão 2008/633/JAI do Conselho (Decisão VIS/acesso para fins de aplicação da lei)
- [Regulamento ETIAS]
- [Regulamento Eurodac]
- [Regulamentos SIS]
- [Regulamento ECRIS-TCN, incluindo as disposições correspondentes do Regulamento (UE) n.º 2016/1624 (Regulamento Guarda Europeia de Fronteiras e Costeira)]
- [Regulamento eu-LISA]

A presente proposta e a proposta conexa contêm disposições específicas para as alterações necessárias aos instrumentos jurídicos que são atualmente textos estáveis, conforme aprovados pelos colegisladores: o Código das Fronteiras Schengen, o Regulamento SES, o Regulamento VIS, a Decisão 2008/633/JAI do Conselho e a Decisão 2004/512/CE do Conselho.

Os outros instrumentos referidos (Regulamentos relativos ao ETIAS, Eurodac, SIS, ECRIS-TCN, eu-LISA) encontram-se presentemente em fase de negociação no Parlamento Europeu e no Conselho. Em relação a estes instrumentos, não é, por conseguinte, possível definir as alterações necessárias nesta fase. A Comissão apresentará as alterações para cada um destes instrumentos no prazo de duas semanas após chegar a um acordo político sobre os respetivos projetos de regulamento.

- **Coerência com as disposições existentes no mesmo domínio de intervenção**

A presente proposta insere-se no quadro do processo mais vasto que foi lançado pela Comunicação de abril de 2016 intitulada *Sistemas de informação mais sólidos e mais inteligentes para controlar as fronteiras e garantir a segurança*, e dos trabalhos posteriores do grupo de peritos de alto nível sobre os sistemas de informação e interoperabilidade. Tem como finalidade concretizar três objetivos:

a) reforçar e maximizar as vantagens dos **sistemas de informação atuais**;

b) colmatar lacunas de informação, mediante a criação de novos sistemas de informação;

c) reforçar a interoperabilidade entre estes sistemas.

Relativamente ao primeiro objetivo, a Comissão adotou propostas em dezembro de 2016 para reforçar o atual Sistema de Informação Schengen (SIS)[25]. Relativamente ao Eurodac, na sequência da proposta da Comissão de maio de 2016[26], as negociações relativamente à base

[25] COM(2016) 883 final.
[26] COM(2016) 272 final.

jurídica revista foram aceleradas. Encontra-se igualmente em preparação uma nova base jurídica para o Sistema de Informação sobre Vistos (VIS), que será apresentada no segundo trimestre de 2018.

Com respeito ao segundo objetivo, as negociações sobre a proposta de abril de 2016 da Comissão para criar um Sistema de Entrada/Saída (SES)[27] foram concluídas logo no início de julho de 2017, altura em que os colegisladores chegaram a um acordo político, confirmado pelo Parlamento Europeu em outubro de 2017 e adotado formalmente pelo Conselho em novembro de 2017. A base jurídica entrará em vigor em dezembro de 2017. As negociações sobre a proposta de novembro de 2016 para a criação de um Sistema Europeu de Informação e Autorização de Viagem (ETIAS)[28] já começaram e está previsto que terminem nos próximos meses. Em junho de 2017, a Comissão propôs uma base jurídica para colmatar outra lacuna em matéria de informação: o Sistema Europeu de Informação sobre Registos Criminais para nacionais de países terceiros (sistema ECRIS-TCN)[29]. Uma vez mais os colegisladores indicaram que pretendem uma adoção rápida dessa base jurídica.

A presente proposta aborda o terceiro objetivo identificado na Comunicação de abril de 2016.

- **Coerência com outras políticas da União no domínio da Justiça e dos Assuntos Internos**

A presente proposta, juntamente com a proposta conexa cumpre, e está em consonância com a Agenda Europeia da Migração e as comunicações subsequentes, incluindo a comunicação sobre a preservação e o reforço de Schengen[30], bem como a Agenda Europeia para a Segurança[31] e os relatórios da Comissão sobre o trabalho e os progressos alcançados rumo a uma União da Segurança genuína e eficaz[32]. É coerente com outras políticas da União, nomeadamente:

- Segurança interna: a Agenda Europeia para a Segurança afirma que é fundamental estabelecer normas comuns de gestão das fronteiras para prevenir a criminalidade transnacional e o terrorismo. A presente proposta contribui para atingir um elevado nível de segurança interna na medida em que coloca à disposição das autoridades os meios necessários para acederem de forma rápida, contínua, sistemática e controlada às informações de que necessitam.

- Asilo: a proposta inclui o Eurodac como um dos sistemas centrais da UE que será abrangido pela interoperabilidade.

- A gestão das fronteiras externas e a segurança: a presente proposta reforça os sistemas SIS e VIS, que contribuem para o controlo eficaz das fronteiras externas da União, bem como o futuro SES e os sistemas ETIAS e ECRIS-TCN propostos.

[27] COM(2016) 194 final.
[28] COM(2016) 731 final.
[29] COM(2017) 344 final.
[30] COM(2017)570 final.
[31] COM(2015)185 final.
[32] COM(2016)230 final.

2. BASE JURÍDICA, SUBSIDIARIEDADE E PROPORCIONALIDADE

• Base jurídica

Os artigos do Tratado sobre o Funcionamento da União Europeia a seguir indicados constituirão a principal base jurídica: artigo 16.º, n.º 2, artigo 74.º, artigo 77.º, n.º 2, alíneas a), b), d) e e).

Nos termos do artigo 16.º, n.º 2, a União tem o poder de adotar medidas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados. Nos termos do artigo 74.º, o Conselho pode adotar medidas destinadas a assegurar a cooperação administrativa entre os serviços dos Estados-Membros no domínio da justiça, liberdade e segurança. Nos termos do artigo 77.º, n.º 2, alíneas a), b), d) e e), respetivamente, o Parlamento Europeu e o Conselho podem aprovar medidas relativas à política comum em matéria de vistos e outras autorizações de residência de curta duração, bem como aos controlos a que são sujeitas as pessoas na passagem das fronteiras externas, qualquer medida necessária à introdução gradual de um sistema integrado de gestão das fronteiras externas e a ausência de quaisquer controlos de pessoas, independentemente da sua nacionalidade, na passagem das fronteiras internas.

• Subsidiariedade

A liberdade de circulação na UE requer que as fronteiras externas da União sejam geridas de forma eficaz para garantir a segurança. Os Estados-Membros acordaram, por conseguinte, em fazer face a estes desafios coletivamente, em particular mediante a partilha de informações através dos sistemas centralizados da UE no domínio da justiça e dos assuntos internos. Este facto é confirmado pelas várias conclusões que foram adotadas pelo Conselho Europeu e pelo Conselho, em particular desde 2015.

A ausência de controlos nas fronteiras internas requer uma boa gestão das fronteiras externas de Schengen, em que cada Estado-Membro ou país associado de Schengen tem a obrigação de controlar a fronteira externa em nome dos outros Estados Schengen. Por conseguinte, nenhum Estado-Membro é capaz de fazer face unilateralmente à migração irregular e à criminalidade transfronteiras. Os nacionais de países terceiros que entrem no espaço sem controlos nas fronteiras internas podem viajar livremente no seu interior. Num espaço sem fronteiras internas, as medidas contra a imigração irregular e a criminalidade e o terrorismo internacionais, incluindo através da deteção de fraude de identidade, têm de ser tomadas em comum, e a sua abordagem só será bem-sucedida se for empreendida ao nível da UE.

A nível da UE já existem ou já estão a ser implementados sistemas de informação comuns relevantes. Uma maior interoperabilidade entre esses sistemas de informação implica necessariamente uma ação a nível da UE. O objetivo central desta proposta consiste na melhoria da eficiência e da utilização de sistemas centralizados geridos pela eu-LISA. Em virtude da dimensão, dos efeitos e do impacto das ações previstas, os objetivos fundamentais só serão alcançados com eficiência e de forma sistemática a nível da UE.

- **Proporcionalidade**

Tal como se explica em pormenor na avaliação de impacto que acompanha a presente proposta de regulamento, as escolhas políticas apresentadas na mesma são consideradas proporcionais. Não excedem o que é necessário para alcançar os objetivos acordados.

O **portal europeu de pesquisa (ESP)** é um instrumento necessário para reforçar a utilização autorizada dos sistemas de informação atuais e futuros da UE. O impacto do ESP em termos de tratamento de dados é muito limitado. Não armazenará dados, com exceção das informações sobre os vários perfis de utilizadores do ESP, bem como os dados e sistemas de informação aos quais têm acesso, e o acompanhamento da sua utilização através de registos. A função do ESP como intermediário de mensagens, catalisador e facilitador, é proporcional, necessária e limitada em termos de pesquisas e de direitos de acesso no âmbito dos mandatos das bases jurídicas relacionadas com os sistemas de informação e o regulamento proposto em matéria de interoperabilidade.

O **serviço partilhado de correspondências biométricas (BMS)** é necessário para o funcionamento do ESP, do repositório comum de dados de identificação e do detetor de identidades múltiplas, e facilita a utilização e a manutenção dos atuais e futuros sistemas de informação da UE pertinentes. A sua funcionalidade permite pesquisar dados biométricos provenientes de várias fontes, de forma eficiente, contínua e sistemática. Os dados biométricos são armazenados e mantidos pelos sistemas subjacentes. O BMS cria modelos, mas elimina as imagens reais. Como tal, os dados são armazenados num único local, uma única vez.

O **repositório comum de dados de identificação (CIR)** é necessário para atingir o objetivo da identificação correta de nacionais de países terceiros, por exemplo, durante um controlo de identidade no espaço Schengen. O CIR suporta também o funcionamento do detetor de identidades múltiplas e é, por conseguinte, um componente necessário para alcançar o duplo objetivo de facilitar os controlos de identidade de viajantes de boa-fé e combater a fraude de identidade. O acesso ao CIR para este efeito está limitado aos utilizadores que necessitam dessa informação para poderem desempenhar as suas funções (que exige que esses controlos se tornem um novo objetivo complementar do Eurodac, do VIS, do futuro SES e dos sistemas ETIAS e ECRIS-TCN propostos). Os tratamentos dos dados são rigorosamente limitados ao que é necessário para atingir este objetivo, e serão criadas salvaguardas adequadas a fim de garantir o respeito pelos direitos de acesso, e que os dados armazenados no CIR se limitam ao mínimo necessário. A fim de assegurar a minimização dos dados e evitar a sua duplicação desnecessária, o CIR detém os dados biográficos necessários de cada um dos sistemas subjacentes – armazenados, acrescentados, alterados e eliminados em conformidade com a respetiva base jurídica – sem cópia dos mesmos. As condições de conservação dos dados estão totalmente alinhadas com as disposições em matéria de conservação de dados dos sistemas de informação subjacentes que fornecem os dados de identificação.

O **detetor de identidades múltiplas (MID)** é necessário para assegurar uma solução para a deteção de identidades múltiplas, com o duplo objetivo de facilitar os controlos de identidade de viajantes de boa-fé e combater a fraude de identidade. O MID conterá as ligações entre as pessoas presentes em mais de um sistema de informação central, estritamente limitadas aos dados necessários para verificar se uma pessoa está registada lícita ou ilicitamente sob diferentes identidades biográficas em sistemas diferentes, mas também para clarificar situações em que duas pessoas com dados biográficos semelhantes podem não ser a mesma pessoa. O tratamento de dados através do MID e do BMS a fim de ligar os processos individuais entre os sistemas individuais, é mantido dentro dos mínimos indispensáveis. O

MID incluirá salvaguardas contra eventuais discriminações ou decisões desfavoráveis para pessoas com identidades múltiplas lícitas.

- **Escolha do instrumento**

É proposto um regulamento do Parlamento Europeu e do Conselho. A legislação proposta aborda diretamente o funcionamento dos sistemas de informação centrais da UE para controlar fronteiras e garantir a segurança, que foram criados, ou com proposta de criação, no âmbito dos regulamentos. Do mesmo modo, a eu-LISA, que será responsável pela conceção e desenvolvimento e, na devida altura, pela gestão técnica, dos componentes, foi igualmente criada no âmbito de um regulamento. Um regulamento, é, portanto, uma opção adequada como instrumento.

3. RESULTADOS DAS CONSULTAS DAS PARTES INTERESSADAS E DAS AVALIAÇÕES DE IMPACTO

- **Consulta pública**

No quadro da preparação da presente proposta, a Comissão lançou, em julho de 2017, uma consulta pública para recolher as opiniões das partes interessadas sobre o tema da interoperabilidade. Foram recebidas 18 respostas de uma grande variedade de partes interessadas, incluindo de governos dos Estados-Membros, de organizações do setor privado, de outras organizações, como ONG e grupos de reflexão, assim como de particulares[33]. De um modo geral, as respostas estavam largamente a favor dos princípios subjacentes da presente proposta de interoperabilidade. A grande maioria dos inquiridos concordou que os problemas identificados pela consulta estavam corretos e que os objetivos que o pacote de interoperabilidade pretende alcançar estão corretos. Em especial, os inquiridos consideraram que as opções delineadas no documento de consulta iriam:

- ajudar o pessoal no terreno a aceder à informação de que necessita;
- evitar a duplicação de dados, reduzir as sobreposições e evidenciar discrepâncias nos dados;
- identificar as pessoas de forma mais fiável, incluindo pessoas com identidades múltiplas, e reduzir a fraude de identidade.

Uma clara maioria dos inquiridos apoiou cada uma das opções propostas e considerou-as como sendo necessárias para atingir os objetivos da presente iniciativa, sublinhando, nas suas respostas, a necessidade de medidas fortes e claras em matéria de proteção dos dados, em particular no que respeita ao acesso às informações armazenadas nos sistemas e à conservação de dados, e a necessidade de dados atualizados e de elevada qualidade nos sistemas e de medidas para o garantir.

Todos os pontos levantados foram tidos em conta na elaboração da presente proposta.

[33] Para informações mais pormenorizadas, consultar o relatório de síntese anexo à avaliação de impacto.

- **Inquérito Eurobarómetro**

Em junho de 2017, foi realizado um inquérito Eurobarómetro Especial[34], demonstrando que a estratégia da UE de partilha de informações a nível da UE na luta contra a criminalidade e o terrorismo tem um apoio generalizado do público: quase todos os inquiridos (92 %) concordam que as autoridades nacionais devem partilhar informações com as autoridades de outros Estados-Membros, a fim de melhor lutar contra a criminalidade e o terrorismo.

Uma clara maioria (69 %) dos inquiridos manifestou a opinião de que a polícia e outras autoridades nacionais de aplicação da lei devem partilhar as informações com outros países da UE numa base sistemática. Em todos os Estados-Membros, a maioria dos inquiridos considera que as informações devem ser partilhadas em todos os casos.

- **Grupo de peritos de alto nível em matéria de sistemas de informação e interoperabilidade**

Tal como referido na introdução, a presente proposta tem por base as recomendações do **grupo de peritos de alto nível sobre os sistemas de informação e interoperabilidade**[35]. Este grupo foi criado em junho de 2016 com o objetivo de dar resposta aos desafios jurídicos, técnicos e operacionais das opções disponíveis com vista à interoperabilidade entre sistemas centrais da UE para controlar fronteiras e garantir a segurança. O grupo adotou uma perspetiva ampla e abrangente relativamente à arquitetura de gestão de dados para a gestão das fronteiras e de aplicação da lei, tendo igualmente em conta as funções, responsabilidades e sistemas das autoridades aduaneiras relevantes.

O grupo reuniu peritos dos Estados-Membros e dos países associados de Schengen, bem como das seguintes agências da UE: eu-LISA, Europol, Gabinete Europeu de Apoio em matéria de Asilo, Agência Europeia da Guarda de Fronteiras e Costeira e Agência dos Direitos Fundamentais da União Europeia. O Coordenador da UE da Luta Antiterrorista e a Autoridade Europeia para a Proteção de Dados também participaram no grupo de peritos como membros de pleno direito. Além disso, representantes do Secretariado da Comissão das Liberdades Cívicas, Justiça e Assuntos Internos do Parlamento Europeu e do Secretariado-Geral do Conselho estiveram presentes enquanto observadores.

O **relatório final do grupo de peritos de alto nível** foi publicado em maio de 2017[36]. Chamou a atenção para a necessidade de colmatar as lacunas estruturais identificadas na Comunicação de abril de 2016. Delineou uma série de recomendações destinadas a reforçar e a desenvolver os sistemas de informação e a interoperabilidade da UE. Concluiu que é **necessário e tecnicamente viável trabalhar rumo ao portal europeu de pesquisa, ao serviço partilhado de correspondências biométricas e ao repositório comum de dados de identificação como soluções de interoperabilidade** e que estes podem, em princípio, gerar ganhos operacionais e ser estabelecidos em conformidade com as exigências em matéria de proteção de dados. O grupo recomendou igualmente considerar a opção adicional de uma

---

[34] O *Relatório sobre as atitudes dos europeus em relação à segurança* analisa os resultados do inquérito Eurobarómetro Especial (464b) que sonda a opinião pública no que respeita à sensibilização, experiências e perceções em geral dos cidadãos relativamente à segurança. Este inquérito foi realizado pela rede TNS Political & Social nos 28 Estados-Membros entre 13 e 26 de junho de 2017. Foram entrevistados cerca de 28 093 cidadãos da UE de diferentes categorias sociais e demográficas.

[35] Decisão da Comissão de 17 de junho de 2016 que institui o Grupo de Peritos de Alto Nível em matéria de sistemas de informação e interoperabilidade – 2016/C 257/03.

[36] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

abordagem em duas fases no sentido do acesso para fins de aplicação da lei, com base numa funcionalidade de indicadores de respostas positivas.

A presente proposta de regulamento responde igualmente às recomendações do grupo de peritos de alto nível relativamente à qualidade dos dados, ao Formato de Mensagem Universal (UMF) e à criação de um armazém de dados (aqui apresentado como o repositório central para a elaboração de relatórios e estatísticas (CRRS).

O grupo de peritos de alto nível não identificou o quarto componente de interoperabilidade proposto no presente projeto de regulamento (o detetor de identidades múltiplas), tendo o mesmo surgido no decurso da análise técnica adicional e da avaliação da proporcionalidade realizada pela Comissão.

- **Estudos técnicos**

Foram encomendados três estudos de apoio à preparação da proposta. A Unisys, contratada pela Comissão, apresentou um relatório sobre um estudo de viabilidade para o portal europeu de pesquisa. A eu-LISA encomendou um relatório técnico à Gartner (com a Unisys) para apoiar o desenvolvimento do serviço partilhado de correspondências biométricas. A PWC apresentou à Comissão um relatório técnico sobre um repositório comum de dados de identificação.

- **Avaliação de impacto**

A presente proposta é apoiada por uma avaliação de impacto apresentada no documento de trabalho dos serviços da Comissão SWD(2017) 473.

O Comité de Controlo da Regulamentação analisou o projeto de avaliação de impacto na sua reunião de 6 de dezembro de 2017 e emitiu o seu parecer (positivo com reservas) em 8 de dezembro, indicando que a avaliação de impacto deve ser adaptada, a fim de integrar as recomendações do Comité sobre aspetos específicos. Estas dizem respeito, em primeiro lugar, a medidas adicionais no âmbito da opção preferida que otimiza os direitos existentes em matéria de acesso aos dados dos utilizadores finais nos sistemas de informação da UE, e para ilustrar salvaguardas conexas em matéria de proteção de dados e direitos fundamentais. A segunda consideração principal consistiu em clarificar a integração do Sistema de Informação Schengen na opção 2, incluindo a eficácia e os custos para facilitar a sua comparação com a opção 3 preferida. A Comissão atualizou a sua avaliação de impacto para responder a estas considerações principais e refletir outras observações feitas pelo Comité.

A avaliação de impacto analisou se, e de que modo, é possível alcançar cada um dos objetivos identificados utilizando um ou mais dos componentes técnicos identificados pelo grupo de peritos de alto nível e através de uma análise posterior. Nos casos em que considerou ser necessário, analisou também as subopções necessárias para atingir estes objetivos, respeitando sempre o quadro da proteção de dados. A avaliação de impacto concluiu que:

- Para cumprir o objetivo de fornecer aos utilizadores autorizados um acesso rápido, contínuo, sistemático e controlado aos sistemas de informação pertinentes, é necessário criar um portal europeu de pesquisa (ESP), assente num serviço partilhado de correspondências biométricas (BMS) para lidar com todas as bases de dados.

- Para cumprir o objetivo de facilitar os controlos de identidade de nacionais de países terceiros, no território de um Estado-Membro, por agentes autorizados, é necessário

criar um repositório comum de dados de identificação (CIR), contendo o conjunto mínimo de dados de identificação e assente no mesmo BMS.

- Para cumprir o objetivo da deteção de identidades múltiplas ligadas ao mesmo conjunto de dados biométricos, com o duplo objetivo de facilitar os controlos de identidade para viajantes de boa-fé e combater a fraude de identidade, é necessário construir um detetor de identidades múltiplas (MID), contendo ligações entre identidades múltiplas nos sistemas.

- Para cumprir o objetivo de facilitar e otimizar o acesso das autoridades de aplicação da lei aos sistemas de informação com finalidades não coercivas, para efeitos de prevenção, investigação, deteção ou repressão de crimes graves e terrorismo, deve incluir-se uma funcionalidade de «indicadores de respostas positivas» no CIR.

Uma vez que todos os objetivos devem ser cumpridos, a **solução completa é a combinação do ESP, do CIR (com indicadores de respostas positivas) e do MID, todos assentes no BMS**.

O impacto positivo mais importante será a melhoria da gestão de fronteiras e uma maior segurança interna na União Europeia. Os novos componentes irão otimizar e acelerar o acesso das autoridades nacionais às informações necessárias e à identificação de nacionais de países terceiros. Permitirão às autoridades cruzar ligações com informações necessárias e já existentes sobre indivíduos durante controlos de fronteira, para pedidos de vistos ou de asilo e para o trabalho da polícia. Tal permitirá aceder a informações que podem ajudar na tomada de decisões fiáveis, quer relacionadas com investigações de crimes graves e terrorismo, quer com decisões no domínio da migração e do asilo. Muito embora não afetem diretamente os cidadãos da UE (as medidas propostas visam principalmente os nacionais de países terceiros cujos dados se encontram registados num sistema de informação centralizado da UE), as propostas deverão gerar uma maior confiança junto dos cidadãos, garantindo que a sua conceção e utilização do sistema aumenta a segurança dos cidadãos da UE.

Os impactos financeiros e económicos imediatos da proposta estarão limitados à conceção, desenvolvimento e operação de novos recursos. Os custos ficarão a cargo do orçamento da UE e das autoridades dos Estados-Membros que utilizam os sistemas. O impacto no turismo será positivo, uma vez que as medidas propostas melhorarão a segurança da União Europeia e devem também contribuir para um controlo fronteiriço mais rápido. Do mesmo modo, o impacto nos aeroportos, portos marítimos e transportadoras deverá ser positivo, em especial devido à maior rapidez com que se processam os controlos fronteiriços.

- **Direitos fundamentais**

A avaliação de impacto contemplou em particular os impactos das medidas propostas em matéria de direitos fundamentais e, em especial, o direito à proteção dos dados.

Em conformidade com a Carta dos Direitos Fundamentais da União Europeia, que vincula as instituições da UE e os Estados-Membros quando estes aplicam o direito da União (artigo 51.º, n.º 1, da Carta), as oportunidades, oferecidas pela interoperabilidade como uma medida para reforçar a segurança e a proteção das fronteiras externas, devem ser equilibradas com a obrigação de garantir que as interferências nos direitos fundamentais que possam resultar do novo ambiente de interoperabilidade são limitadas ao estritamente necessário para cumprir efetivamente os objetivos de interesse geral prosseguidos, na observância do princípio da proporcionalidade (artigo 52.º, n.º 1, da Carta).

As soluções de interoperabilidade propostas são componentes complementares de sistemas existentes. Como tal, não iriam alterar o equilíbrio já assegurado por cada um dos sistemas centrais existentes no que diz respeito ao seu impacto positivo sobre os direitos fundamentais.

No entanto, a interoperabilidade tem potencial para ter um impacto indireto adicional sobre uma série de direitos fundamentais. Com efeito, a identificação correta de uma pessoa tem um impacto positivo no direito ao respeito pela vida privada e, em especial, o direito à sua própria identidade (artigo 7.º da Carta), na medida em que pode contribuir para evitar confusões de identidade. Por outro lado, a realização de controlos com base em dados biométricos pode ser considerada uma interferência no direito à dignidade da pessoa (em especial, nos casos em que é considerado como humilhante) (artigo 1.º). No entanto, num inquérito[37] realizado pela Agência dos Direitos Fundamentais da União Europeia, perguntou-se especificamente aos inquiridos se consideravam humilhante terem de fornecer os seus dados biométricos no contexto de um controlo fronteiriço. A maioria dos inquiridos foi da opinião que não era humilhante.

Os componentes de interoperabilidade propostos oferecem a oportunidade de adotar medidas preventivas direcionadas com vista ao reforço da segurança. Como tal, podem contribuir para a proteção do direito à vida das pessoas (artigo 2.º da Carta), o que implica também uma obrigação positiva por parte das autoridades de tomarem medidas operacionais preventivas para protegerem uma pessoa cuja vida esteja em risco, caso saibam ou devam saber da existência de um risco imediato[38], bem como defender a proibição da escravidão e do trabalho forçado (artigo 5.º). Através de uma identificação fiável, mais acessível e mais fácil, a interoperabilidade pode apoiar a deteção de crianças desaparecidas ou sujeitas a tráfico de seres humanos, e facilitar respostas rápidas e fiáveis.

Uma identificação fiável, mais acessível e mais fácil pode também contribuir para garantir que o direito de asilo (artigo 18.º da Carta) e a proibição de repulsão (artigo 19.º da Carta) são efetivamente assegurados. A interoperabilidade pode, com efeito, prevenir situações em que os requerentes de asilo sejam intercetados e detidos ilegalmente, e sujeitos a uma expulsão indevida. Além disso, através da interoperabilidade, a fraude de identidade será mais facilmente identificada. Reduziria também a necessidade de partilhar dados e informações sobre os requerentes de asilo com países terceiros (em especial, o país de origem), a fim de determinar a identidade da pessoa e obter documentos de viagem, que poderiam pôr em perigo a pessoa em causa.

- **Proteção de dados pessoais**

Tendo em conta os dados pessoais envolvidos, a interoperabilidade terá, em especial, repercussões sobre o direito à proteção dos dados pessoais. Este direito está consagrado no artigo 8.º da Carta e no artigo 16.º do Tratado sobre o Funcionamento da União Europeia e no artigo 8.º da Convenção Europeia dos Direitos do Homem. Conforme salientado pelo Tribunal de Justiça da União Europeia[39], o direito à proteção de dados pessoais não é um direito

[37] *Inquérito da FRA no quadro do projeto piloto da eu-LISA sobre fronteiras inteligentes – as opiniões e as experiências dos viajantes relativamente às fronteiras inteligentes,* Relatório da Agência dos Direitos Fundamentais da União Europeia: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_pilot_-_technical_report_annexes_en.pdf.

[38] Tribunal Europeu dos Direitos do Homem, Osman v. Reino Unido, 87/1997/871/1083, 28 de outubro de 1998, n.º 116.

[39] Tribunal de Justiça da União Europeia, acórdão de 9.11.2010 nos processos apensos C-92/09 e C-93/09, Volker e Markus Schecke e Eifert (Coletânea 2010, I-0000).

absoluto, mas deve ser considerado em relação à sua função na sociedade[40]. A proteção de dados está estreitamente relacionada com o respeito pela vida privada e familiar, protegido pelo artigo 7.º da Carta.

De acordo com o Regulamento Geral sobre a Proteção de Dados[41], a livre circulação de dados na UE não deve ser restringida por motivos de proteção de dados. No entanto, é preciso que sejam preenchidos vários princípios. Com efeito, para ser lícita, qualquer restrição ao exercício dos direitos fundamentais protegidos pela Carta deve satisfazer os seguintes critérios, enunciados no seu artigo 52.º, n.º 1:

- deve ser prevista por lei;
- deve respeitar a essência dos direitos;
- deve corresponder efetivamente a objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros;
- deve ser necessária; e
- deve ser proporcional.

A presente proposta incorpora todas estas regras em matéria de proteção de dados, tal como indicado em pormenor na avaliação de impacto que acompanha a presente proposta de regulamento. A proposta tem por base os princípios da proteção de dados desde a conceção e por defeito. Inclui todas as disposições adequadas que limitam o tratamento de dados ao estritamente necessário para as finalidades específicas e só autorizando o acesso aos dados às entidades com «necessidade de tomar conhecimento». Os períodos de conservação de dados (se for caso disso) são adequados e limitados. O acesso aos dados está reservado em exclusivo ao pessoal devidamente autorizado das autoridades dos Estados-Membros ou organismos da UE que são competentes para os fins específicos de cada sistema de informação, e limitado aos dados necessários à execução das tarefas, em conformidade com estes fins.

4. INCIDÊNCIA ORÇAMENTAL

As implicações orçamentais estão incluídas na ficha financeira anexa. Abrange o período remanescente do atual quadro financeiro plurianual (até 2020) e os sete anos do período seguinte (2021-2027). O orçamento proposto para o ano de 2021 e seguintes está incluído a título ilustrativo e não prejudica o próximo quadro financeiro plurianual.

A execução da presente proposta exigirá dotações orçamentais para:

(1) O **desenvolvimento** e a integração pela eu-LISA dos quatro componentes de interoperabilidade, e o repositório central para a elaboração de relatórios e estatísticas

[40] Nos termos do artigo 52.º, n.º 1, da Carta, podem ser impostas restrições ao exercício do direito à proteção de dados desde que sejam previstas por lei, respeitem o conteúdo essencial desse direito e liberdade e, na observância do princípio da proporcionalidade, só podem ser introduzidas se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União Europeia, ou à necessidade de proteção dos direitos e liberdades de terceiros.

[41] 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 (Regulamento Geral sobre a Proteção de Dados).

e a sua posterior **manutenção e operações**.

(2) A **migração dos dados** para o serviço partilhado de correspondências biométricas (BMS) e o repositório comum de dados de identificação (CIR). No caso do BMS, é necessário recriar os modelos biométricos dos dados correspondentes dos três sistemas que utilizam atualmente a biometria (SIS, VIS e Eurodac) no BMS. No caso do CIR, é necessário migrar os elementos dos dados pessoais do VIS para o CIR, e é necessário validar as eventuais ligações detetadas entre identidades presentes no SIS, VIS e Eurodac. Este último processo, em particular, exige muitos recursos.

(3) A atualização pela eu-LISA da **interface nacional uniforme** (IUN) já incluída no Regulamento SES para se tornar um componente genérico que permita o intercâmbio de mensagens entre os Estados-Membros e os sistemas centrais.

(4) A **integração dos sistemas nacionais dos Estados-Membros** na IUN que enviará as mensagens trocadas com o CIR/detetor de identidades múltiplas através do portal europeu de pesquisa.

(5) A **formação** sobre a utilização dos componentes de interoperabilidade pelos utilizadores finais, inclusivamente através da Agência da União Europeia para a Formação Policial (CEPOL).

Os componentes de interoperabilidade são construídos e mantidos sob a forma de um programa. Embora o portal europeu de pesquisa (ESP) e o detetor de identidades múltiplas sejam componentes inteiramente novos, juntamente com o repositório central para a elaboração de relatórios e estatísticas (CRRS), o BMS e o CIR são componentes partilhados que combinam os dados existentes, guardados (ou que vão ser guardados) em sistemas novos ou existentes, com as suas estimativas orçamentais existentes.

O **ESP** implementará interfaces conhecidas e existentes no SIS, no VIS e no Eurodac e irá, em devido tempo, ser alargado a novos sistemas.

O ESP será utilizado pelos Estados-Membros e agências através de uma interface baseada no formato de mensagem universal (UMF). Esta nova interface exigirá desenvolvimentos, adaptações, integrações e testes a realizar pelos Estados-Membros, eu-LISA, Europol e Agência Europeia da Guarda de Fronteiras e Costeira. O ESP utilizaria os conceitos da interface nacional uniforme (IUN) introduzida para o SES, que reduziria os esforços de integração.

O ESP irá gerar custos adicionais para a Europol, a fim de tornar a interface QUEST disponível para utilização com dados com o nível básico de proteção (BPL).

A base do **BMS** será estabelecida *de facto* com a criação do novo SES uma vez que constitui, de longe, o maior volume de novos dados biométricos. O orçamento necessário foi reservado ao abrigo do instrumento jurídico do SES. A adição de mais dados biométricos do VIS, do SIS e do Eurodac ao BMS constitui um custo suplementar essencialmente associado à migração dos dados existentes. Está estimado em 10 milhões de EUR para os três sistemas. A adição de novos dados biométricos do sistema ECRIS-TCN proposto constitui um custo adicional limitado que pode ser coberto pelos fundos reservados ao instrumento jurídico do ECRIS-TCN proposto para criar um sistema automático de identificação dactiloscópica ECRIS-TCN.

O **repositório comum de dados de identificação** será estabelecido com a criação do SES futuro, e posteriormente alargado quando se desenvolver o ETIAS proposto. O armazenamento e os motores de busca para estes dados foram incluídos no orçamento reservado aos instrumentos jurídicos do SES futuro e do ETIAS proposto. A adição de novos dados biográficos, tanto do Eurodac como do sistema ECRIS-TCN proposto, constitui um pequeno custo adicional que já se encontrava reservado aos instrumentos jurídicos do Eurodac e do ECRIS-TCN proposto.

O orçamento total necessário no período de nove anos (2019-2027) é de 424,7 milhões de EUR, abrangendo os seguintes elementos:

(1) Um orçamento de 225 milhões de EUR para a eu-LISA que cobre o custo total do desenvolvimento do programa que fornece os cinco componentes de interoperabilidade (68,3 milhões de EUR), os custos de manutenção a partir do momento em que os componentes são entregues até 2027 (56,1 milhões de EUR), um orçamento específico de 25 milhões de EUR para a migração dos dados dos sistemas existentes para o BMS, e os custos adicionais para a atualização da IUN, rede, formação e reuniões. Um orçamento específico de 18,7 milhões de EUR cobre o custo de modernização e de funcionamento do ECRIS-TCN em modo de alta disponibilidade a partir de 2022.

(2) Um orçamento de 136,3 milhões de EUR para os Estados-Membros, para cobrir as alterações nos respetivos sistemas nacionais para poderem utilizar os componentes de interoperabilidade, a IUN fornecida pela eu-LISA, e um orçamento para a formação da comunidade substancial de utilizadores finais.

(3) Um orçamento de 48,9 milhões de EUR para a Europol, para cobrir a atualização dos sistemas informáticos da Europol em função do volume de mensagens a tratar e dos crescentes níveis de desempenho[42]. Os componentes de interoperabilidade serão utilizados pelo ETIAS tendo em vista a consulta dos dados da Europol.

(4) Um orçamento de 4,8 milhões de EUR para a Agência Europeia da Guarda de Fronteiras e Costeira, para acolher uma equipa de especialistas que, durante um ano, irá validar as ligações entre identidades assim que o detetor de identidades múltiplas for lançado.

(5) Um orçamento de 2,0 milhões de EUR para a Agência da União Europeia para a Formação Policial (CEPOL), para cobrir a preparação e realização de ações de formação para o pessoal operacional.

(6) Uma provisão de 7,7 milhões de EUR afetada à DG Migração e Assuntos Internos, para cobrir um aumento limitado de pessoal e custos conexos durante o período de desenvolvimento dos diferentes componentes, na medida em que a Comissão terá igualmente de desempenhar outras tarefas durante esse período e assume a responsabilidade pelo comité que está a tratar do Formato de Mensagem Universal.

O Regulamento relativo ao FSI Fronteiras é o instrumento financeiro no qual foi incluído o orçamento para a execução da iniciativa de interoperabilidade. No seu artigo 5.º, alínea b),

[42] A atual capacidade de tratamento de informações da Europol não é compatível com os volumes substanciais (média de 100 000 consultas por dia) e o reduzido tempo de resposta que será exigido pelo ETIAS.

prevê a aplicação de 791 milhões de EUR através de um programa para o desenvolvimento de sistemas informáticos, com base em sistemas informáticos existentes e/ou novos, de apoio à gestão dos fluxos migratórios nas fronteiras externas, sob reserva da adoção dos atos legislativos pertinentes da União e nos termos do artigo 15.º, n.º 5. Deste montante de 791 milhões de EUR, 480,2 milhões de EUR estão reservados ao desenvolvimento do SES, 210 milhões de EUR ao ETIAS e 67,9 milhões de EUR à revisão do SIS. A parte remanescente (32,9 milhões de EUR) será reafetada utilizando os mecanismos FSI-F. A atual proposta prevê 32,1 milhões de EUR para o atual período do quadro financeiro plurianual (2019/20) que é, pois, coerente com o orçamento restante.

5. INFORMAÇÕES SUPLEMENTARES

- **Planos de execução e mecanismos de acompanhamento, de avaliação e de informação**

A eu-LISA é responsável pela gestão operacional de sistemas informáticos em grande escala no domínio da liberdade, segurança e justiça. Como tal, tem já a seu cargo o funcionamento e os aperfeiçoamentos técnicos e operacionais de sistemas existentes e o desenvolvimento dos futuros sistemas já previstos. No quadro da presente proposta de regulamento, define a conceção da arquitetura física dos componentes de interoperabilidade, desenvolve e implementa-os e, em última análise, aloja-os. Os respetivos componentes serão implementados gradualmente, em conjunto com o desenvolvimento dos sistemas subjacentes.

A Comissão assegurará a criação de sistemas que irão acompanhar o desenvolvimento e o funcionamento dos quatro componentes (portal europeu de pesquisa, serviço partilhado de correspondências biométricas, repositório comum de dados de identificação, detetor de identidades múltiplas) e do repositório central para a elaboração de relatórios e estatísticas, e irá avaliá-los em relação aos principais objetivos políticos. Quatro anos após a criação e a entrada em funcionamento das funcionalidades e, posteriormente, de quatro em quatro anos, a eu-LISA deve apresentar ao Parlamento Europeu, ao Conselho e à Comissão um relatório sobre o funcionamento técnico dos componentes de interoperabilidade. Além disso, cinco anos após a criação e a entrada em funcionamento das funcionalidades e, posteriormente, de quatro em quatro anos, a Comissão deve apresentar uma avaliação global dos componentes, incluindo sobre o impacto direto ou indireto dos componentes e sobre a sua aplicação prática em matéria de direitos fundamentais. Deve examinar os resultados obtidos relativamente aos objetivos fixados e determinar se os princípios de base continuam a ser válidos e quais as eventuais implicações para as futuras opções. A Comissão deverá apresentar os relatórios de avaliação ao Parlamento Europeu e ao Conselho.

- **Explicação pormenorizada das disposições específicas da proposta**

O capítulo I estabelece as disposições gerais do presente regulamento. Explica: os princípios subjacentes ao regulamento; os componentes nele estabelecidos; os objetivos que a interoperabilidade procura tratar; o âmbito do presente regulamento; as definições dos termos utilizados no presente regulamento; e o princípio da não discriminação em matéria de tratamento de dados nos termos do presente regulamento.

O capítulo II estabelece as disposições para o portal europeu de pesquisa (ESP). Este capítulo prevê a criação do ESP e da sua arquitetura técnica, que será desenvolvida pela eu-LISA. Especifica o objetivo do ESP e identifica quem pode utilizá-lo e o modo como deverá utilizá-lo de acordo com os direitos de acesso já existentes para cada um dos sistemas centrais. Existe uma disposição para a eu-LISA criar perfis de utilizador para cada categoria de utilizador. Este capítulo define o modo como o ESP irá consultar os sistemas centrais e determina o conteúdo e formato das respostas aos utilizadores. O capítulo II estabelece igualmente que a eu-LISA deve conservar registos de todas as operações de tratamento de dados, e prevê o procedimento alternativo no caso de o ESP não conseguir aceder a um ou mais sistemas centrais.

O capítulo III estabelece as disposições relativas ao serviço partilhado de correspondências biométricas (BMS). Este capítulo prevê a criação do BMS e da sua arquitetura técnica, que será desenvolvida pela eu-LISA. Especifica o objetivo do BMS e define quais os dados que armazena. Explica a relação entre o BMS e os outros componentes. O capítulo III prevê igualmente que o BMS não continuará a armazenar dados quando estes deixarem de fazer parte do respetivo sistema central, e prevê que a eu-LISA conservará registos de todas as operações de tratamento.

O capítulo IV estabelece as disposições para o repositório comum de dados de identificação (CIR). Este capítulo prevê a criação do CIR e da sua arquitetura técnica, que será desenvolvida pela eu-LISA. Define o objetivo do CIR e clarifica quais os dados que serão armazenados, e como, incluindo disposições para garantir a qualidade dos dados armazenados. Este capítulo prevê que o CIR criará processos individuais com base em dados existentes nos sistemas centrais, e que os processos individuais serão atualizados no seguimento de alterações nos sistemas centrais individuais. O capítulo IV especifica igualmente como se processará o funcionamento do CIR em relação ao detetor de identidades múltiplas. O presente capítulo identifica as pessoas que podem ter acesso ao CIR e a forma como podem aceder aos dados, em conformidade com os direitos de acesso, e disposições mais específicas consoante o acesso seja para efeitos de identificação ou, como uma primeira etapa da abordagem em duas fases, para aceder ao SES, ao VIS, ao ETIAS e ao Eurodac, através do CIR, para fins de aplicação da lei. O capítulo IV prevê igualmente que a eu-LISA conservará registos de todas as operações de tratamento relativas ao CIR.

O capítulo V estabelece as disposições para o detetor de identidades múltiplas (MID). Este capítulo prevê a criação do MID e da sua arquitetura técnica, que será desenvolvida pela eu-LISA. Explica o objetivo do MID e regula a sua utilização em conformidade com os direitos de acesso a cada um dos sistemas centrais. O capítulo V define quando, e de que modo, o MID lançará as pesquisas para detetar identidades múltiplas, e o modo como os resultados são entregues e devem ser seguidos, incluindo, se necessário, através de verificação manual. O capítulo V define uma classificação dos tipos de ligação que podem resultar da pesquisa, consoante o resultado revele uma identidade única, identidades múltiplas ou dados de identificação partilhados. Este capítulo prevê que o MID armazenará dados ligados existentes em sistemas centrais, enquanto os dados se mantiverem em dois ou mais sistemas centrais individuais. O capítulo V prevê igualmente que a eu-LISA conservará registos de todas as operações de tratamento relativas ao MID.

O capítulo VI prevê medidas destinadas a apoiar a interoperabilidade. Prevê a melhoria da qualidade dos dados, através da criação do Formato de Mensagem Universal como a norma comum para o intercâmbio de informações de apoio à interoperabilidade, e do estabelecimento de um repositório central para a elaboração de relatórios e estatísticas.

O capítulo VII diz respeito à proteção de dados. Este capítulo estabelece disposições para garantir que os dados tratados nos termos do presente regulamento são tratados legalmente e de forma adequada, nos termos das disposições do Regulamento n.º 45/2001. Explica quem será o subcontratante de dados para cada uma das medidas de interoperabilidade propostas no presente regulamento, define medidas necessárias da eu-LISA e das autoridades dos Estados-Membros, a fim de assegurar a segurança do tratamento dos dados, a confidencialidade dos dados, o tratamento adequado dos incidentes de segurança e a monitorização adequada do cumprimento das medidas estabelecidas no presente regulamento. O capítulo também inclui disposições relativas aos direitos dos titulares dos dados, incluindo o direito de ser informado de que os dados a seu respeito foram armazenados e tratados nos termos do presente regulamento, e o direito de aceder, retificar e apagar os dados pessoais armazenados e tratados nos termos do presente regulamento. Este capítulo estabelece ainda o princípio de que os dados tratados nos termos do presente regulamento não devem ser transferidos ou disponibilizados a países terceiros, organizações internacionais ou entidades privadas, com exceção da Interpol para algumas finalidades específicas, bem como os dados recebidos da Europol através do portal europeu de pesquisa em que se aplicam as regras do Regulamento 2016/794 em matéria de tratamento de dados subsequente. Por último, o capítulo estabelece as disposições relativas à supervisão e auditoria em matéria de proteção de dados.

O capítulo VIII estabelece as responsabilidades da eu-LISA antes e depois da entrada em funcionamento das medidas previstas na presente proposta, bem como dos Estados -Membros, da Europol e da unidade central do ETIAS.

O capítulo IX diz respeito a alterações a outros instrumentos da União. O presente capítulo apresenta as alterações necessárias a outros instrumentos jurídicos, para assegurar a plena aplicação da presente proposta de interoperabilidade. A presente proposta contém disposições pormenorizadas para as alterações necessárias aos instrumentos jurídicos que são atualmente textos estáveis, conforme aprovados pelos colegisladores: o Código das Fronteiras Schengen, o Regulamento SES, o Regulamento VIS (CE), a Decisão 2004/512/CE do Conselho (Decisão VIS) e a Decisão 2008/633/JAI do Conselho (Decisão VIS/acesso para fins de aplicação da lei).

O capítulo X define em pormenor: os requisitos em termos de estatísticas e elaboração de relatórios relacionados com o tratamento de dados nos termos do presente regulamento; medidas transitórias que serão necessárias; disposições relativas aos custos decorrentes do presente regulamento; requisitos relativos às notificações; o processo para o início do funcionamento das medidas propostas no presente regulamento; mecanismos de governação, incluindo a constituição de um comité e de um grupo consultivo, a responsabilidade da eu-LISA em relação à formação e um manual prático de apoio à aplicação e gestão dos componentes de interoperabilidade; os procedimentos relativos ao acompanhamento e à avaliação das medidas propostas no presente regulamento; e a disposição para a entrada em vigor do presente regulamento.

2017/0351 (COD)

Proposta de

REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO

relativo à criação de um quadro para a interoperabilidade entre os sistemas de informação da UE (fronteiras e vistos) e que altera a Decisão 2004/512/CE do Conselho, o Regulamento (CE) n.º 767/2008, a Decisão 2008/633/JAI do Conselho, o Regulamento (UE) 2016/399 e o Regulamento (UE) 2017/2226

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 16.º, n.º 2, o artigo 74.º e o artigo 77.º, n.º 2, alíneas a), b), d) e e),

Tendo em conta a proposta da Comissão Europeia,

Após transmissão do projeto de ato legislativo aos parlamentos nacionais,

Após consulta da Autoridade Europeia para a Proteção de Dados,

Tendo em conta o parecer do Comité Económico e Social Europeu,[43]

Tendo em conta o parecer do Comité das Regiões,[44]

Deliberando de acordo com o processo legislativo ordinário,

Considerando o seguinte:

(1) Na sua Comunicação, de 6 de abril de 2016, intitulada *«Sistemas de informação mais sólidos e inteligentes para controlar as fronteiras e garantir a segurança»*[45], a Comissão sublinhou a necessidade de melhorar a arquitetura de gestão de dados da União para fins de controlo das fronteiras e de segurança. A comunicação iniciou um processo no sentido de alcançar a interoperabilidade entre os sistemas de informação da UE para a segurança e a gestão de fronteiras e da migração, a fim de enfrentar as deficiências estruturais relacionadas com estes sistemas que dificultam o trabalho das autoridades nacionais, e assegurar que os guardas de fronteira, as autoridades aduaneiras, os agentes de polícia e as autoridades judiciárias dispõem das informações necessárias.

(2) No seu Roteiro para intensificar o intercâmbio e a gestão de informações, incluindo soluções de interoperabilidade no domínio da Justiça e Assuntos Internos de 6 de

[43] JO C , , p. .

[44]

[45] COM(2016) 205 de 6.4.2016.

junho de 2016[46], o Conselho identificou vários desafios de caráter jurídico, técnico e operacional na interoperabilidade dos sistemas de informação da UE e apelou à procura de soluções.

(3) Na sua resolução de 6 de julho de 2016 sobre as prioridades estratégicas do Programa de Trabalho da Comissão para 2017[47], o Parlamento Europeu apelou à apresentação de propostas para melhorar e desenvolver os atuais sistemas de informação da UE, colmatar lacunas de informação e avançar rumo à interoperabilidade, bem como propostas de partilha obrigatória de informações a nível da UE, acompanhadas das necessárias salvaguardas em matéria de proteção de dados.

(4) O Conselho Europeu de 15 de dezembro de 2016[48] apelou a que se desse continuidade à interoperabilidade dos sistemas de informação e das bases de dados da UE.

(5) No seu relatório final de 11 de maio de 2017[49], o grupo de peritos de alto nível sobre sistemas de informação e interoperabilidade concluiu que é necessário e tecnicamente viável trabalhar rumo a soluções práticas de interoperabilidade e que estas podem, em princípio, gerar ganhos operacionais e ser estabelecidas em conformidade com as exigências em matéria de proteção de dados.

(6) Na sua Comunicação de 16 de maio de 2017 com o título *Sétimo relatório sobre os progressos alcançados rumo à criação de uma União da Segurança genuína e eficaz*[50], a Comissão definiu, na linha da sua Comunicação de 6 de abril de 2016, tendo sido confirmado pelas conclusões e recomendações do grupo de peritos de alto nível sobre sistemas de informação e interoperabilidade, uma nova abordagem à gestão de dados para fins de controlo das fronteiras, segurança e migração onde todos os sistemas de informação da UE para a segurança, gestão de fronteiras e migração são interoperáveis no pleno respeito dos direitos fundamentais.

(7) Nas suas Conclusões de 9 de junho de 2017[51] sobre o caminho a seguir para melhorar o intercâmbio de informações e garantir a interoperabilidade dos sistemas de informação da UE, o Conselho convidou a Comissão a procurar soluções de interoperabilidade, conforme proposto pelo grupo de peritos de alto nível.

(8) O Conselho Europeu de 23 de junho de 2017[52] sublinhou a necessidade de melhorar a interoperabilidade entre as bases de dados e convidou a Comissão a preparar, com a maior brevidade possível, projetos de legislação para concretizar as propostas apresentadas pelo grupo de peritos de alto nível sobre sistemas de informação e interoperabilidade.

(9) A fim de melhorar a gestão das fronteiras externas, contribuir para a prevenção e o combate à migração irregular e contribuir para um nível de segurança elevado no domínio da liberdade, da segurança e da justiça da União, incluindo a manutenção da

---

[46] Roteiro de 6 de junho de 2016 para intensificar o intercâmbio e a gestão de informações, incluindo soluções de interoperabilidade no domínio da Justiça e Assuntos Internos – 9368/1/16 REV 1.

[47] Resolução do Parlamento Europeu, de 6 de julho de 2016, sobre as prioridades estratégicas para o Programa de Trabalho da Comissão para 2017 (2016/2773(RSP)).

[48] http://www.consilium.europa.eu/en/press/press-releases/2016/12/15/euco-conclusions-final/.

[49] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

[50] COM(2017) 261 final de 16.5.2017.

[51] http://www.consilium.europa.eu/media/22186/st10136en17-vf.pdf.

[52] Conclusões do Conselho Europeu, 22-23 de junho de 2017.

segurança e da ordem pública e a salvaguarda da segurança nos territórios dos Estados-Membros, deve estabelecer-se a interoperabilidade entre os sistemas de informação da UE, nomeadamente [o Sistema de Entrada/Saída (SES)], o Sistema de Informação sobre Vistos (VIS), [o Sistema Europeu de Informação e Autorização de Viagem (ETIAS)], o Eurodac, o Sistema de Informação Schengen (SIS) e [o Sistema Europeu de Informação sobre Registos Criminais de nacionais de países terceiros (ECRIS-TCN)] para que estes sistemas de informação da UE e os respetivos dados se complementem mutuamente. Para concretizar este objetivo, é necessário criar um portal europeu de pesquisa, um serviço partilhado de correspondências biométricas (BMS), um repositório comum de dados de identificação (CIR) e um detetor de identidades múltiplas (MID) que serão os componentes de interoperabilidade.

(10) A interoperabilidade entre os sistemas de informação da UE deverá permitir aos referidos sistemas complementarem-se mutuamente a fim de facilitar a correta identificação de pessoas, contribuir para combater a fraude de identidade, melhorar e harmonizar os requisitos de qualidade dos dados dos respetivos sistemas de informação da UE, facilitar a aplicação, por parte dos Estados-Membros, dos aspetos técnicos e operacionais dos sistemas de informação da UE existentes e futuros, reforçar e simplificar as salvaguardas em matéria de segurança e proteção de dados que regem os respetivos sistemas de informação da UE, simplificar o acesso para fins de aplicação da lei ao SES, ao VIS, ao [ETIAS] e ao Eurodac, e apoiar os objetivos do SES, do VIS, do [ETIAS], do Eurodac, do SIS e do [sistema ECRIS-TCN].

(11) Os componentes de interoperabilidade devem abranger o SES, o VIS, o [ETIAS], o Eurodac, o SIS e o [sistema ECRIS-TCN]. Devem igualmente abranger os dados da Europol na medida em que possam ser consultados em simultâneo com estes sistemas de informação da UE.

(12) Os componentes de interoperabilidade devem dizer respeito a pessoas cujos dados pessoais possam ser tratados nos sistemas de informação da UE e pela Europol, designadamente os nacionais de países terceiros cujos dados pessoais sejam tratados nos sistemas de informação da UE e pela Europol, e aos cidadãos da UE cujos dados pessoais sejam tratados no SIS e pela Europol.

(13) O portal europeu de pesquisa (ESP) deve ser criado para facilitar, tecnicamente, a capacidade de as autoridades dos Estados-Membros e de os organismos da UE acederem de forma rápida, contínua, eficiente, sistemática e controlada aos sistemas de informação da UE, aos dados da Europol, bem como às bases de dados da Interpol, necessários ao desempenho das suas funções, em conformidade com os respetivos direitos de acesso, e a fim de apoiar os objetivos do SES, do VIS, do [ETIAS], do Eurodac, do SIS, do [sistema ECRIS-TCN] e dos dados da Europol. Ao permitir consultar simultaneamente todos os sistemas de informação da UE pertinentes em paralelo, bem como os dados da Europol e as bases de dados da Interpol, o ESP funcionará como um «balcão único» ou um «intermediário de mensagens» para pesquisar diferentes sistemas centrais e obter as informações necessárias de forma contínua, e respeitando plenamente os requisitos de controlo de acessos e de proteção de dados dos sistemas subjacentes.

(14) A base de dados relativa a Documentos de Viagem Roubados e Extraviados (SLTD) da Organização Internacional de Polícia Criminal (Interpol) permite às entidades autorizadas responsáveis pela aplicação da lei nos Estados-Membros, incluindo os

agentes de imigração e de controlo das fronteiras, determinarem a validade de um documento de viagem. O [ETIAS] consulta a base de dados SLTD e a base de dados de Documentos de Viagem Associados a Notificações (TDAWN) da Interpol, no contexto de avaliar se uma pessoa que solicita uma autorização de viagem é suscetível, por exemplo, de migrar de forma irregular ou pode constituir uma ameaça para a segurança. O portal europeu de pesquisa (ESP) centralizado deverá permitir a consulta das bases de dados SLTD e TDAWN utilizando os dados de identificação de um indivíduo. Sempre que sejam transferidos dados pessoais da União para a Interpol através do ESP, aplicam-se as disposições relativas às transferências internacionais constantes do capítulo V do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho[53], ou as disposições nacionais de transposição do capítulo V da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho[54]. Não deverá prejudicar as regras específicas previstas na Posição Comum 2005/69/JAI[55] do Conselho e na Decisão 2007/533/JAI do Conselho[56].

(15) O portal europeu de pesquisa (ESP) deve ser desenvolvido e configurado de modo que, na consulta, não seja possível utilizar campos de dados que não estejam relacionados com pessoas ou documentos de viagem, ou que não estejam presentes num sistema de informação da UE, nos dados da Europol ou na base de dados da Interpol.

(16) A fim de assegurar uma utilização rápida e sistemática de todos os sistemas de informação da UE, o portal europeu de pesquisa (ESP) deve ser utilizado para consultar o repositório comum de dados de identificação, o SES, o VIS, [o ETIAS], o Eurodac e [o sistema ECRIS-TCN]. No entanto, deve manter-se a ligação nacional aos diferentes sistemas de informação da UE a fim de proporcionar uma alternativa técnica. O ESP deve ser igualmente utilizado pelos organismos da União para consultar o SIS Central, em conformidade com os respetivos direitos de acesso e para o desempenho das suas funções. O ESP deve constituir um meio suplementar de consulta do SIS Central, dos dados da Europol e dos sistemas da Interpol, complementando as interfaces específicas existentes.

(17) Os dados biométricos, como as impressões digitais e as imagens faciais, são únicos e, por conseguinte, muito mais fiáveis do que os dados alfanuméricos de identificação de uma pessoa. O serviço partilhado de correspondências biométricas (BMS) deve ser um instrumento técnico para reforçar e facilitar o trabalho dos sistemas de informação da UE pertinentes e de outros componentes de interoperabilidade. O principal objetivo do BMS deve ser facilitar a identificação de uma pessoa que possa estar registada em bases de dados diferentes, procurando correspondências com os seus dados

---

[53] 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 (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

[54] Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho (JO L 119 de 4.5.2016, p. 89).

[55] Posição Comum 2005/69/JAI do Conselho, de 24 de janeiro de 2005, relativa ao intercâmbio de certos dados com a Interpol (JO L 27 de 29.1.2005, p. 61).

[56] Decisão 2007/533/JAI do Conselho, de 12 de junho de 2007, relativa ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação Schengen de segunda geração (SIS II) (JO L 205 de 7.8.2007, p. 63).

biométricos nos diferentes sistemas e baseando-se num único componente tecnológico em vez de em cinco diferentes, em cada um dos sistemas subjacentes. O BMS trará vantagens em termos de segurança, bem como em termos financeiros, de manutenção e operacionais na medida em que assentará num único componente tecnológico, em vez de vários componentes diferentes em cada um dos sistemas subjacentes. Todos os sistemas automáticos de identificação dactiloscópica, incluindo os que são presentemente utilizados no Eurodac, no VIS e no SIS, utilizam modelos biométricos constituídos por dados provenientes de uma extração de características de amostras biométricas reais. O BMS deve reunir e armazenar todos estes modelos biométricos num único local, facilitando as comparações entre sistemas, mediante utilização de dados biométricos, e permitindo economias de escala no desenvolvimento e manutenção de sistemas centrais da UE.

(18) Os dados biométricos constituem dados pessoais sensíveis. O presente regulamento deve estabelecer a base e as garantias do tratamento desses dados com a finalidade de identificar em exclusivo as pessoas em causa.

(19) Os sistemas criados pelo Regulamento (UE) 2017/2226 do Parlamento Europeu e do Conselho[57], pelo Regulamento (CE) n.º 767/2008 do Parlamento Europeu e do Conselho[58], pelo [Regulamento ETIAS] para a gestão das fronteiras da União, o sistema criado pelo [Regulamento Eurodac] para identificar os requerentes de proteção internacional e combater a migração irregular, e o sistema criado pelo [Regulamento do sistema ECRIS-TCN] necessitam, para serem eficazes, apoiar-se na correta identificação dos nacionais de países terceiros cujos dados pessoais estão armazenados nestes sistemas.

(20) O repositório comum de dados de identificação (CIR) deve, por conseguinte, facilitar e apoiar a identificação correta das pessoas registadas no SES, no VIS, [no ETIAS], no Eurodac e [no sistema ECRIS-TCN].

(21) Os dados pessoais armazenados nestes sistemas de informação da UE podem dizer respeito às mesmas pessoas, mas sob identidades diferentes ou incompletas. Os Estados-Membros dispõem de meios eficazes para identificar os seus cidadãos ou residentes permanentes registados no seu território, mas o mesmo não acontece com os nacionais de países terceiros. A interoperabilidade entre os sistemas de informação da UE deve contribuir para a correta identificação dos nacionais de países terceiros. O repositório comum de dados de identificação (CIR) deve armazenar os dados pessoais relativos a nacionais de países terceiros presentes nos sistemas, dados esses que são necessários para permitir uma identificação mais exata desses indivíduos, incluindo, portanto, a sua identidade, documentos de viagem e dados biométricos, independentemente do sistema nos quais os dados foram originalmente recolhidos. No CIR apenas deverão ser armazenados os dados pessoais estritamente necessários à realização de um rigoroso controlo de identidade. Os dados pessoais registados no CIR

[57] Regulamento (UE) 2017/2226 do Parlamento Europeu e do Conselho, de 30 de novembro de 2017, que estabelece o Sistema de Entrada/Saída (SES) para registo dos dados das entradas e saídas e dos dados das recusas de entrada dos nacionais de países terceiros aquando da passagem das fronteiras externas dos Estados-Membros da União Europeia e que determina as condições de acesso ao SES para efeitos de aplicação da lei, e altera a Convenção que implementa o Acordo de Schengen e os Regulamentos (CE) n.º 767/2008 e (UE) n.º 1077/2011 (Regulamento SES) (JO L 327 de 9.12.2017, p. 20–82).

[58] Regulamento (CE) n.º 767/2008 do Parlamento Europeu e do Conselho, de 9 de julho de 2008, relativo ao Sistema de Informação sobre Vistos (VIS) e ao intercâmbio de dados entre os Estados-Membros sobre os vistos de curta duração (Regulamento VIS) (JO L 218 de 13.8.2008, p. 60).

não devem ser conservados por mais tempo do que o estritamente necessário para efeitos dos sistemas subjacentes e devem ser automaticamente eliminados quando os dados forem eliminados nos respetivos sistemas, de acordo com a sua separação lógica.

(22) A nova operação de tratamento que consiste no armazenamento desses dados no repositório comum de dados de identificação (CIR) em vez do armazenamento em cada um dos diferentes sistemas, é necessária para aumentar o rigor da identificação, que é possível graças à comparação e correspondência automatizadas desses dados. O facto de os dados de identificação e biométricos de nacionais de países terceiros serem armazenados no CIR não deve levantar qualquer obstáculo ao tratamento de dados para efeitos dos Regulamentos SES, VIS, ETIAS, Eurodac ou sistema ECRIS-TCN, na medida em que o CIR será um novo componente partilhado desses sistemas subjacentes.

(23) A este respeito, é necessário criar um processo individual no repositório comum de dados de identificação (CIR) para cada pessoa registada no SES, no VIS, no ETIAS, no Eurodac ou no sistema ECRIS-TCN, para atingir o objetivo da correta identificação dos nacionais de países terceiros no espaço Schengen, e apoiar o detetor de identidades múltiplas com o duplo objetivo de facilitar os controlos de identidade de viajantes de boa-fé e combater a fraude de identidade. O processo individual deve ser armazenado num único local e os utilizadores finais devidamente autorizados deverão ter acesso a todas as possíveis identidades ligadas a uma pessoa.

(24) O repositório comum de dados de identificação (CIR) deve, por isso, apoiar o funcionamento do detetor de identidades múltiplas e facilitar e simplificar o acesso das autoridades de aplicação da lei aos sistemas de informação da UE que não foram estabelecidos exclusivamente para efeitos de prevenção, investigação, deteção ou repressão de crimes graves.

(25) O repositório comum de dados de identificação (CIR) deve prever um recipiente partilhado para dados de identificação e biométricos dos nacionais de países terceiros registados no SES, no VIS, [no ETIAS], no Eurodac e [no sistema ECRIS-TCN], funcionando como o elemento partilhado entre esses sistemas para o armazenamento destes dados, e para permitir a sua consulta.

(26) Todos os registos no repositório comum de dados de identificação (CIR) devem ser separados por uma ordem lógica mediante a identificação automática de cada um deles com o sistema subjacente ao qual pertencem. O controlo de acessos do CIR deve utilizar essas identificações para determinar a disponibilidade do acesso aos mesmos.

(27) A fim de assegurar a correta identificação de uma pessoa, as autoridades dos Estados-Membros competentes para prevenir e combater a migração irregular e as autoridades competentes na aceção do artigo 3.º, n.º 7, da Diretiva 2016/680, devem ser autorizadas a consultar o repositório comum de dados de identificação (CIR) com os dados biométricos dessa pessoa obtidos durante um controlo de identidade.

(28) Sempre que não seja possível utilizar os dados biométricos da pessoa, ou se a consulta com esses dados falhar, a consulta deve ser efetuada com os dados de identificação dessa pessoa combinados com os dados dos documentos de viagem. Se a consulta indicar que os dados relativos a essa pessoa se encontram armazenados no repositório

comum de dados de identificação (CIR), as autoridades dos Estados-Membros devem ter acesso ao sistema para consultar os dados de identificação dessa pessoa armazenados no CIR, sem fornecer nenhuma indicação quanto ao sistema de informação da UE ao qual os dados pertencem.

(29) Os Estados-Membros devem adotar medidas legislativas nacionais, no sentido de designar as autoridades competentes para efetuar controlos de identidade recorrendo à utilização do repositório comum de dados de identificação (CIR) e estabelecer os procedimentos, condições e critérios de realização desses controlos em conformidade com o princípio da proporcionalidade. Em especial, o poder para recolher dados biométricos durante um controlo de identidade de uma pessoa presente perante o membro dessas autoridades, deve ser objeto de disposições legislativas nacionais.

(30) O presente regulamento deve também introduzir uma nova possibilidade de simplificação do acesso a dados, para além dos dados de identificação existentes no SES, no VIS, [no ETIAS] ou no Eurodac, por parte das autoridades responsáveis pela aplicação da lei dos Estados-Membros e da Europol. Os dados, incluindo outros dados além dos dados de identificação, presentes nesses sistemas, podem ser necessários para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas ou infrações penais graves num caso específico.

(31) O pleno acesso aos dados contidos nos sistemas de informação da UE, necessários para fins de prevenção, deteção e investigação de infrações terroristas ou outras infrações penais graves, para além dos dados de identificação pertinentes cobertos pelo repositório comum de dados de identificação (CIR), obtidos usando dados biométricos dessa pessoa que foram recolhidos durante um controlo de identidade, deve continuar a ser regido pelas disposições nos respetivos instrumentos jurídicos. As autoridades designadas responsáveis pela aplicação da lei e a Europol não sabem de antemão quais são os sistemas de informação da UE que contêm dados das pessoas que necessitam de investigar. Esta situação gera atrasos e ineficiências no exercício das suas funções. O utilizador final autorizado pela autoridade designada deve, por conseguinte, receber permissão para ver qual é o sistema de informação da UE onde estão registados os dados correspondentes à consulta introduzida. O sistema em causa seria, assim, assinalado na sequência da verificação automática da presença de uma resposta positiva no sistema (a chamada funcionalidade de indicadores de respostas positivas).

(32) Os registos das consultas do repositório comum de dados de identificação devem indicar a finalidade da consulta. Nos casos em que a consulta foi efetuada utilizando a abordagem em duas fases à consulta de dados, os registos devem incluir uma referência ao processo nacional da investigação ou do caso, indicando, portanto, que a consulta foi iniciada para fins de prevenção, deteção e investigação de infrações terroristas ou outras infrações penais graves.

(33) A consulta do repositório comum de dados de identificação (CIR) por autoridades designadas dos Estados-Membros e pela Europol a fim de obter uma resposta com indicador de resposta positiva referindo que os dados estão registados no SES, no VIS, [no ETIAS] ou no Eurodac, exige o tratamento automatizado dos dados pessoais. Um indicador de resposta positiva não deve revelar dados pessoais da pessoa em causa, dando apenas a indicação de que alguns dos dados estão armazenados num dos sistemas. O utilizador final autorizado nunca poderá tomar uma decisão desfavorável para a pessoa em causa apenas com base na ocorrência de um indicador de resposta

positiva. Por conseguinte, o acesso do utilizador final a um indicador de resposta positiva terá uma interferência muito limitada no direito à proteção de dados pessoais da pessoa em causa, sendo necessário autorizar a autoridade designada e a Europol a dirigirem o seu pedido de acesso aos dados pessoais de forma mais eficaz diretamente ao sistema que foi assinalado como contendo os dados.

(34) A abordagem em duas fases à consulta de dados é particularmente útil nos casos em que se desconhece quem é o suspeito, o autor ou presumível vítima de uma infração terrorista ou outra infração penal grave. Com efeito, nesses casos, o repositório comum de dados de identificação (CIR) deverá permitir identificar o sistema de informação que conhece a pessoa, numa única pesquisa. Ao criar a obrigação de utilizar esta nova abordagem de acesso para efeitos de aplicação da lei em casos como estes, o acesso aos dados pessoais armazenados no SES, no VIS, [no ETIAS] e no Eurodac deve decorrer sem os requisitos de uma pesquisa prévia nas bases de dados nacionais e o lançamento de uma pesquisa prévia no sistema automático de identificação dactiloscópica de outros Estados-Membros ao abrigo da Decisão 2008/615/JAI. De facto, o princípio da pesquisa prévia limita a possibilidade de as autoridades dos Estados-Membros consultarem os sistemas para efeitos de aplicação da lei e pode, por conseguinte, resultar na perda de oportunidades para revelar informações necessárias. Os requisitos de uma pesquisa prévia nas bases de dados nacionais e o lançamento de uma pesquisa prévia no sistema automático de identificação dactiloscópica de outros Estados-Membros ao abrigo da Decisão 2008/615/JAI só deixarão de se aplicar depois de ficar operacional a salvaguarda alternativa da abordagem em duas fases ao acesso para fins de aplicação da lei através do CIR.

(35) O detetor de identidades múltiplas (MID) deve ser criado para apoiar o funcionamento do repositório comum de dados de identificação e para apoiar os objetivos do SES, do VIS, [do ETIAS], do Eurodac, do SIS e [do sistema ECRIS-TCN]. Para ser eficaz no cumprimento dos respetivos objetivos, todos estes sistemas de informação da UE exigem a identificação precisa das pessoas cujos dados pessoais estão armazenados nos mesmos.

(36) A possibilidade de alcançar os objetivos dos sistemas de informação da UE é prejudicada pela atual incapacidade de as autoridades utilizarem estes sistemas para realizar verificações suficientemente fiáveis de identidades dos nacionais de países terceiros cujos dados estão armazenados em sistemas diferentes. Essa incapacidade é determinada pelo facto de o conjunto dos dados de identificação armazenados num determinado sistema individual poderem ser fraudulentos, incorretos ou incompletos, e de que atualmente não existe qualquer possibilidade de detetar esse género de dados comparando-os com os dados armazenados noutro sistema. Para remediar esta situação, é necessário dispor de um instrumento técnico a nível da União que permita a identificação precisa dos nacionais de países terceiros para estes fins.

(37) O detetor de identidades múltiplas (MID) deve criar e armazenar ligações entre dados em diferentes sistemas de informação da UE a fim de detetar identidades múltiplas, com o duplo objetivo de facilitar os controlos de identidade de viajantes de boa-fé e combater a fraude de identidade. O MID deve conter apenas as ligações entre as pessoas presentes em mais de um sistema de informação da UE, estritamente limitado aos dados necessários para verificar se uma pessoa está registada lícita ou ilicitamente sob diferentes identidades biográficas em sistemas diferentes, ou para clarificar

situações em que duas pessoas com dados biográficos semelhantes podem não ser a mesma pessoa. O tratamento de dados através do portal europeu de pesquisa (ESP) e do serviço partilhado de correspondências biométricas (BMS) com o objetivo de estabelecer ligações entre os processos individuais e os sistemas individuais deve ser mantido num mínimo absoluto e, por conseguinte, está limitado a uma deteção de identidades múltiplas no momento em que são adicionados dados novos a um dos sistemas de informação que fazem parte do repositório comum de dados de identificação e no SIS. O MID deve incluir salvaguardas contra eventuais discriminações ou decisões desfavoráveis para pessoas com identidades múltiplas lícitas.

(38) O presente regulamento prevê novas operações de tratamento de dados que visam identificar as pessoas em causa de forma correta. Tal constitui uma interferência nos seus direitos fundamentais protegidos pelos artigos 7.º e 8.º da Carta dos Direitos Fundamentais. Uma vez que a aplicação eficaz dos sistemas de informação da UE depende da identificação correta das pessoas em causa, essa interferência é justificada pelos mesmos objetivos pelos quais cada um desses sistemas foi criado, pela gestão eficaz das fronteiras da União, pela segurança interna da União, pela aplicação eficaz das políticas de asilo e de vistos da União e pela luta contra a migração irregular.

(39) Sempre que uma autoridade nacional ou um organismo da UE cria novos registos, o portal europeu de pesquisa (ESP) e o serviço partilhado de correspondências biométricas (BMS) devem comparar os dados referentes a pessoas existentes no repositório comum de dados de identificação (CIR) e no SIS. Esta comparação deve ser automatizada. O CIR e o SIS devem utilizar o BMS para detetar eventuais ligações com base em dados biométricos. O CIR e o SIS devem utilizar o ESP para detetar eventuais ligações com base em dados alfanuméricos. O CIR e o SIS devem ser capazes de identificar dados idênticos ou dados semelhantes sobre os nacionais de países terceiros armazenados em vários sistemas. Sempre que se aplique, deve criar-se uma ligação indicando que se trata da mesma pessoa. O CIR e o SIS devem ser configurados de forma a que os pequenos erros de transliteração ou ortográficos detetados não criem qualquer obstáculo injustificado ao nacional de país terceiro em causa.

(40) A autoridade nacional ou organismo da UE que registou os dados no respetivo sistema de informação da UE deve confirmar ou alterar estas ligações. Esta autoridade deve ter acesso aos dados armazenados no repositório comum de dados de identificação (CIR) ou no SIS e no detetor de identidades múltiplas (MID) para efeitos da verificação manual da identidade.

(41) O acesso ao detetor de identidades múltiplas (MID) pelas autoridades dos Estados-Membros e organismos da UE que têm acesso a, pelo menos, um sistema de informação da UE incluído no repositório comum de dados de identificação (CIR) ou no SIS, deve limitar-se às chamadas ligações vermelhas onde os dados ligados partilham a mesma biometria, mas dados de identificação diferentes, tendo a autoridade responsável pela verificação das diferentes identidades concluído que se referem ilegalmente à mesma pessoa, ou onde os dados ligados possuem dados de identificação semelhantes e a autoridade responsável pela verificação das diferentes identidades concluiu que se referem ilegalmente à mesma pessoa. Quando os dados de identificação ligados não são semelhantes, deve criar-se uma ligação amarela e

efetuar-se uma verificação manual a fim de confirmar a ligação ou para mudar a sua cor em conformidade.

(42) A verificação manual de identidades múltiplas deve ser assegurada pela autoridade que cria ou atualiza os dados que desencadearam uma resposta positiva, resultando numa ligação com dados já armazenados noutro sistema de informação da UE. A autoridade responsável pela verificação de identidades múltiplas deve analisá-las para determinar se são legais ou ilegais. Essa análise deve ser efetuada, sempre que possível, na presença do nacional de país terceiro e, quando necessário, solicitando esclarecimentos ou informações adicionais. Essa análise deve ser efetuada sem demora, em conformidade com as obrigações legais quanto à exatidão das informações ao abrigo do direito da União e nacional.

(43) Para as ligações obtidas relativamente ao Sistema de Informação Schengen (SIS), relacionadas com as indicações sobre pessoas procuradas para efeitos de detenção, entrega ou extradição, sobre pessoas desaparecidas ou vulneráveis, sobre pessoas procuradas no âmbito de um processo judicial, sobre pessoas para efeitos de vigilância discreta ou controlos específicos, ou sobre pessoas desconhecidas procuradas, a autoridade responsável pela verificação de identidades múltiplas deve ser o gabinete SIRENE do Estado-Membro que criou a indicação. Com efeito essas categorias de indicações do SIS são sensíveis e não devem ser necessariamente partilhadas com as autoridades que criam ou atualizam os dados num dos outros sistemas de informação da UE. A criação de uma ligação com os dados do SIS não deverá prejudicar as medidas a adotar em conformidade com os [Regulamentos SIS].

(44) A eu-LISA deve criar mecanismos automatizados de controlo de qualidade de dados e indicadores comuns da qualidade dos dados. A eu-LISA deve ser responsável por desenvolver uma capacidade central de monitorização da qualidade dos dados, bem como elaborar periodicamente relatórios de análise de dados para melhorar o controlo da aplicação e execução dos sistemas de informação da UE por parte dos Estados-Membros. Os indicadores comuns de qualidade devem incluir as normas mínimas de qualidade para armazenar dados nos sistemas de informação da UE ou nos componentes de interoperabilidade. O objetivo destas normas de qualidade para os dados é permitir que os sistemas de informação da UE e os componentes de interoperabilidade identifiquem automaticamente dados aparentemente incorretos ou incoerentes, de modo que o Estado-Membro de origem possa verificar os dados e tomar as medidas necessárias para corrigir os erros.

(45) A Comissão deve avaliar os relatórios de qualidade da eu-LISA e deve emitir recomendações para os Estados-Membros, se for caso disso. Os Estados-Membros devem ser responsáveis por elaborar um plano de ação que descreva as ações para corrigir eventuais deficiências na qualidade dos dados e devem apresentar regularmente um relatório sobre os progressos registados.

(46) O Formato de Mensagem Universal (UMF) deve definir uma norma para o intercâmbio estruturado de informações transfronteiras entre os sistemas de informação, autoridades e/ou organizações no domínio da Justiça e Assuntos Internos. O UMF deve definir um vocabulário comum e estruturas lógicas para informações habitualmente trocadas com o objetivo de facilitar a interoperabilidade, permitindo a criação e a leitura do conteúdo da troca de forma coerente e semanticamente equivalente.

(47) Deverá criar-se um repositório central para a elaboração de relatórios e estatísticas (CRRS) a fim de gerar dados estatísticos entre sistemas e relatórios analíticos para efeitos políticos, operacionais e de qualidade dos dados. A eu-LISA deve criar, aplicar e alojar o CRRS nos seus sítios técnicos contendo dados estatísticos anónimos dos sistemas acima mencionados, do repositório comum de dados de identificação, do detetor de identidades múltiplas e do serviço partilhado de correspondências biométricas. Os dados contidos no CRRS não devem permitir identificar pessoas. A eu-LISA deve tornar os dados anónimos e deve registar esses mesmos dados anónimos no CRRS. O processo de tornar os dados anónimos deve ser automatizado e o pessoal da eu-LISA não terá acesso direto aos dados pessoais armazenados nos sistemas de informação da UE ou nos componentes de interoperabilidade.

(48) O Regulamento (UE) 2016/679 deve aplicar-se ao tratamento de dados pessoais ao abrigo do presente regulamento, pelas autoridades nacionais, salvo se tal tratamento for efetuado pelas autoridades designadas ou pontos de acesso centrais dos Estados-Membros para fins de prevenção, deteção ou investigação de infrações terroristas ou de outras infrações penais graves, e neste caso aplica-se a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho.

(49) As disposições específicas sobre proteção de dados do [Regulamento SES], do Regulamento (CE) n.º 767/2008, [do Regulamento ETIAS] e [do Regulamento relativo ao SIS no domínio dos controlos das fronteiras], devem aplicar-se ao tratamento de dados pessoais nesses sistemas respetivos.

(50) O Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho[59] deve aplicar-se ao tratamento de dados pessoais pela eu-LISA e outras instituições e órgãos da União na execução das suas responsabilidades ao abrigo do presente regulamento, sem prejuízo do Regulamento (UE) 2016/794, que deve aplicar-se ao tratamento de dados pessoais pela Europol.

(51) As autoridades nacionais de controlo criadas em conformidade com o [Regulamento (UE) 2016/679] devem controlar a legalidade do tratamento dos dados pessoais pelos Estados-Membros, enquanto a Autoridade Europeia para a Proteção de Dados, criada pelo Regulamento (CE) n.º 45/2001, deve controlar as atividades das instituições e dos órgãos da União relacionadas com o tratamento de dados pessoais. A Autoridade Europeia para a Proteção de Dados e as autoridades de controlo deverão cooperar entre si no âmbito do controlo do tratamento dos dados pessoais pelos componentes de interoperabilidade.

(52) «(...) A Autoridade Europeia para a Proteção de Dados foi consultada nos termos do artigo 28.º, n.º 2, do Regulamento (CE) n.º 45/2001 e emitiu parecer em …»

(53) No que respeita à confidencialidade, as disposições pertinentes do Estatuto dos Funcionários da União Europeia e do Regime Aplicável aos Outros Agentes da União são aplicáveis aos funcionários ou outros agentes empregados e a trabalhar em ligação com o SIS.

[59] Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados (JO L 8 de 12.1.2001, p. 1).

(54) Os Estados-Membros e a eu-LISA devem manter planos de segurança para facilitar a aplicação das obrigações de segurança e deverão cooperar entre si para tratar de questões de segurança. A eu-LISA deve igualmente assegurar a utilização contínua das mais recentes evoluções tecnológicas necessárias para garantir a integridade dos dados relativamente ao desenvolvimento, conceção e gestão dos componentes de interoperabilidade.

(55) A aplicação dos componentes de interoperabilidade prevista no presente regulamento irá ter um impacto na forma como os controlos são efetuados nos pontos de passagem de fronteira. Estes impactos resultarão de uma aplicação combinada das regras existentes do Regulamento (UE) 2016/399 do Parlamento Europeu e do Conselho[60] e das regras em matéria de interoperabilidade previstas no presente regulamento.

(56) Como consequência desta aplicação combinada das regras, o portal europeu de pesquisa (ESP) deverá constituir o principal ponto de acesso para a consulta sistemática obrigatória de bases de dados relativamente a nacionais de países terceiros nos pontos de passagem de fronteiras previstos pelo Código das Fronteiras Schengen. Além disso, para determinar se a pessoa reúne as condições de entrada estabelecidas no Código das Fronteiras Schengen, os guardas de fronteira deverão ter em consideração os dados de identificação que fizeram com que uma ligação no detetor de identidades múltiplas (MID) fosse classificada como ligação vermelha. Todavia, a presença de uma ligação vermelha não deve constituir, por si só, um motivo de recusa de entrada e os atuais motivos de recusa da entrada constantes no Código das Fronteiras Schengen não devem, por conseguinte, ser alterados.

(57) Seria oportuno atualizar o Manual prático para os guardas de fronteira para tornar estes esclarecimentos explícitos.

(58) No entanto, a fim de não prolongar o tempo de espera nos controlos de primeira linha, será necessário introduzir uma alteração no Regulamento (UE) 2016/399, nomeadamente, acrescentar a obrigação de o guarda de fronteira encaminhar os nacionais de países terceiros para o controlo de segunda linha no caso de a consulta do detetor de identidades múltiplas (MID) através do portal europeu de pesquisa (ESP) indicar a existência de uma ligação amarela ou de uma ligação vermelha.

(59) Se a consulta do detetor de identidades múltiplas (MID) através do portal europeu de pesquisa (ESP) se traduzir numa ligação amarela ou detetar uma ligação vermelha, o guarda de fronteira na segunda linha deve consultar o repositório comum de dados de identificação ou o Sistema de Informação Schengen, ou ambos, para avaliar as informações sobre a pessoa controlada, para verificar manualmente a identidade diferente e para adaptar a cor da ligação, caso se aplique.

(60) Para efeitos de estatísticas e para a elaboração de relatórios, o pessoal autorizado das autoridades, instituições e organismos competentes identificados no presente regulamento necessitará de autorização de acesso para poder consultar determinados dados relacionados com determinados componentes de interoperabilidade, sem permitir identificar as pessoas.

[60] Regulamento (UE) 2016/399 do Parlamento Europeu e do Conselho, de 9 de março de 2016, que estabelece o código da União relativo ao regime de passagem de pessoas nas fronteiras, JO L 77 de 23.3.2016, p. 1.

(61) Para as autoridades competentes e os órgãos da UE se adaptarem aos novos requisitos de utilização do portal europeu de pesquisa (ESP), é necessário prever um período de transição. De igual modo, a fim de permitir o funcionamento coerente e ótimo do detetor de identidades múltiplas (MID), deverão ser estabelecidas medidas transitórias para a sua entrada em funcionamento.

(62) Os custos de desenvolvimento dos componentes de interoperabilidade projetados ao abrigo do atual Quadro Financeiro Plurianual são inferiores ao montante remanescente no orçamento reservado às fronteiras inteligentes no Regulamento (UE) n.º 515/2014 do Parlamento Europeu e do Conselho[61]. Por conseguinte, o presente regulamento, em conformidade com o artigo 5.º, n.º 5, alínea b), do Regulamento (UE) n.º 515/2014, deve reafetar o montante atualmente atribuído para o desenvolvimento de sistemas informáticos de apoio à gestão dos fluxos migratórios nas fronteiras externas.

(63) A fim de complementar determinados aspetos técnicos pormenorizados do presente regulamento, o poder de adotar atos em conformidade com o artigo 290.º do Tratado sobre o Funcionamento da União Europeia deve ser delegado à Comissão no que se refere aos perfis dos utilizadores do portal europeu de pesquisa (ESP) e ao conteúdo e formato das respostas do ESP. É particularmente importante que a Comissão proceda às consultas adequadas durante os trabalhos preparatórios, incluindo peritos, e que essas consultas sejam realizadas em conformidade com os princípios estabelecidos no Acordo Interinstitucional «Legislar Melhor» de 13 de abril de 2016[62]. Em especial, a fim de assegurar a igualdade de participação na preparação dos atos delegados, o Parlamento Europeu e o Conselho devem receber todos os documentos ao mesmo tempo do que os peritos dos Estados-Membros, e os seus peritos devem participar sistematicamente nas reuniões dos grupos de peritos da Comissão dedicadas à preparação dos atos delegados.

(64) A fim de assegurar condições uniformes para a aplicação do presente regulamento, deverão ser atribuídas à Comissão competências de execução para a adoção de regras específicas sobre: mecanismos, procedimentos e indicadores automatizados de controlo da qualidade dos dados; o desenvolvimento da norma UMF; procedimentos para determinar casos de semelhança de identidades; o funcionamento do repositório central para a elaboração de relatórios e estatísticas; e o procedimento de cooperação em caso de incidentes de segurança. Esses poderes devem ser exercidos em conformidade com o Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho[63].

(65) O Regulamento (UE) 2016/794 é aplicável a qualquer tratamento de dados da Europol para efeitos do presente regulamento.

(66) O presente regulamento aplica-se sem prejuízo da aplicação da Diretiva 2004/38/CE.

---

[61] Regulamento (UE) n.º 515/2014 do Parlamento Europeu e do Conselho, de 16 de abril de 2014, que cria, no âmbito do Fundo para a Segurança Interna, um instrumento de apoio financeiro em matéria de fronteiras externas e de vistos e que revoga a Decisão n.º 574/2007/CE (JO L 150 de 20.5.2014, p. 143).

[62] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.123.01.0001.01.ENG.

[63] Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho, de 16 de fevereiro de 2011, que estabelece as regras e os princípios gerais relativos aos mecanismos de controlo pelos Estados-Membros do exercício das competências de execução pela Comissão (JO L 55 de 28.2.2011, p. 13).

(67) O presente regulamento constitui um desenvolvimento das disposições do acervo de Schengen.

(68) Nos termos dos artigos 1.º e 2.º do Protocolo n.º 22, relativo à posição da Dinamarca, anexo ao Tratado da União Europeia e ao Tratado sobre o Funcionamento da União Europeia, a Dinamarca não participa na adoção do presente regulamento, não ficando por ele vinculada nem sujeita à sua aplicação. Uma vez que o presente regulamento se baseia no acervo de Schengen, a Dinamarca deve decidir, nos termos do artigo 4.° desse Protocolo, e no prazo de seis meses a contar da data de aprovação do presente regulamento, se procede à respetiva transposição para o seu direito interno.

(69) O presente regulamento constitui um desenvolvimento das disposições do acervo de Schengen em que o Reino Unido não participa, em conformidade com a Decisão 2000/365/CE do Conselho[64]; por conseguinte, o Reino Unido não participa na adoção do presente regulamento, não ficando por ele vinculado nem sujeito à sua aplicação.

(70) O presente regulamento constitui um desenvolvimento das disposições do acervo de Schengen em que a Irlanda não participa, em conformidade com a Decisão 2002/192/CE do Conselho[65]; por conseguinte, a Irlanda não participa na adoção do presente regulamento, não ficando por ele vinculada nem sujeita à sua aplicação.

(71) Em relação à Islândia e à Noruega, o presente regulamento constitui um desenvolvimento das disposições do acervo de Schengen, na aceção do Acordo celebrado pelo Conselho da União Europeia e a República da Islândia e o Reino da Noruega relativo à associação destes dois Estados à execução[66], à aplicação e ao desenvolvimento do acervo de Schengen, que se insere no domínio a que se referem os pontos A, B e G do artigo 1.º da Decisão 1999/437/CE do Conselho, de 17 de maio de 1999, relativa a determinadas regras de aplicação do referido acordo[67].

(72) Em relação à Suíça, o presente regulamento constitui um desenvolvimento das disposições do acervo de Schengen, na aceção do Acordo assinado pela União Europeia, a Comunidade Europeia e a Confederação Suíça relativo à associação da Confederação Suíça à execução, à aplicação e ao desenvolvimento do acervo de Schengen[68], que se insere no domínio a que se referem os pontos A, B e G do artigo 1.º da Decisão 1999/437/CE, em conjugação com o artigo 3.º da Decisão 2008/146/CE[69] do Conselho.

(73) No que diz respeito ao Liechtenstein, o presente regulamento constitui um desenvolvimento das disposições do acervo de Schengen, na aceção do Protocolo entre a União Europeia, a Comunidade Europeia, a Confederação Suíça e o Principado do Liechtenstein relativo à adesão do Principado do Liechtenstein ao Acordo entre a União Europeia, a Comunidade Europeia e a Confederação Suíça relativo à associação da Confederação Suíça à execução, à aplicação e ao desenvolvimento do acervo de

---

64 Decisão 2000/365/CE do Conselho, de 29 de maio de 2000, sobre o pedido do Reino Unido da Grã-Bretanha e da Irlanda do Norte para participar em algumas das disposições do acervo de Schengen (JO L 131 de 1.6.2000, p. 43).

65 Decisão 2002/192/CE do Conselho, de 28 de fevereiro de 2002, sobre o pedido da Irlanda para participar em algumas das disposições do acervo de Schengen (JO L 64 de 7.3.2002, p. 20).

66 JO L 176 de 10.7.1999, p. 36.

67 JO L 176 de 10.7.1999, p. 31.

68 JO L 53 de 27.2.2008, p. 52.

69 JO L 53 de 27.2.2008, p. 1.

Schengen[70] que se insere no domínio a que se referem os pontos A, B e G do artigo 1.º da Decisão 1999/437/CE, conjugado com o artigo 3.º da Decisão 2011/350/UE do Conselho[71].

(74) No que diz respeito ao Chipre, as disposições relativas ao SIS e ao VIS constituem disposições baseadas no acervo de Schengen ou de algum modo com ele relacionadas, na aceção do artigo 3.º, n.º 2, do Ato de Adesão de 2003.

(75) No que diz respeito à Bulgária e à Roménia, as disposições relativas ao SIS e ao VIS constituem disposições baseadas no acervo de Schengen ou de algum modo com ele relacionadas, na aceção do artigo 4.º, n.º 2, do Ato de Adesão de 2005, em conjugação com a Decisão 2010/365/UE[72] do Conselho e a Decisão (UE) 2017/1908[73] do Conselho.

(76) No que diz respeito à Croácia, as disposições relativas ao SIS e ao VIS constituem disposições baseadas no acervo de Schengen ou de algum modo com ele relacionadas, na aceção do artigo 4.º, n.º 2, do Ato de Adesão de 2011, em conjugação com a Decisão (UE) 2017/733[74] do Conselho.

(77) O presente regulamento respeita os direitos fundamentais e observa os princípios reconhecidos, nomeadamente, na Carta dos Direitos Fundamentais da União Europeia e será aplicado em conformidade com esses direitos e princípios.

(78) Para que o presente regulamento possa ser integrado no quadro jurídico vigente, o Regulamento (UE) 2016/399, o Regulamento (UE) 2017/2226, a Decisão 2008/633/JAI do Conselho, o Regulamento (CE) n.º 767/2008 e a Decisão 2004/512/CE do Conselho deverão ser alterados em conformidade,

---

[70] JO L 160 de 18.6.2011, p. 21.

[71] JO L 160 de 18.6.2011, p. 19.

[72] Decisão 2010/365/UE do Conselho, de 29 de junho de 2010, relativa à aplicação das disposições do acervo de Schengen respeitantes ao Sistema de Informação Schengen na República da Bulgária e na Roménia, JO L 166 de 1.7.2010, p. 17.

[73] Decisão (UE) 2017/1908 do Conselho, de 12 de outubro de 2017, relativa à aplicação das disposições do acervo de Schengen respeitantes ao Sistema de Informação sobre Vistos na República da Bulgária e na Roménia, JO L 269 de 19.10.2017, p. 39.

[74] Decisão (UE) 2017/733 do Conselho, de 25 de abril de 2017, relativa à aplicação, na República da Croácia, das disposições do acervo de Schengen referentes ao Sistema de Informação de Schengen. JO L 108 de 26.4.2017, p. 31.

ADOTARAM O PRESENTE REGULAMENTO:

CAPÍTULO I
Disposições gerais

Artigo 1.º
Objeto

1. O presente regulamento, juntamente com [o Regulamento 2018/xx relativo à interoperabilidade em matéria de cooperação policial e judiciária, asilo e migração], estabelece um quadro para assegurar a interoperabilidade entre o Sistema de Entrada/Saída (SES), o Sistema de Informação sobre Vistos (VIS), [o Sistema Europeu de Informação e Autorização de Viagem (ETIAS)], o Eurodac, o Sistema de Informação Schengen (SIS) e [o Sistema Europeu de Informação sobre os Registos Criminais de nacionais de países terceiros (ECRIS-TCN)] a fim de que os referidos sistemas e dados se complementem mutuamente.

2. O quadro inclui os seguintes componentes de interoperabilidade:

   (a) Um portal europeu de pesquisa (ESP);

   (b) Um serviço partilhado de correspondências biométricas (BMS);

   (c) Um repositório comum de dados de identificação (CIR);

   (d) Um detetor de identidades múltiplas (MID).

3. O presente regulamento também inclui disposições sobre os requisitos de qualidade dos dados, sobre um formato de mensagem universal (UMF), sobre um repositório central para a elaboração de relatórios e estatísticas (CRRS), e define as responsabilidades dos Estados-Membros e da Agência europeia para a gestão operacional de sistemas informáticos de grande escala no espaço da liberdade, segurança e justiça (eu-LISA), no que diz respeito à conceção e ao funcionamento dos componentes de interoperabilidade.

4. O presente regulamento adapta igualmente os procedimentos e condições que vão reger o acesso das autoridades responsáveis pela aplicação da lei dos Estados-Membros e da Agência da União Europeia para a Cooperação Policial (Europol) ao Sistema de Entrada/Saída (SES), ao Sistema de Informação sobre Vistos (VIS), [ao Sistema Europeu de Informação e Autorização de Viagem (ETIAS)] e ao Eurodac para fins de prevenção, deteção e investigação de infrações terroristas ou de outras infrações penais graves abrangidas pelas respetivas competências.

Artigo 2.º
Objetivos de interoperabilidade

1. Mediante a interoperabilidade, o presente regulamento tem os seguintes objetivos:

   (a) Melhorar a gestão das fronteiras externas;

(b) Contribuir para a prevenção e combate contra a migração irregular;

(c) Contribuir para um maior nível de segurança no espaço da liberdade, de segurança e de justiça da União, incluindo a manutenção da segurança e ordem públicas, e salvaguardar a segurança nos territórios dos Estados-Membros;

(d) Melhorar a aplicação da política comum de vistos; e

(e) Ajudar a analisar os pedidos de proteção internacional.

2. Os objetivos de interoperabilidade são alcançados mediante:

(a) A garantia da identificação correta das pessoas;

(b) O contributo para combater a fraude de identidade;

(c) A melhoria e harmonização dos requisitos de qualidade dos dados dos respetivos sistemas de informação da UE;

(d) A facilitação da aplicação, por parte dos Estados-Membros, dos aspetos técnicos e operacionais dos sistemas de informação da UE atuais e futuros;

(e) O reforço, a simplificação e tornando mais uniformes as condições de segurança e de proteção dos dados que regem os respetivos sistemas de informação da UE;

(f) A racionalização das condições de acesso, para efeitos de aplicação, da lei ao SES, VIS, [ETIAS] e Eurodac;

(g) O apoio aos objetivos do SES, do VIS, [do ETIAS], do Eurodac, do SIS e [do sistema ECRIS-TCN].

Artigo 3.º
Âmbito de aplicação

1. O presente regulamento aplica-se [ao Sistema de Entrada/Saída (SES)], ao Sistema de Informação sobre Vistos (SIS), [ao Sistema Europeu de Informação e Autorização de Viagem (ETIAS)] e ao Sistema de Informação Schengen (SIS).

2. O presente regulamento aplica-se às pessoas cujos dados pessoais possam ser processados nos sistemas de informação da UE referidos no n.º 1.

Artigo 4.º
Definições

Para efeitos do presente regulamento, entende-se por:

(1) «Fronteiras externas», as fronteiras externas, tal como definidas no artigo 2.º, n.º 2, do Regulamento (UE) 2016/399;

(2) «Controlos de fronteira», os controlos de fronteira tal como definidos no artigo 2.º, n.º 11, do Regulamento (UE) 2016/399;

(3) «Autoridade responsável pelas fronteiras», o guarda de fronteira encarregado, nos termos do direito nacional, de efetuar controlos de fronteira;

(4) «Autoridades de controlo», a autoridade de controlo criada nos termos do artigo 51.º, n.º 1, do Regulamento (UE) 2016/679 e a autoridade de controlo criada nos termos do artigo 41.º, n.º 1, da Diretiva (EU) 2016/680;

(5) «Verificação», o processo que consiste em comparar séries de dados com vista a estabelecer a validade de uma identidade declarada (controlo «um para um»);

(6) «Identificação», o processo que consiste em determinar a identidade de uma pessoa através da pesquisa numa base de dados e em efetuar comparações com várias séries de dados (controlo «um para muitos»);

(7) «Nacional de um país terceiro», uma pessoa que não é um cidadão da União, na aceção do artigo 20.º, n.º 1, do Tratado, ou um apátrida, ou uma pessoa cuja nacionalidade é desconhecida;

(8) «Dados alfanuméricos», os dados representados por letras, dígitos, caracteres especiais, espaços e sinais de pontuação;

(9) «Dados de identificação», os dados a que se refere o artigo 27.º, n.º 3, alíneas a) a h);

(10) «Dados dactiloscópicos», os dados relativos às impressões digitais de um indivíduo;

(11) «Imagem facial», a imagem digitalizada do rosto;

(12) «Dados biométricos», os dados dactiloscópicos e/ou a imagem facial;

(13) «Modelo biométrico», uma representação matemática obtida por extração de características a partir de dados biométricos limitada às características necessárias para efetuar identificações e verificações;

(14) «Documento de viagem», um passaporte ou documento equivalente que permita ao seu titular transpor as fronteiras externas e no qual possa ser aposto um visto;

(15) «Dados do documento de viagem», o tipo, número e país de emissão do documento de viagem, a data de termo de validade do documento de viagem e o código de três letras do país emissor do documento de viagem;

(16) «Autorização de viagem», uma autorização de viagem, tal como definida no artigo 3.º [do Regulamento ETIAS];

(17) «Visto de curta duração», o visto tal como definido no artigo 2.º, n.º 2, alínea a) do Regulamento (CE) n.º 810/2009;

(18) «Sistemas de informação da UE», os sistemas informáticos de grande escala geridos pela eu-LISA;

(19) «Dados da Europol», os dados pessoais facultados à Europol para os fins previstos no artigo 18.º, n.º 2, alínea a), do Regulamento (UE) 2016/794;

(20) «Bases de dados da Interpol», a base de dados da Interpol relativa a Documentos de Viagem Roubados e Extraviados (SLTD) e a base de dados da Interpol relativa a Documentos de Viagem Associados a Notificações (TDAWN da Interpol);

(21) «Correspondência», existência de uma correspondência estabelecida pela comparação de duas ou mais ocorrências de dados pessoais registados, ou a ser registados, num sistema de informação ou numa base de dados;

(22) «Resposta positiva», a confirmação de uma ou várias correspondências;

(23) «Autoridade policial», uma «autoridade competente», tal como definida no artigo 3.º, n.º 7, da Diretiva 2016/680;

(24) «Autoridades designadas», as autoridades designadas dos Estados-Membros a que se referem o artigo 29.º, n.º 1, do Regulamento (UE) 2017/2226, o artigo 3.º, n.º 1, da Decisão 2008/633/JAI do Conselho, [o artigo 43.º do Regulamento ETIAS] e [o artigo 6.º do Regulamento Eurodac];

(25) «Infração terrorista», a infração definida pela legislação nacional que corresponda ou seja equivalente a uma das infrações referidas na Diretiva (UE) 2017/541;

(26) «Infração penal grave», a infração que corresponda ou seja equivalente a uma das infrações referidas no artigo 2.º, n.º 2, da Decisão-Quadro 2002/584/JAI, se for punível, nos termos do direito nacional, com pena ou medida de segurança privativa de liberdade de duração máxima não inferior a três anos;

(27) «SES», o Sistema de Entrada/Saída, tal como referido no Regulamento (EU) 2017/2226;

(28) «VIS», o Sistema de Informação sobre Vistos, tal como referido no Regulamento (EU) n.º 767/2008;

(29) [«ETIAS», o Sistema Europeu de Informação e Autorização de Viagem, tal como referido no Regulamento ETIAS];

(30) «Eurodac», Eurodac, tal como referido no [Regulamento Eurodac];

(31) «SIS», o Sistema de Informação Schengen, tal como referido [no Regulamento relativo ao SIS no domínio dos controlos das fronteiras, no Regulamento relativo ao SIS no domínio da aplicação da lei e no Regulamento relativo ao SIS no domínio do regresso ilegal];

(32) [«Sistema ECRIS-TCN», o Sistema Europeu de Informação sobre Registos Criminais que possui informações sobre condenações de nacionais de países terceiros e de apátridas, tal como referido no Regulamento ECRIS-TCN];

(33) «ESP», o portal europeu de pesquisa, tal como referido no artigo 6.º;

(34) «BMS», o serviço partilhado de correspondências biométricas, tal como referido no artigo 15.º;

(35) «CIR», o repositório comum de dados de identificação, tal como referido no artigo 17.º;

(36) «MID», o detetor de identidades múltiplas, tal como referido no artigo 25.º;

(37) «CRRS», o repositório central para a elaboração de relatórios e estatísticas, tal como referido no artigo 39.º.

Artigo 5.º
Não discriminação

O tratamento de dados pessoais para efeitos do presente regulamento não deve originar discriminação de pessoas em razão do sexo, origem racial ou étnica, religião ou crença, deficiência, idade ou orientação sexual. O respeito pela dignidade e integridade humanas deve ser integralmente assegurado. Deve ser dispensada particular atenção às crianças, aos idosos e às pessoas com deficiência.

CAPÍTULO II
Portal europeu de pesquisa

Artigo 6.º
Portal europeu de pesquisa

1. É criado um portal europeu de pesquisa (ESP) para as autoridades dos Estados-Membros e os organismos da UE usufruírem de um acesso rápido, contínuo, eficiente, sistemático e controlado aos sistemas de informação da UE, aos dados da Europol e às bases de dados da Interpol, de que necessitam para o desempenho das suas funções, em conformidade com os respetivos direitos de acesso, e a fim de apoiar os objetivos do SES, do VIS, [do ETIAS], do Eurodac, do SIS, [do sistema ECRIS-TCN] e dos dados da Europol.

2. O ESP é composto por:

   (a) Uma infraestrutura central, que inclui um portal de pesquisa que permite consultar, em simultâneo, o SES, o VIS, [o ETIAS], o Eurodac, o SIS, [o sistema ECRIS-TCN], bem como os dados da Europol e as bases de dados da Interpol;

   (b) Um canal de comunicação seguro entre o ESP, os Estados-Membros e os organismos da UE que têm o direito de utilizar o ESP em conformidade com o

direito da União;

(c) Uma infraestrutura de comunicação segura entre o ESP e o SES, o VIS, [o ETIAS], o Eurodac, o SIS Central, [o sistema ECRIS-TCN], os dados da Europol e as bases de dados da Interpol, bem como entre o ESP e as infraestruturas centrais do repositório comum de dados de identificação (CIR) e o detetor de identidades múltiplas.

3. A eu-LISA deve desenvolver o ESP, ficando responsável pela sua gestão técnica.

Artigo 7.º
Utilização do portal europeu de pesquisa

1. A utilização do ESP está reservada às autoridades dos Estados-Membros e aos organismos da UE que dispõem de acesso ao SES, [ao ETIAS], ao VIS, ao SIS, ao Eurodac e [ao sistema ECRIS-TCN], ao CIR e ao detetor de identidades múltiplas, bem como aos dados da Europol e às bases de dados da Interpol, em conformidade com o direito da União ou nacional que regula o referido acesso.

2. As autoridades referidas no n.º 1 devem utilizar o ESP para pesquisar dados relativos a pessoas ou aos seus documentos de viagem nos sistemas centrais do SES, do VIS e [do ETIAS], em conformidade com os seus direitos de acesso, ao abrigo do direito da União e nacional. Devem igualmente utilizar o ESP para consultar o CIR em conformidade com os respetivos direitos de acesso nos termos do presente regulamento para os efeitos referidos nos artigos 20.º, 21.º e 22.º.

3. As autoridades dos Estados-Membros referidas no n.º 1 podem utilizar o ESP para pesquisar dados relativos a pessoas ou aos seus documentos de viagem no SIS Central referido no [Regulamento relativo ao SIS no domínio dos controlos das fronteiras e no Regulamento relativo ao SIS no domínio da aplicação da lei]. O acesso ao SIS Central através do ESP é estabelecido através do sistema nacional (N.SIS) em cada Estado-Membro, em conformidade com o [artigo 4.º, n.º 2, do Regulamento relativo ao SIS no domínio dos controlos das fronteiras e do Regulamento relativo ao SIS no domínio da aplicação da lei].

4. Os organismos da UE devem utilizar o ESP para pesquisar dados relativos a pessoas ou aos seus documentos de viagem no SIS Central.

5. As autoridades referidas no n.º 1 podem utilizar o ESP para pesquisar dados relativos a pessoas ou aos seus documentos de viagem nas bases de dados da Interpol, em conformidade com os seus direitos de acesso ao abrigo do direito da União e nacional.

Artigo 8.º
Perfis de utilizadores do portal europeu de pesquisa

1. Para utilizar o ESP, a eu-LISA deve criar um perfil para cada categoria de utilizador do ESP, em conformidade com os pormenores técnicos e os direitos de acesso referidos no n.º 2, incluindo, em conformidade com o direito da União e nacional:

(a) Os campos de dados que serão utilizados para a consulta;

(b) Os sistemas de informação da UE, os dados da Europol e as bases de dados da Interpol que serão, e podem ser, consultados e que apresentarão uma resposta ao utilizador; e

(c) Os dados fornecidos em cada resposta.

2. A Comissão deve adotar atos delegados, em conformidade com o artigo 63.º, a fim de especificar os pormenores técnicos dos perfis referidos no n.º 1 para os utilizadores do ESP referidos no artigo 7.º, n.º 1, em conformidade com os respetivos direitos de acesso.

Artigo 9.º
Consultas

1. Os utilizadores do ESP iniciam uma consulta introduzindo dados no ESP, em conformidade com o respetivo perfil de utilizador e direitos de acesso. Ao iniciar-se uma consulta, o ESP, utilizando os dados introduzidos pelo utilizador do ESP, consulta simultaneamente o SES*,* [o ETIAS], o VIS, o SIS, o Eurodac, [o sistema ECRIS-TCN] e o CIR, bem como os dados da Europol e as bases de dados da Interpol.

2. Os campos de dados utilizados para iniciar uma consulta através do ESP correspondem aos campos de dados relacionados com pessoas ou documentos de viagem que podem ser utilizados para consultar os vários sistemas de informação da UE, os dados da Europol e as bases de dados da Interpol, em conformidade com os instrumentos jurídicos que lhes são aplicáveis.

3. A eu-LISA deve desenvolver para o ESP um documento de controlo das interfaces (ICD) baseado no UMF referido no artigo 38.º.

4. O SES, [o ETIAS], o VIS, o SIS, o Eurodac, [o sistema ECRIS-TCN], o CIR e o detetor de identidades múltiplas, bem como os dados da Europol e as bases de dados da Interpol, devem fornecer os dados em sua posse, em resposta a uma consulta do ESP.

5. Durante uma consulta das bases de dados da Interpol, a conceção do ESP não permitirá que os dados utilizados pelo utilizador do ESP na sua consulta sejam partilhados com os proprietários dos dados da Interpol.

6. A resposta ao utilizador do ESP é única e contém todos os dados aos quais o utilizador tem acesso ao abrigo do direito da União. Sempre que for necessário, a resposta fornecida pelo ESP indica qual é o sistema de informação ou a base de dados a que os dados pertencem.

7. A Comissão deve adotar um ato delegado, em conformidade com o artigo 63.º, para especificar o conteúdo e o formato das respostas do ESP.

Artigo 10.º
Manutenção de registos

1. Sem prejuízo do disposto no [artigo 46.º do Regulamento SES], no artigo 34.º do Regulamento (CE) n.º 767/2008, no [artigo 59.º da proposta do ETIAS] e nos artigos 12.º e 18.º do Regulamento relativo ao SIS no domínio dos controlos das fronteiras, a eu-LISA deve conservar registos de todas as operações de tratamento de dados realizadas no ESP. Esses registos devem incluir, em especial, o seguinte:

   (a) A autoridade do Estado-Membro e o utilizador individual do ESP, incluindo o perfil de ESP utilizado, tal como referido no artigo 8.º;

   (b) A data e a hora da consulta;

   (c) Os sistemas de informação da UE e as bases de dados da Interpol consultadas;

   (d) Em conformidade com as regras nacionais ou, quando aplicável o Regulamento (UE) n.º 45/2001, a identificação da pessoa que efetuou a consulta.

2. Os registos só podem ser utilizados para controlar a proteção de dados, incluindo para verificar a admissibilidade de uma consulta e a legalidade do tratamento dos dados, e para garantir a segurança dos dados nos termos do artigo 42.º. Esses registos devem estar protegidos por medidas adequadas contra acesso não autorizado e ser apagados um ano após a sua criação, salvo se forem necessários para procedimentos de controlo que já tenham sido iniciados.

Artigo 11.º
Procedimentos alternativos em caso de impossibilidade técnica de utilizar o portal europeu de pesquisa

1. No caso de impossibilidade técnica de utilizar o ESP para consultar um ou vários sistemas de informação da UE referidos no artigo 9.º, n.º 1, ou o CIR, devido a uma falha do ESP, os utilizadores do ESP devem ser notificados pela eu-LISA.

2. No caso de impossibilidade técnica de utilizar o ESP para consultar um ou vários sistemas de informação da UE referidos no artigo 9.º, n.º 1, ou o CIR, devido a uma falha da infraestrutura nacional de um Estado-Membro, a autoridade competente do Estado-Membro deve notificar a eu-LISA e a Comissão.

3. Em ambos os casos, e até que a falha técnica seja resolvida, a obrigação referida no artigo 7.º, n.º 2 e n.º 4 não se aplica e os Estados-Membros podem aceder aos sistemas de informação referidos no artigo 9.º, n.º 1, ou ao CIR, diretamente através das respetivas interfaces nacionais uniformes ou infraestruturas de comunicação nacionais.

CAPÍTULO III
Serviço partilhado de correspondências biométricas

Artigo 12.º
Serviço partilhado de correspondências biométricas

1. É criado um serviço partilhado de correspondências biométricas (BMS) onde são armazenados modelos biométricos e que permite consultar vários sistemas de informação da UE usando dados biométricos, para efeitos de apoio do CIR, do detetor de identidades múltiplas e dos objetivos do SES, do VIS, do Eurodac, do SIS e [do sistema ECRIS-TCN].

2. O BMS é composto por:

   (a) Uma infraestrutura central, incluindo um motor de busca e o armazenamento dos dados referidos no artigo 13.º;

   (b) Uma infraestrutura de comunicação segura entre o BMS, o SIS Central e o CIR.

3. A eu-LISA deve desenvolver o BMS , ficando responsável pela sua gestão técnica.

Artigo 13.º
Dados armazenados no serviço partilhado de correspondências biométricas

1. O BMS armazena os modelos biométricos que obtém dos seguintes dados biométricos:

   (a) Os dados referidos no artigo 16.º, n.º 1, alínea d) e no artigo 17.º, n.º 1, alíneas b) e c) do Regulamento (UE) 2017/2226;

   (b) Os dados referidos no artigo 9.º, n.º 6 do Regulamento (CE) n.º 767/2008;

   (c) [Os dados referidos no artigo 20.º, n.º 2, alíneas w) e x) do Regulamento relativo ao SIS no domínio dos controlos das fronteiras;

   (d) Os dados referidos no artigo 20.º, n.º 3, alíneas w) e x) do Regulamento relativo ao SIS no domínio da aplicação da lei;

   (e) Os dados referidos no artigo 4.º, n.º 3, alíneas t) e u) do Regulamento relativo ao SIS no domínio do regresso ilegal];

   (f) [Os dados referidos no artigo 13.º, alínea a) do Regulamento Eurodac;]

   (g) [Os dados referidos no artigo 5.º, n.º 1, alínea b) e no artigo 5.º, n.º 2, do Regulamento ECRIS-TCN.]

2. O BMS inclui em cada modelo biométrico uma referência aos sistemas de informação onde estão armazenados os dados biométricos correspondentes.

3. Os modelos biométricos são introduzidos no BMS somente após um controlo automatizado da qualidade dos dados biométricos adicionados a um dos sistemas de informação. Esse controlo é efetuado pelo BMS para determinar se cumprem as normas mínimas em termos de qualidade de dados.

4. O armazenamento dos dados referido no n.º 1 deve cumprir as normas de qualidade referidas no artigo 37.º, n.º 2.

Artigo 14.º

Pesquisar dados biométricos utilizando o serviço partilhado de correspondências biométricas

Para pesquisar os dados biométricos armazenados no CIR e no SIS, o CIR e o SIS devem utilizar modelos biométricos armazenados no BMS. As consultas com dados biométricos devem ser efetuadas em conformidade com os fins previstos no presente regulamento e no Regulamento SES, no Regulamento VIS, no Regulamento Eurodac, nos [Regulamentos SIS] e [no Regulamento ECRIS-TCN].

Artigo 15.º

Conservação de dados no serviço partilhado de correspondências biométricas

Os dados referidos no artigo 13.º devem ser conservados no BMS enquanto os dados biométricos correspondentes estiverem armazenados no CIR ou no SIS.

Artigo 16.º

Manutenção de registos

1. Sem prejuízo do disposto no [artigo 46.º do Regulamento SES], no artigo 34.º do Regulamento (CE) n.º 767/2008 e nos [artigos 12.º e 18.º do Regulamento relativo ao SIS no domínio da aplicação da lei], a eu-LISA deve conservar registos de todas as operações de tratamento de dados realizadas no BMS. Esses registos devem incluir, em especial, o seguinte:

   (a) O histórico relacionado com a criação e o armazenamento de modelos biométricos;

   (b) Uma referência aos sistemas de informação da UE consultados utilizando os modelos biométricos armazenados no BMS;

   (c) A data e a hora da consulta;

   (d) O tipo de dados biométricos utilizados para iniciar a consulta;

   (e) A duração da consulta;

   (f) Os resultados da consulta e a data e hora do resultado;

   (g) Em conformidade com as regras nacionais ou, quando aplicável o Regulamento (UE) n.º 45/2001, a identificação da pessoa que efetuou a consulta.

2. Os registos só podem ser utilizados para controlar a proteção de dados, inclusivamente para verificar a admissibilidade de uma consulta e a legalidade do

tratamento dos dados, e para garantir a segurança dos dados nos termos do artigo 42.º. Esses registos devem estar protegidos por medidas adequadas contra o acesso não autorizado e ser apagados um ano após a sua criação, salvo se forem necessários para procedimentos de controlo que já tenham sido iniciados. Os registos referidos no n.º 1, alínea a), devem ser apagados assim que os dados forem apagados.

CAPÍTULO IV
Repositório comum de dados de identificação

Artigo 17.º
Repositório comum de dados de identificação

1. É criado um repositório comum de dados de identificação (CIR), que estabelece um processo individual para cada pessoa registada no SES, no VIS, [no ETIAS], no Eurodac ou [no sistema ECRIS-TCN] contendo os dados referidos no artigo 18.º, com o objetivo de facilitar e apoiar a identificação correta das pessoas registadas no SES, no VIS, [no ETIAS], no Eurodac e [no sistema ECRIS-NPT], de apoiar o funcionamento do detetor de identidades múltiplas e de facilitar e simplificar o acesso das autoridades de aplicação da lei aos sistemas de informação com finalidades não coercivas a nível da UE, sempre que tal for necessário para efeitos de prevenção, investigação, deteção ou repressão de formas graves de criminalidade.

2. O CIR é composto por:

   (a) Uma infraestrutura central que substitui os sistemas centrais, respetivamente, do SES, do VIS, [do ETIAS], do Eurodac e [do sistema ECRIS-TCN] na medida em que armazenar os dados referidos no artigo 18.º;

   (b) Um canal de comunicação seguro entre o CIR, os Estados-Membros e os organismos da UE que têm o direito de utilizar o portal europeu de pesquisa (ESP) em conformidade com o direito da União;

   (c) Uma infraestrutura de comunicação segura entre o CIR e o SES, [o ETIAS], o VIS, o Eurodac e [o sistema ECRIS-TCN], bem como com as infraestruturas centrais do ESP, do BMS e do detetor de identidades múltiplas.

3. A eu-LISA deve desenvolver o CIR, ficando responsável pela sua gestão técnica.

Artigo 18.º
Dados do repositório comum de dados de identificação

1. O CIR deve armazenar os dados a seguir indicados, separados segundo um método lógico, de acordo com o sistema de informação de onde os dados são originários:

   (a) Os dados referidos no [artigo 16.º, n.º 1), alíneas a) a d) e no artigo 17.º, n.º 1, alíneas a) a c) do Regulamento SES];

   (b) Os dados referidos no artigo 9.º, n.º 4, alíneas a) a c), n.º 5 e n.º 6 do

Regulamento (CE) n.º 767/2008;

(c) [Os dados referidos no artigo 15.º, n.º 2, alíneas a) a e) do [Regulamento Eurodac;]

(d) – (Não aplicável)

(e) – (Não aplicável)

2. Para cada série de dados a que se refere o n.º 1, o CIR deve incluir uma referência aos sistemas de informação a que os dados pertencem.

3. O armazenamento dos dados referido no n.º 1 deve cumprir as normas de qualidade referidas no artigo 37.º, n.º 2.

Artigo 19.º

Aditamento, alteração e eliminação de dados no repositório comum de dados de identificação

1. Sempre que se adicionarem, alterarem ou eliminarem dados no SES, no VIS e [no ETIAS], os dados referidos no artigo 18.º armazenados no processo individual do CIR devem ser adicionados, alterados ou eliminados, em conformidade, de uma forma automatizada.

2. Sempre que o detetor de identidades múltiplas criar uma ligação branca ou vermelha em conformidade com os artigos 32.º e 33.º entre os dados de dois ou mais dos sistemas de informação da UE que constituem o CIR, em vez de criar um processo individual novo, o CIR deve adicionar os dados novos ao processo individual dos dados ligados.

Artigo 20.º

Acesso ao repositório comum de dados de identificação para fins de identificação

1. Sempre que uma autoridade policial de um Estado-Membro tenha sido habilitada para o efeito por medidas legislativas nacionais, tal como referido no n.º 2, pode, exclusivamente para efeitos de identificação de uma pessoa, consultar o CIR usando os dados biométricos dessa pessoa que foram obtidos durante um controlo de identidade.

Sempre que a consulta indicar que os dados relativos a essa pessoa estão armazenados no CIR, a autoridade do Estado-Membro deve ter acesso para consultar os dados referidos no artigo 18.º, n.º 1.

Sempre que não seja possível utilizar os dados biométricos da pessoa, ou se a consulta com esses dados falhar, a consulta deve ser efetuada com os dados de identificação dessa pessoa combinados com os dados dos documentos de viagem ou com os dados de identificação fornecidos por essa pessoa.

2. Os Estados-Membros que pretendam usar a possibilidade prevista no presente artigo devem adotar medidas legislativas nacionais. Essas medidas legislativas devem especificar exatamente os objetivos dos controlos de identidade referidos no

artigo 2.º, n.º 1, alíneas b) e c). Devem designar as autoridades policiais competentes e estabelecer os procedimentos, as condições e os critérios desses controlos.

Artigo 21.º
Acesso ao repositório comum de dados de identificação para a deteção de identidades múltiplas

1. Sempre que uma consulta do CIR se traduzir numa ligação amarela, em conformidade com o artigo 28.º, n.º 4, a autoridade responsável pela verificação de identidades diferentes, determinada em conformidade com o artigo 29.º, deve ter acesso, unicamente para efeitos dessa verificação, aos dados de identificação armazenados no CIR, pertencentes aos vários sistemas de informação ligados a uma ligação amarela.

2. Sempre que uma consulta do CIR se traduzir numa ligação vermelha, em conformidade com o artigo 32.º, as autoridades referidas no artigo 26.º, n.º 2, devem ter acesso, unicamente para efeitos do combate à fraude de identidade, aos dados de identificação armazenados no CIR, pertencentes aos vários sistemas de informação associados a uma ligação vermelha.

Artigo 22.º
Consulta do repositório comum de dados de identificação para efeitos de aplicação da lei

1. Para fins de prevenção, deteção e investigação de infrações terroristas ou outras infrações penais graves num caso específico, e para obter informações sobre se existem dados sobre uma determinada pessoa no SES, no VIS e [no ETIAS], as autoridades designadas dos Estados-Membros e a Europol podem consultar o CIR.

2. As autoridades designadas dos Estados-Membros e a Europol não estão autorizadas a consultar dados pertencentes [ao ECRIS-TCN] quando consultarem o CIR para os fins referidos no n.º 1.

3. Sempre que, em resposta a uma consulta, o CIR indicar a presença de dados sobre essa pessoa no SES, no VIS e [no ETIAS], o CIR deve fornecer às autoridades designadas dos Estados-Membros e à Europol uma resposta sob a forma de uma referência indicando quais são os sistemas de informação que contêm os dados das correspondências a que se refere o artigo 18.º, n.º 2. O CIR deve responder de forma a não comprometer a segurança dos dados.

4. O pleno acesso aos dados contidos nos sistemas de informação da UE para efeitos de prevenção, deteção e investigação de infrações terroristas ou outras infrações penais graves continua sujeito às condições e procedimentos definidos nos respetivos instrumentos legislativos que regulam esse acesso.

Artigo 23.º
Conservação de dados no repositório comum de dados de identificação

1. Os dados referidos no artigo 18.º, n.º 1 e n.º 2 devem ser eliminados do CIR em conformidade com as disposições em matéria de conservação de dados [do Regulamento SES], do Regulamento VIS e [do Regulamento ETIAS], respetivamente.

2. O processo individual deve permanecer armazenado no CIR enquanto os dados correspondentes permanecerem armazenados em, pelo menos, um dos sistemas de informação cujos dados estão contidos no CIR. A criação de uma ligação não afeta o período de conservação de cada um dos elementos dos dados ligados.

Artigo 24.º
Manutenção de registos

1. Sem prejuízo do disposto no [artigo 46.º do Regulamento SES], no artigo 34.º do Regulamento (CE) n.º 767/2008 e no [artigo 59.º da proposta ETIAS], a eu-LISA deve conservar registos de todas as operações de tratamento de dados realizadas no CIR em conformidade com o n.º 2, o n.º 3 e o n.º 4.

2. No que respeita a qualquer acesso ao CIR ao abrigo do artigo 20.º, a eu-LISA deve conservar registos de todas as operações de tratamento de dados realizadas no CIR. Esses registos incluem, em especial, o seguinte:

   (a) A finalidade do acesso do utilizador que faz a consulta através do CIR;

   (b) A data e a hora da consulta;

   (c) O tipo de dados utilizados para iniciar a consulta;

   (d) Os resultados da consulta;

   (e) Em conformidade com as regras nacionais ou com o Regulamento (UE) 2016/794 ou, quando aplicável o Regulamento (UE) n.º 45/2001, a identificação da pessoa que efetuou a consulta.

3. No que respeita a qualquer acesso ao CIR ao abrigo do artigo 21.º, a eu-LISA deve conservar registos de todas as operações de tratamento de dados realizadas no CIR. Esses registos devem incluir, em particular, o seguinte:

   (a) A finalidade do acesso do utilizador que faz a consulta através do CIR;

   (b) A data e a hora da consulta;

   (c) Sempre que for pertinente, os dados utilizados para iniciar a consulta;

   (d) Sempre que for pertinente, os resultados da consulta;

   (e) Em conformidade com as regras nacionais ou com o Regulamento (UE) 2016/794 ou, quando aplicável o Regulamento (UE) n.º 45/2001, a identificação da pessoa que efetuou a consulta.

4. No que respeita a qualquer acesso ao CIR ao abrigo do artigo 22.º, a eu-LISA deve conservar registos de todas as operações de tratamento de dados realizadas no CIR. Esses registos devem incluir, em particular, o seguinte:

   (a) A referência do processo nacional;

   (b) A data e a hora da consulta;

(c) O tipo de dados utilizados para iniciar a consulta;

(d) Os resultados da consulta;

(e) O nome da autoridade que consulta o CIR;

(f) Em conformidade com as regras nacionais ou com o Regulamento (UE) 2016/794 ou, quando aplicável o Regulamento (UE) n.º 45/2001, a identificação do funcionário que efetuou a consulta e do funcionário que encomendou a consulta.

Os registos desse acesso devem ser verificados regularmente pela autoridade de controlo competente, estabelecida em conformidade com o artigo 51.º do Regulamento (UE) 2016/679 ou em conformidade com o artigo 41.º da Diretiva 2016/680, a intervalos não superiores a seis meses, a fim de verificar se os procedimentos e condições estabelecidos no artigo 22.º, n.º 1 a n.º 3 são cumpridos.

5. Cada Estado-Membro deve manter registos das consultas efetuadas por pessoal devidamente autorizado para utilizar o CIR nos termos dos artigos 20.º, 21.º e 22.º.

6. Os registos referidos no n.º 1 e n.º 5 só podem ser utilizados para controlar a proteção de dados, incluindo para verificar a admissibilidade de um pedido e a legalidade do tratamento dos dados, e para garantir a segurança dos dados nos termos do artigo 42.º. Esses registos devem estar protegidos por medidas adequadas contra o acesso não autorizado e ser apagados um ano após a sua criação, salvo se forem necessários para procedimentos de controlo que já tenham sido iniciados.

7. A eu-LISA deve manter os registos relacionados com o histórico dos dados armazenados no processo individual, para os efeitos definidos no n.º 6. Os registos relacionados com o histórico dos dados armazenados devem ser apagados assim que os dados forem apagados.

CAPÍTULO V
Detetor de identidades múltiplas

Artigo 25.º
Detetor de identidades múltiplas

1. É criado um detetor de identidades múltiplas (MID) que cria e armazena ligações entre os dados nos sistemas de informação da UE que fazem parte do repositório comum de dados de identificação (CIR) e do SIS e, consequentemente, deteta identidades múltiplas, com o duplo objetivo de facilitar os controlos de identidade e lutar contra a fraude de identidade, com o objetivo de apoiar o funcionamento do CIR e os objetivos do SES, do VIS, [do ETIAS], do Eurodac, do SIS e [do sistema ECRIS-TCN].

2. O MID é composto por:

(a) Uma infraestrutura central, que armazena ligações e referências aos sistemas de informação;

(b) Uma infraestrutura de comunicação segura para ligar o MID ao SIS e as infraestruturas centrais do portal europeu de pesquisa e o CIR.

3. A eu-LISA deve desenvolver o MID, ficando responsável pela sua gestão técnica.

Artigo 26.º
Acesso ao detetor de identidades múltiplas

1. Para efeitos de verificação manual da identidade a que se refere o artigo 29.º, deve ser concedido às entidades abaixo indicadas acesso aos dados referidos no artigo 34.º, armazenados no MID:

(a) Autoridades responsáveis pelas fronteiras, aquando da criação ou atualização de um processo individual, tal como previsto no artigo 14.º do [Regulamento SES];

(b) Autoridades competentes a que se refere o artigo 6.º, n.º 1 e 2 do Regulamento n.º 767/2008 ao criar ou atualizar um processo de requerimento de visto no VIS, em conformidade com o artigo 8.º do Regulamento (CE) n.º 767/2008;

(c) [A unidade central do ETIAS e as unidades nacionais do ETIAS durante a realização da avaliação referida nos artigos 20.º e 22.º do Regulamento ETIAS;]

(d) - (Não aplicável);

(e) Gabinetes SIRENE do Estado-Membro que criar uma [indicação SIS em conformidade com o Regulamento relativo ao SIS no domínio dos controlos das fronteiras];

(f) - (Não aplicável).

2. As autoridades dos Estados-Membros e os organismos da UE que tenham acesso a, pelo menos, um sistema de informação da UE incluídos no *repositório comum de dados de identificação ou ao SIS* devem ter acesso aos dados referidos no artigo 34.º, alíneas a) e alínea b) sobre quaisquer ligações vermelhas, tal como referido no artigo 32.º.

Artigo 27.º
Deteção de identidades múltiplas

1. Deve ser iniciada uma deteção de identidades múltiplas no repositório comum de dados de identificação e no SIS se:

(a) For criado um processo individual ou atualizado no [SES, em conformidade com o artigo 14.º do Regulamento SES];

(b) For criado ou atualizado um processo de pedido no VIS em conformidade com o artigo 8.º do Regulamento (CE) n.º 767/2008;

(c) [For criado ou atualizado um processo de pedido no ETIAS, em conformidade

com o artigo 17.º do Regulamento ETIAS;]

(d) - (Não aplicável);

(e) [For criada ou atualizada uma indicação sobre uma pessoa no SIS em conformidade com o capítulo V do Regulamento relativo ao SIS no domínio dos controlos das fronteiras];

(f) - (Não aplicável).

2. Se os dados contidos num sistema de informação a que se refere o n.º 1 contiverem dados biométricos, o repositório comum de dados de identificação (CIR) e o SIS Central devem utilizar o serviço partilhado de correspondências biométricas (BMS) a fim de realizar a deteção de identidades múltiplas. O BMS deve comparar os modelos biométricos obtidos a partir de quaisquer novos dados biométricos com os modelos biométricos já constantes do BMS para verificar se os dados pertencentes ao mesmo nacional de país terceiro se encontram ou não já armazenados no CIR ou no SIS Central.

3. Para além do processo a que se refere o n.º 2, o CIR e o SIS Central devem utilizar o portal europeu de pesquisa para pesquisar os dados armazenados no CIR e SIS Central utilizando os seguintes dados:

(a) Apelido; nome(s) próprio(s); data de nascimento, sexo e nacionalidade(s), como referido no artigo 16.º, n.º 1, alínea a), do [Regulamento SES];

(b) Apelido; nome(s) próprio(s); data de nascimento, sexo e nacionalidade(s), como referido no artigo 9.º, n.º 4, alínea a), do Regulamento (CE) n.º 767/2008;

(c) [Apelido; nome(s) próprio(s); apelido de nascimento; data de nascimento, local de nascimento, sexo e nacionalidade(s) a que se refere o artigo 15.º, n.º 2, do Regulamento ETIAS;]

(d) - (Não aplicável);

(e) [Apelido(s); nome(s) próprio(s); nome(s) de nascimento, nomes e pseudónimos utilizados anteriormente; data de nascimento, local de nascimento, nacionalidade (s) e sexo a que se refere o artigo 20.º, n.º 2, do Regulamento relativo ao SIS no domínio dos controlos das fronteiras;]]

(f) - (Não aplicável);

(g) - (Não aplicável);

(h) - (Não aplicável).

4. A deteção de identidades múltiplas só deve ser lançada para comparar os dados disponíveis num sistema de informação com os dados disponíveis de outros sistemas de informação.

Artigo 28.º
Resultados da deteção de identidades múltiplas

1. Nos casos em que as consultas referidas no artigo 27.º, n.º 2 e 3 não indicarem qualquer resposta positiva, o procedimento referido no artigo 27.º, n.º 1, deve continuar em conformidade com os respetivos regulamentos que os regem.

2. Se a pesquisa prevista no artigo 27.º, n.º 2 e 3 indicar uma ou várias respostas positivas, o repositório comum de dados de identificação e, se for caso disso, o SIS deve(m) criar uma ligação entre os dados utilizados para lançar a pesquisa e os dados que desencadearam a resposta positiva.

   Quando são comunicadas várias respostas positivas, deve ser criada uma ligação entre todos os dados que desencadearam a resposta positiva. Quando os dados já se encontram ligados, a ligação existente será alargada aos dados utilizados para lançar a pesquisa.

3. Se a consulta referida no artigo 27.º, n.º 2 ou 3, indicar uma ou várias respostas positivas e os dados de identificação dos ficheiros ligados forem idênticos ou semelhantes, deve ser criada uma ligação branca em conformidade com o artigo 33.º.

4. Se a consulta referida no artigo 27.º, n.º 2 ou 3 detetar uma ou várias respostas positivas e os dados de identificação dos ficheiros ligados não puderem ser considerados similares, deve ser criada uma ligação amarela em conformidade com o artigo 30.º e com o procedimento previsto no artigo 29.º.

5. A Comissão deve estabelecer em atos de execução os procedimentos para determinar os casos em que dados de identidade podem ser considerados idênticos ou similares. Esses atos de execução devem ser adotados em conformidade com o procedimento de exame a que se refere o artigo 64.º, n.º 2.

6. As ligações devem ser conservadas no processo de confirmação de identidade a que se refere o artigo 34.º.

A Comissão deve estabelecer as regras técnicas necessárias para a ligação de dados de diferentes sistemas de informação através de atos de execução. Esses atos de execução devem ser adotados em conformidade com o procedimento de exame a que se refere o artigo 64.º, n.º 2.

Artigo 29.º
Verificação manual das diferentes identidades

1. Sem prejuízo do disposto no n.º 2, a autoridade responsável pela verificação de identidades diferentes deve ser:

   (a) A autoridade responsável pelas fronteiras no que respeita a respostas positivas que ocorreram aquando da criação ou atualização de um processo individual no [SES em conformidade com o artigo 14.º do Regulamento SES];

   (b) As autoridades competentes referidas no artigo 6.º, n.º 1 e 2 do Regulamento 767/2008 para respostas positivas que ocorreram aquando da criação ou

atualização de um processo de requerimento de visto no VIS, em conformidade com o artigo 8.º do Regulamento (CE) n.º 767/2008;

(c) [A unidade central do ETIAS e as unidades nacionais do ETIAS para respostas positivas que ocorreram em conformidade com os artigos 18.º, 20.º e 22.º do Regulamento ETIAS;]

(d) - (Não aplicável);

(e) Os gabinetes SIRENE do Estado-Membro para respostas positivas que ocorreram aquando da criação de uma indicação no SIS em conformidade com o [Regulamento relativo ao SIS no domínio dos controlos das fronteiras];

(f) - (Não aplicável).

O detetor de identidades múltiplas deve indicar a autoridade responsável pela verificação de identidades diferentes no processo de verificação da identidade.

2. A autoridade responsável pela verificação de identidades diferentes no processo de confirmação de identidade é o gabinete SIRENE do Estado-Membro que criou a indicação quando é estabelecida uma ligação com os dados contidos:

(a) Numa indicação de pessoas procuradas para efeitos de detenção, entrega ou extradição, tal como referido no artigo 26.º do [Regulamento relativo ao SIS no domínio da aplicação da lei];

(b) Numa indicação sobre pessoas desaparecidas ou vulneráveis, tal como referido no artigo 32.º do [Regulamento relativo ao SIS no domínio da aplicação da lei];

(c) Numa indicação sobre pessoas procuradas no âmbito de um processo judicial, tal como referido no artigo 34.º do [Regulamento relativo ao SIS no domínio da aplicação da lei];

(d) [Numa indicação de regresso, em conformidade com o Regulamento relativo ao SIS no domínio do regresso ilegal];

(e) Numa indicação sobre pessoas para efeitos de vigilância discreta, controlo de verificação ou de controlo específico referido no artigo 36.º do [Regulamento relativo ao SIS no domínio da aplicação da lei];

(f) Numa indicação sobre pessoas procuradas desconhecidas para efeitos de identificação nos termos do direito nacional e consulta com recurso a dados biométricos como referido no artigo 40.º do [Regulamento relativo ao SIS no domínio da aplicação da lei].

3. Sem prejuízo do disposto no n.º 4, a autoridade responsável pela verificação de identidades diferentes deve ter acesso aos dados relacionados contidos no ficheiro de confirmação de identidade pertinente e aos dados de identificação ligados no repositório comum de dados de identificação e, se for caso disso, no SIS, e deve avaliar as diversas identidades e atualizar a ligação, em conformidade com os artigos 31.º, 32.º e 33.º e adicioná-la ao processo de confirmação de identidade sem demora.

4. Sempre que a autoridade responsável pela verificação de identidades diferentes no processo de confirmação de identidade for a autoridade responsável pelas fronteiras que cria ou atualiza um processo individual no SES, em conformidade com o artigo 14.º do Regulamento SES e quando é obtida uma ligação amarela, a autoridade responsável pelas fronteiras deve realizar verificações adicionais no âmbito de um controlo de segunda linha. Durante o controlo de segunda linha, as autoridades responsáveis pelas fronteiras devem ter acesso aos dados pertinentes contidos no processo de confirmação de identidade e avaliar as diferentes identidades, atualizar a ligação nos termos dos artigos 31.º a 33.º e acrescentá-la ao processo de confirmação de identidade sem demora.

5. No caso de mais de uma ligação, a autoridade responsável pela verificação das diferentes identidades deve avaliar cada ligação separadamente.

6. Quando os dados que comunicam uma resposta positiva já foram ligados, a autoridade responsável pela verificação das diferentes identidades deve ter em consideração as ligações existentes ao avaliar a criação de novas ligações.

Artigo 30.º
Ligação amarela

1. Uma ligação entre os dados de dois ou mais sistemas de informação deve ser classificada a amarelo em qualquer dos seguintes casos:

   (a) Os dados ligados partilham os mesmos dados biométricos, mas dados de identificação diferentes e não foi feita a verificação manual da identificação diferente;

   (b) Os dados ligados possuem dados de identidade diferentes e não foi feita a verificação manual de identificação diferente.

2. Quando uma ligação é classificada a amarelo, em conformidade com o disposto no n.º 1, deve aplicar-se o procedimento previsto no artigo 29.º.

Artigo 31.º
Ligação verde

1. Uma ligação entre os dados de dois ou mais sistemas de informação deve ser classificada como verde se os dados ligados não partilham os mesmos dados de identidade biométricos, mas apresentam dados de identidade similares e a autoridade responsável pela verificação de identificações diferentes concluiu que se refere a duas pessoas diferentes.

2. Quando o repositório comum de dados de identificação (CIR) ou o SIS são consultados e se existe uma ligação verde entre dois ou mais sistemas de informação que constituem o CIR ou com o SIS, o detetor de identidades múltiplas indica que os dados de identificação dos dados ligados não corresponde à mesma pessoa. O sistema de informação consultado responde indicando apenas os dados da pessoa cujos dados foram utilizados para a consulta, sem desencadear uma resposta positiva com recurso aos dados que são objeto de ligação verde.

Artigo 32.º
Ligação vermelha

1. Uma ligação entre os dados de dois ou mais sistemas de informação deve ser classificada a vermelho, em qualquer dos seguintes casos:

   (a) Os dados ligados partilham os mesmos dados biométricos mas apresentam dados de identificação diferentes e a autoridade responsável pela verificação de diferentes identidades concluiu que se refere ilegalmente à mesma pessoa;

   (b) Os dados ligados possuem dados de identidade semelhantes e a autoridade responsável pela verificação das diferentes identidades concluiu que se refere ilegalmente à mesma pessoa.

2. Quando o CIR ou o SIS são consultados e existe uma ligação vermelha entre dois ou mais sistemas de informação que constituem o CIR ou com o SIS, o detetor de identidades múltiplas responde indicando os dados referidos no artigo 34.º. O seguimento de uma ligação vermelha deve ter lugar em conformidade com a legislação da União e nacional.

3. Nos casos em que é criada uma luz vermelha de ligação entre os dados do SES, do VIS, [ETIAS], Eurodac ou [do sistema ECRIS-TCN], o processo individual, guardado no CIR deve ser atualizado em conformidade com o artigo 19.º, n.º 1.

4. Sem prejuízo das disposições relativas ao tratamento de indicações no SIS referidas nos [Regulamentos do SIS no domínio dos controlos das fronteiras e do SIS no domínio da aplicação da lei e do SIS no domínio do regresso ilegal], e sem prejuízo das restrições necessárias para proteger a segurança e a ordem pública, prevenir o crime e garantir que qualquer investigação nacional não será prejudicada, sempre que uma luz vermelha de ligação é criada a autoridade responsável pela verificação das diferentes identidades deve informar o utilizador da existência de identidades múltiplas ilegais.

5. Nos casos em que uma ligação vermelha é criada, a autoridade responsável pela verificação das diferentes identidades deve constituir uma referência para as autoridades responsáveis pelos dados relacionados.

Artigo 33.º
Ligação branca

1. Uma ligação entre os dados de dois ou mais sistemas de informação deve ser classificada a branco em qualquer dos seguintes casos:

   (a) Os dados ligados partilham os mesmos dados biométricos e os mesmos dados de identidade ou semelhantes;

   (b) Os dados ligados partilham os mesmos dados de identidade ou semelhantes e pelo menos um dos sistemas de informação não dispõe de dados biométricos da pessoa;

   (c) Os dados ligados partilham os mesmos dados biométricos, mas os dados de identidade são diferentes e a autoridade responsável pela verificação das

diferentes identidades concluiu que se referem à mesma pessoa detentora legalmente de dados de identidade diferentes.

2. Quando o CIR ou o SIS são consultados e existe uma ligação branca entre um ou mais dos sistemas de informação que constituem o CIR ou com o SIS, o detetor de identidades múltiplas indica que os dados de identificação de dados ligados correspondem à mesma pessoa. Os sistemas de informação consultados respondem indicando, se for caso disso, todos os dados ligados sobre a pessoa, desencadeando assim uma resposta positiva em relação aos dados que são objeto da ligação branca, se a autoridade que lança a consulta tem acesso aos dados ligados ao abrigo do direito da União ou do direito nacional.

3. Quando é criada uma ligação branca entre os dados do SES, do VIS, [do ETIAS], do Eurodac ou do [sistema ECRIS-TCN] o processo individual conservado no CIR deve ser atualizado em conformidade com o artigo 19.º, n.º 1.

4. Sem prejuízo das disposições relativas ao tratamento de indicações no SIS referidas nos [Regulamentos do SIS no domínio dos controlos das fronteiras e do SIS no domínio da aplicação da lei e do SIS no domínio do regresso ilegal], sempre que é criada uma ligação branca na sequência de uma verificação manual de identidades múltiplas, a autoridade responsável pela verificação das diferentes identidades deve informar sobre a existência de discrepâncias entre os seus dados pessoais entre sistemas e apresentar uma referência para as autoridades responsáveis pelos dados relacionados.

Artigo 34.º
Processo de confirmação de identidade

O processo de confirmação de identidade deve conter os seguintes dados:

(a) As ligações, incluindo a sua descrição sob a forma de cores, tal como referido nos artigos 30.º a 33.º;

(b) Uma referência aos sistemas de informação, cujos dados estão ligados;

(c) Um número de identificação único, permitindo a extração dos dados a partir dos sistemas de informação dos ficheiros ligados correspondentes;

(d) Se for caso disso, a autoridade responsável pela verificação de identidades diferentes.

Artigo 35.º
Conservação de dados no detetor de identidades múltiplas

Os processos de confirmação de identidade e respetivos dados, incluindo as ligações, devem ser armazenados no detetor de identidades múltiplas (MID) apenas enquanto os dados permanecerem armazenados em dois ou mais sistemas de informação da UE.

Artigo 36.º
Manutenção de registos

1. A eu-LISA deve conservar os registos de todas as operações de tratamento de dados efetuadas pelo MID. Esses registos devem incluir, em especial, o seguinte:

   (a) O objetivo do acesso do utilizador e o seu direito de acesso aos mesmos;

   (b) A data e a hora da consulta;

   (c) O tipo de dados utilizados para a iniciar a consulta ou consultas;

   (d) A referência aos dados associados;

   (e) O histórico do processo de confirmação de identidade;

   (f) A identificação da pessoa que efetuou a consulta.

2. Cada Estado-Membro deve conservar registos do pessoal devidamente autorizado a utilizar o MID.

3. Os registos só podem ser utilizados para controlo da proteção dos dados, incluindo a verificação da admissibilidade de um pedido e da legalidade do tratamento dos dados, bem como para garantir a sua segurança, nos termos do artigo 42.º. Os registos devem ser protegidos por medidas adequadas contra o acesso não autorizado e apagados um ano após a sua criação, exceto se forem necessários para procedimentos de controlo que já tenham tido início. Os registos relativos ao histórico do processo de confirmação de identidade devem ser apagadas logo que os dados no processo de confirmação de identidade sejam apagados.

CAPÍTULO VI
Medidas de apoio à interoperabilidade

Artigo 37.º
Qualidade dos dados

1. A eu-LISA deve criar mecanismos e procedimentos automatizados de controlo de qualidade de dados sobre os dados armazenados no SES, [ETIAS], VIS, SIS, no serviço partilhado de correspondências biométricas (BMS), no repositório comum de dados de identificação (CIR) e no detetor de identidades múltiplas (MID).

2. A eu-LISA deve estabelecer indicadores comuns de qualidade dos dados e as normas mínimas de qualidade para armazenar os dados no SES, [ETIAS], VIS, SIS, BMS, CIR e MID.

3. A eu-LISA deve apresentar aos Estados-Membros relatórios periódicos sobre os mecanismos e procedimentos automatizados de controlo de qualidade de dados e os indicadores comuns sobre a qualidade dos dados. A eu-LISA deve também

apresentar um relatório periódico à Comissão sobre os problemas encontrados e os Estados-Membros em causa.

4. As informações pormenorizadas relativas aos mecanismos e procedimentos automatizados de controlo da qualidade e indicadores comuns de qualidade dos dados e normas mínimas de qualidade para armazenar os dados no SES, [ETIAS], VIS, SIS, BMS, CIR e o MID, em particular no que se refere aos dados biométricos, devem ser estabelecidos em atos de execução. Esses atos de execução devem ser adotados em conformidade com o procedimento de exame a que se refere o artigo 64.º, n.º 2.

5. Um ano após a criação dos mecanismos e procedimentos automatizados de controlo da qualidade dos dados e indicadores comuns da qualidade dos dados e, posteriormente, todos os anos, a Comissão deve avaliar a execução por parte dos Estados-Membros da qualidade dos dados e formular as recomendações necessárias. Os Estados-Membros devem apresentar à Comissão um plano de ação destinado a corrigir as deficiências identificadas no relatório de avaliação e comunicar quaisquer progressos neste plano de ação até que seja plenamente aplicado. A Comissão deve transmitir o relatório de avaliação ao Parlamento Europeu, ao Conselho, à Autoridade Europeia para a Proteção de Dados e à Agência dos Direitos Fundamentais da União Europeia, criada pelo Regulamento (CE) n.º 168/2007 do Conselho[75].

Artigo 38.º
Formato de mensagem universal

1. Pelo presente é instituída a norma Formato de Mensagem Universal (UMF). A UMF define as normas relativas a determinados elementos do conteúdo de intercâmbio de informações transfronteiras, entre sistemas de informação, autoridades e/ou organizações no domínio da Justiça e Assuntos Internos.

2. A norma UMF deve ser utilizada no desenvolvimento do SES, do [ETIAS], do portal europeu de pesquisa, do CIR, do MID e, se for caso disso, no desenvolvimento pela eu-LISA ou qualquer outro organismo da UE de novos modelos de intercâmbio de informações e de sistemas de informação no domínio da Justiça e Assuntos Internos.

3. A aplicação da norma UMF pode ser tida em consideração no VIS, SIS e em quaisquer modelos de intercâmbio de informações transfronteiras e sistemas de informação, existentes ou novos, no domínio da Justiça e Assuntos Internos, desenvolvidos pelos Estados-Membros ou países associados.

4. A Comissão deve adotar um ato de execução para estabelecer e desenvolver a norma UMF referida no n.º 1. Esses atos de execução devem ser adotados em conformidade com o procedimento de exame a que se refere o artigo 64.º, n.º 2.

[75] Regulamento (CE) n.º 168/2007 do Conselho, de 15 de fevereiro de 2007, que cria a Agência dos Direitos Fundamentais da União Europeia (JO L 53 de 22.2.2007, p. 1).

Artigo 39.º
Repositório central para a elaboração de relatórios e estatísticas

1. É criado um repositório central para a elaboração de relatórios e estatísticas (CRRS) para efeitos de apoio aos objetivos do SES, do VIS, [do ETIAS] e do SIS e para gerar dados estatísticos intersistemas e relatórios analíticos para fins políticos, operacionais e para efeitos de qualidade dos dados.

2. A eu-Lisa deve criar, implementar e alojar o CRRS nas suas instalações técnicas, contendo os dados referidos no [artigo 63.º do Regulamento do SES], no artigo 17.º do Regulamento (CE) n.º 767/2008 [no artigo 73.º do Regulamento do ETIAS] e [no artigo 54.º do Regulamento relativo ao SIS no domínio dos controlos das fronteiras], logicamente separados. Os dados contidos no CRRS não devem permitir a identificação de pessoas. O acesso ao repositório deve ser concedido mediante um acesso seguro através da rede de Serviços Seguros Transeuropeus de Telemática entre as Administrações (TESTA) com controlo do acesso e perfis de utilizador específicos, unicamente com a finalidade de elaboração de relatórios e estatísticas, às autoridades a que se refere o [artigo 63.º do Regulamento SES], o artigo 17.º do Regulamento (CE) n.º 767/2008 [o artigo 73.º do Regulamento ETIAS] e [o artigo 54.º do Regulamento relativo ao SIS no domínio dos controlos das fronteiras].

3. A eu-LISA deve tornar os dados anónimos e registar tais dados anónimos no CRRS. O processo de tornar os dados anónimos deve ser automatizado.

4. O CRRS é constituído por:

   (a) Uma infraestrutura central, constituída por um repositório de dados que permita a prestação de dados anónimos;

   (b) Uma infraestrutura de comunicação segura para ligar o CRRS ao SES, [ao ETIAS], ao VIS e ao SIS, bem como às infraestruturas centrais do BMS, do CIR e MID.

5. A Comissão deve estabelecer regras pormenorizadas sobre o funcionamento do CRRS, incluindo garantias específicas para o tratamento dos dados pessoais a que se referem os n.ºs 2 e 3 e regras de segurança aplicáveis ao repositório através de atos de execução. Esses atos de execução devem ser adotados em conformidade com o procedimento de exame a que se refere o artigo 64.º, n.º 2.

CAPÍTULO VII
Proteção de dados

Artigo 40.º
Responsável pelo tratamento de dados

1. No que respeita ao tratamento dos dados no serviço partilhado de correspondências biométricas (BMS), as autoridades dos Estados-Membros que são responsáveis pelo

tratamento de dados do VIS, SES e SIS, respetivamente, devem ser igualmente consideradas responsáveis pelo tratamento dos dados, em conformidade com o artigo 4.º, n.º 7, do Regulamento (UE) 2016/679, no que diz respeito aos modelos biométricos obtidos a partir dos dados referidos no artigo 13.º introduzidos nos sistemas respetivos, sendo responsáveis pelo tratamento dos modelos biométricos no BMS.

2. No que respeita ao tratamento dos dados no repositório comum de dados de identificação (CIR), as autoridades dos Estados-Membros que são responsáveis pelo tratamento de dados para o VIS, SES e [ETIAS], respetivamente, devem ser igualmente consideradas responsáveis pelo tratamento dos dados, em conformidade com o artigo 4.º, n.º 7, do Regulamento (UE) 2016/679 no respeitante aos dados referidos no artigo 18.º introduzidos nos sistemas respetivos, sendo responsáveis pelo tratamento desses dados pessoais no CIR.

3. No que respeita ao tratamento dos dados no detetor de identidades múltiplas:

   (a) A Agência Europeia da Guarda de Fronteiras e Costeira é considerada responsável pelo tratamento dos dados nos termos do artigo 2.º, alínea b), do Regulamento n.º 45/2001, no que diz respeito ao tratamento de dados pessoais pela unidade central do ETIAS;

   (b) As autoridades dos Estados-Membros que adicionarem ou modificarem os dados no processo de confirmação de identidade são igualmente consideradas responsáveis pelo tratamento, em conformidade com o artigo 4.º, n.º 7, do Regulamento (UE) 2016/679, sendo responsáveis pelo tratamento dos dados pessoais no detetor de identidades múltiplas.

Artigo 41.º
Subcontratante de dados

No que respeita ao tratamento de dados pessoais no CIR, a eu-LISA deve ser considerada um subcontratante de dados nos termos do artigo 2.º, alínea e), do Regulamento (CE) n.º 45/2001.

Artigo 42.º
Segurança do tratamento

1. Tanto a eu-LISA como as autoridades dos Estados -Membros devem garantir a segurança do tratamento dos dados pessoais que decorre nos termos do presente regulamento. A eu-LISA, [a unidade central do ETIAS] e as autoridades dos Estados-Membros devem cooperar em tarefas relacionadas com a segurança.

2. Sem prejuízo do artigo 22.º do Regulamento (CE) n.º 45/2001, a eu-LISA deve adotar as medidas necessárias para garantir a segurança dos componentes de interoperabilidade e da respetiva infraestrutura de comunicação conexa.

3. Em especial, a eu-LISA deve adotar as medidas necessárias, incluindo um plano de segurança, um plano de continuidade das atividades e um plano de recuperação na sequência de catástrofes, a fim de:

(a) Proteger fisicamente os dados, nomeadamente através da elaboração de planos de emergência para a proteção da infraestrutura crítica;

(b) Impedir que os suportes de dados possam ser lidos, copiados, alterados ou retirados sem autorização;

(c) Impedir a introdução não autorizada de dados, bem como o controlo, a alteração ou o apagamento não autorizado de dados pessoais armazenados;

(d) Impedir o tratamento não autorizado de dados, bem como a cópia, alteração ou eliminação não autorizada de dados;

(e) Assegurar que as pessoas autorizadas a aceder aos componentes de interoperabilidade tenham acesso apenas aos dados abrangidos pela sua autorização de acesso através de identidades de utilizador individuais e de modos de acesso confidenciais;

(f) Assegurar a possibilidade de verificação e determinação das entidades às quais podem ser transmitidos os dados pessoais através de equipamentos de comunicação de dados;

(g) Assegurar a possibilidade de verificação e determinação dos dados que foram processados nos componentes de interoperabilidade, em que momento, por quem e com que finalidade;

(h) Impedir a leitura, a cópia, a alteração ou a eliminação não autorizadas dos dados pessoais durante a transmissão de dados pessoais para ou a partir de componentes de interoperabilidade, ou durante o transporte dos suportes de dados, designadamente através de técnicas de cifragem adequadas;

(i) Controlar a eficácia das medidas de segurança referidas no presente número e tomar as medidas necessárias a nível organizacional relacionadas com o controlo interno de forma a assegurar a conformidade com o presente regulamento.

4. Os Estados-Membros devem adotar medidas equivalentes às referidas no n.º 3 no que respeita à segurança relativamente ao tratamento dos dados pessoais por parte das autoridades com direitos de acesso a qualquer dos componentes de interoperabilidade.

Artigo 43.º
Confidencialidade dos dados do SIS

1. Cada Estado-Membro deve aplicar as suas regras de sigilo profissional ou outras obrigações de confidencialidade equivalentes a todas as pessoas e entidades que necessitem de trabalhar com dados do SIS, acedidos através de qualquer um dos componentes de interoperabilidade, em conformidade com o respetivo direito interno. A referida obrigação mantém-se igualmente depois de essas pessoas cessarem funções ou deixarem o emprego, ou após a cessação das atividades dessas entidades.

2. Sem prejuízo do disposto no artigo 17.º do Estatuto dos Funcionários da União Europeia e no Regime Aplicável aos outros Agentes da União Europeia, a eu-LISA deve aplicar as normas de sigilo profissional adequadas ou outras obrigações de confidencialidade equivalentes segundo normas equiparáveis às estabelecidas no n.º 1 a todo o seu pessoal que tenha de trabalhar com dados do SIS. A referida obrigação mantém-se depois de essas pessoas cessarem funções ou deixarem o emprego, ou após a cessação das suas atividades.

Artigo 44.º
Incidentes de segurança

1. Qualquer acontecimento que tenha ou possa ter impacto na segurança dos componentes de interoperabilidade e que possa causar-lhes danos ou perda de dados armazenados nos mesmos é considerado um incidente de segurança, nomeadamente na eventualidade de ter havido acesso não autorizado aos dados ou quando a disponibilidade, integridade e confidencialidade dos dados tenha ou possa ter sido posta em causa.

2. Os incidentes de segurança devem ser geridos por forma a assegurar uma resposta rápida, eficaz e adequada.

3. Sem prejuízo da notificação e comunicação da violação de dados pessoais ao abrigo do disposto no artigo 33.º do Regulamento (UE) 2016/679, no artigo 30.º da Diretiva (UE) 2016/680, ou em ambos, os Estados-Membros devem notificar a Comissão, a eu-LISA e a Autoridade Europeia para a Proteção de Dados dos incidentes de segurança. Em caso de incidente de segurança em relação aos componentes de interoperabilidade da infraestrutura central, a eu-LISA deve notificar a Comissão e a Autoridade Europeia para a Proteção de Dados.

4. As informações relativas a um incidente de segurança que tenha ou possa ter impacto no funcionamento dos componentes de interoperabilidade ou na disponibilidade, integridade e confidencialidade dos dados devem ser facultadas aos Estados-Membros e comunicadas em conformidade com o plano de gestão de incidentes fornecido pela eu-LISA.

5. Os Estados-Membros em causa e a eu-LISA devem cooperar em caso de incidente de segurança. A Comissão deve estabelecer as especificações deste processo de cooperação por meio de atos de execução. Esses atos de execução devem ser adotados em conformidade com o procedimento de exame a que se refere o artigo 64.º, n.º 2.

Artigo 45.º
Autocontrolo

Os Estados-Membros e as entidades competentes da UE devem assegurar que cada autoridade com direito de acesso aos componentes de interoperabilidade toma as medidas necessárias para controlar o cumprimento do regulamento e coopera, sempre que necessário, com a autoridade de controlo.

Os responsáveis pelo tratamento dos dados a que se refere o artigo 40.º devem tomar as medidas necessárias para verificar a conformidade do tratamento de dados ao abrigo do presente regulamento, incluindo a verificação dos registos, e cooperar, se necessário, com as autoridades de controlo a que se referem os artigos 49.º e 50.º.

Artigo 46.º
Direito à informação

1. Sem prejuízo do direito à informação previsto nos artigos 11.º e 12.º do Regulamento (CE) n.º 45/2001 e nos artigos 13.º e 14.º do Regulamento (UE) 2016/679, as pessoas cujos dados são conservados no serviço partilhado de correspondências biométricas, no repositório comum de dados de identificação ou no detetor de identidades múltiplas devem ser informadas pela autoridade responsável pela recolha de dados, no momento da recolha dos seus dados, sobre o tratamento de dados pessoais para efeitos da aplicação do presente regulamento, incluindo a identidade e os dados de contacto dos respetivos responsáveis pelo tratamento de dados, e sobre os procedimentos para exercerem os seus direitos de acesso, de retificação e de apagamento, bem como sobre os dados de contacto da Autoridade Europeia para a Proteção de Dados e da autoridade nacional de controlo do Estado-Membro responsável pela recolha dos dados.

2. As pessoas cujos dados estejam registados no SES, no VIS ou [no ETIAS] devem ser informadas sobre o tratamento de dados para efeitos do presente regulamento em conformidade com o disposto no n.º 1, quando:

   (a) [For criado ou atualizado um processo individual no SES, em conformidade com o artigo 14.º do Regulamento SES];

   (b) For criado ou atualizado um processo de pedido no VIS em conformidade com o artigo 8.º do Regulamento (CE) n.º 767/2008;

   (c) [For criado ou atualizado um processo de pedido no ETIAS, em conformidade com o artigo 17.º do Regulamento ETIAS;]

   (d) - (Não aplicável);

   (e) - (Não aplicável).

Artigo 47.º
Direito de acesso, de retificação e de apagamento

1. A fim de exercer os seus direitos ao abrigo dos artigos 13.º, 14.º, 15.º e 16.º do Regulamento (CE) n.º 45/2001 e dos artigos 15.º, 16.º, 17.º e 18.º do Regulamento (UE) 2016/679, qualquer pessoa tem o direito de se dirigir ao Estado-Membro responsável pela verificação manual das diferentes identidades ou de qualquer Estado-Membro, que deve examinar e responder ao pedido.

2. O Estado-Membro responsável pela verificação manual de identidades diferentes, tal como referido no artigo 29.º ou o Estado-Membro ao qual foi apresentado o pedido deve responder a tais pedidos no prazo de 45 dias a contar da receção do pedido.

3. Se for apresentado um pedido de retificação ou apagamento de dados pessoais a um Estado-Membro diferente do Estado-Membro responsável, o Estado-Membro ao qual foi apresentado o pedido deve contactar as autoridades do Estado-Membro responsável no prazo de sete dias e o Estado-Membro responsável deve verificar a exatidão dos dados e a legalidade do tratamento dos dados no prazo de 30 dias a contar desse contacto.

4. Sempre que, na sequência de um exame, se concluir que os dados armazenados no detetor de identidades múltiplas (MID) são factualmente inexatos ou foram registados ilegalmente, o Estado-Membro responsável ou, se for caso disso, o Estado-Membro ao qual foi apresentado o pedido, deve proceder à sua retificação ou ao seu apagamento.

5. Sempre que os dados no MID forem alterados pelo Estado-Membro responsável durante o respetivo período de validade, o Estado-Membro responsável deve proceder ao tratamento previsto no artigo 27.º e, quando aplicável, no artigo 29.º, a fim de determinar se os dados alterados devem ser ligados. Se o tratamento não detetar qualquer resposta positiva, o Estado-Membro responsável ou, se for caso disso, o Estado-Membro ao qual foi apresentado o pedido, deve apagar os dados do processo de confirmação de identidade. Sempre que o tratamento automatizado comunicar uma ou várias respostas positivas, o Estado-Membro responsável deve criar ou atualizar a ligação em questão em conformidade com as disposições aplicáveis do presente regulamento.

6. Sempre que o Estado-Membro responsável ou, se for caso disso, o Estado-Membro ao qual foi apresentado o pedido não considerar que os dados armazenados no MID são factualmente inexatos ou foram registados ilegalmente, deve adotar uma decisão administrativa, explicando por escrito e sem demora à pessoa em causa as razões pelas quais não está disposto a retificar ou a apagar os dados que lhe dizem respeito.

7. A referida decisão deve informar também o interessado sobre a possibilidade de impugnar a decisão tomada relativamente ao pedido referido no n.º 3 e, se for caso disso, sobre a forma de intentar uma ação ou apresentar uma reclamação junto das autoridades ou tribunais competentes, e informar sobre um eventual auxílio, inclusivamente por parte das autoridades nacionais de controlo competentes.

8. Qualquer pedido apresentado em conformidade com o n.º 3 deve incluir as informações necessárias para identificar a pessoa em causa. Essas informações devem ser utilizadas exclusivamente para permitir o exercício dos direitos referidos no n.º 3, após o que serão imediatamente apagadas.

9. O Estado-Membro responsável ou, se for caso disso, o Estado-Membro ao qual foi apresentado o pedido, deve conservar um registo sob a forma de documento escrito relativo à apresentação de um pedido nos termos do n.º 3 e à forma como foi tratado, e disponibilizar sem demora esse documento às autoridades nacionais de controlo da proteção de dados competentes.

Artigo 48.º
Comunicação de dados pessoais a países terceiros, organizações internacionais e entidades privadas

Os dados pessoais armazenados ou consultados pelos componentes de interoperabilidade não devem ser transferidos nem disponibilizados a países terceiros, organizações internacionais ou entidades privadas, com exceção das transferências de dados para a Interpol para efeitos do tratamento automatizado referido no [artigo 18.º, n.º 2, alínea b), e alínea m) do Regulamento ETIAS] ou para efeitos do artigo 8.º, n.º 2, do Regulamento (UE) 2016/399. Estas transferências de dados pessoais para a Interpol devem cumprir as disposições do artigo 9.º do Regulamento (CE) n.º 45/2001 e do capítulo V do Regulamento (UE) 2016/679.

Artigo 49.º
Fiscalização pela autoridade nacional de controlo

1. A autoridade ou autoridades de controlo designada(s) nos termos do artigo 49.º do Regulamento (UE) 2016/679 deve(m) garantir a realização de uma auditoria às operações de tratamento de dados pelas autoridades nacionais competentes em conformidade com as normas internacionais de auditoria aplicáveis, pelo menos de quatro em quatro anos.

2. Os Estados-Membros devem assegurar que a autoridade de controlo dispõe dos meios necessários para cumprir as tarefas que lhe são confiadas no âmbito do presente regulamento.

Artigo 50.º
Fiscalização pelo Autoridade Europeia para a Proteção de Dados

A Autoridade Europeia para a Proteção de Dados deve garantir a realização de uma auditoria às atividades de tratamento de dados pessoais da eu-LISA em conformidade com as normas internacionais de auditoria aplicáveis, pelo menos de quatro em quatro anos. Deve ser enviado um relatório dessa auditoria ao Parlamento Europeu, ao Conselho, à eu-LISA, à Comissão e aos Estados-Membros. Deve ser dada à eu-LISA a oportunidade de efetuar comentários antes da adoção dos relatórios.

Artigo 51.º
Cooperação entre as autoridades nacionais de controlo e a Autoridade Europeia para a Proteção de Dados

1. A Autoridade Europeia para a Proteção de Dados deve atuar em estreita cooperação com as autoridades nacionais de controlo no que respeita a questões específicas que exijam o envolvimento nacional, em particular se a Autoridade Europeia para a Proteção de Dados ou uma autoridade nacional de controlo detetar discrepâncias relevantes entre as práticas dos Estados-Membros ou detetar transferências potencialmente ilegais através dos canais de comunicação dos componentes de interoperabilidade, ou no contexto das questões levantadas por uma ou mais autoridades nacionais de controlo sobre a implementação e a interpretação do presente regulamento.

2. Nos casos referidos no n.º 1, o controlo coordenado deve ser assegurado, em conformidade com o artigo 62.º do Regulamento (UE) XXXX/2018 [Regulamento n.º 45/2001 revisto].

CAPÍTULO VIII
Responsabilidades

Artigo 52.º
Responsabilidades da eu-LISA durante a fase de conceção e desenvolvimento

1. A eu-LISA deve garantir o funcionamento das infraestruturas centrais dos componentes de interoperabilidade em conformidade com o presente regulamento.

2. Os componentes de interoperabilidade devem ser alojados pela eu-LISA nas suas instalações técnicas e fornecerem as funcionalidades estabelecidas no presente regulamento, em conformidade com as condições de segurança, de disponibilidade, de qualidade e de rapidez a que se refere o artigo 53.º, n.º 1.

3. A eu-LISA é responsável pelo desenvolvimento dos componentes de interoperabilidade, de quaisquer adaptações necessárias para estabelecer a interoperabilidade entre os sistemas centrais do SES, VIS, [ETIAS], SIS e do Eurodac, e [do sistema ECRIS-TCN], e o portal europeu de pesquisa, o serviço partilhado de correspondências biométricas, o repositório comum de dados de identificação e o detetor de identidades múltiplas.

   A eu-LISA deve definir a conceção da arquitetura física dos componentes de interoperabilidade, incluindo as infraestruturas de comunicação e especificações técnicas e a respetiva evolução no que diz respeito à infraestrutura central e à infraestrutura de comunicação segura, que será adotada pelo Conselho de Administração, sob reserva do parecer favorável da Comissão. A eu-LISA deve também implementar quaisquer adaptações necessárias do SES, [ETIAS], SIS ou VIS decorrentes do estabelecimento da interoperabilidade e previstas pelo presente regulamento.

   A eu-LISA deve desenvolver e implementar os componentes de interoperabilidade assim que possível após a entrada em vigor do presente regulamento e a adoção pela Comissão das medidas previstas nos artigos 8.º, n.º 2, 9.º, n.º 7, 28.º, n.º 5 e 6, 37.º, n.º 4, 38.º, n.º 4, 39.º, n.º 5 e 44.º , n.º 5.

   O desenvolvimento deve consistir na elaboração e implementação das especificações técnicas, nos testes e na coordenação global do projeto.

4. Durante a fase de conceção e desenvolvimento deve ser criado um Conselho de Gestão do Programa, constituído por um máximo de 10 membros. Esta órgão é constituído por sete membros nomeados pelo Conselho de Administração da eu-LISA de entre os seus membros ou suplentes, pelo presidente do Grupo Consultivo da Interoperabilidade referido no artigo 65.º, por um membro em representação da

eu-LISA nomeado pelo seu Diretor Executivo e por um membro nomeado pela Comissão. Os membros nomeados pelo Conselho de Administração da eu-LISA devem ser escolhidos apenas entre os Estados-Membros que estejam plenamente vinculados no quadro do direito da União pelos instrumentos legislativos que regem o desenvolvimento, o estabelecimento, o funcionamento e a utilização de todos os sistemas informáticos de grande escala geridos pela eu-LISA e que irão participar nos componentes de interoperabilidade.

5. O Conselho de Gestão do Programa deve reunir-se regularmente e pelo menos três vezes por trimestre. O Conselho de Gestão do Programa deve garantir a gestão adequada da fase de conceção e desenvolvimento dos componentes de interoperabilidade.

O Conselho de Gestão do Programa deve apresentar todos os meses ao Conselho de Administração relatórios escritos sobre os progressos do projeto. O Conselho de Gestão do Programa não dispõe de qualquer poder de decisão nem qualquer mandato para representar os membros do Conselho de Administração da eu-LISA.

6. O Conselho de Administração da eu-LISA deve estabelecer o regulamento interno do Conselho de Gestão do Programa, que deve incluir, em particular, as regras sobre:

(a) O exercício da presidência;

(b) Os locais de reunião;

(c) A preparação de reuniões;

(d) A admissão de peritos às reuniões;

(e) Os planos de comunicação que assegurem a disponibilização de informações circunstanciadas aos membros não participantes do Conselho de Administração.

A presidência deve ser assumida por um Estado-Membro que esteja plenamente vinculado no quadro do direito da União pelos instrumentos legislativos que regem o desenvolvimento, o estabelecimento, o funcionamento e a utilização de todos os sistemas informáticos de grande escala geridos pela eu-LISA.

Todas as despesas de viagem e de estadia incorridas pelos membros do Conselho de Gestão do Programa devem ser suportadas pela Agência, aplicando-se o artigo 10.º do regulamento interno da eu-LISA *mutatis mutandis*. A eu-LISA deve assegurar o secretariado ao Conselho de Gestão do Programa.

O Grupo Consultivo de Interoperabilidade, referido no artigo 65.º, deve reunir-se regularmente até à entrada em funcionamento do componente de interoperabilidade. Deve apresentar um relatório após cada reunião do Conselho de Gestão do Programa. O grupo deve fornecer os conhecimentos técnicos necessários para apoiar as atividades do Conselho de Gestão do Programa e proceder ao acompanhamento do nível de preparação dos Estados-Membros.

Artigo 53.º
Responsabilidades da eu-LISA após a entrada em funcionamento

1. Após a entrada em funcionamento de cada componente de interoperabilidade, a eu-LISA deve ser responsável pela gestão técnica da infraestrutura central e pelas interfaces uniformes nacionais. Em cooperação com os Estados-Membros, deve assegurar constantemente a melhor tecnologia disponível, sob reserva de uma análise custo-benefício. A eu-LISA deve ser igualmente responsável pela gestão técnica da infraestrutura de comunicação a que se referem os artigos 6.º, 12.º, 17.º, 25.º e 39.º.

   A gestão técnica dos componentes de interoperabilidade compreende todas as funções necessárias para manter o funcionamento dos componentes de interoperabilidade, 24 horas por dia e 7 dias por semana, em conformidade com o presente regulamento, em especial o trabalho de manutenção e as adaptações técnicas indispensáveis para garantir que os componentes funcionam a um nível de qualidade técnica satisfatório, em especial no que respeita ao tempo de resposta para efeitos de consulta das infraestruturas centrais, em conformidade com as especificações técnicas.

2. Sem prejuízo do disposto no artigo 17.º do Estatuto dos Funcionários da União Europeia, a eu-LISA deve aplicar as normas de sigilo profissional adequadas ou outras obrigações de confidencialidade equivalentes a todo o seu pessoal cujo trabalho envolva os dados armazenados nos componentes de interoperabilidade. Esta obrigação mantém-se depois de essas pessoas cessarem funções ou deixarem o emprego, ou após a cessação das suas atividades.

3. A eu-LISA deve desenvolver e manter um mecanismo e procedimentos para a realização de controlos de qualidade dos dados armazenados no serviço partilhado de correspondências biométricas e no repositório comum de dados de identificação em conformidade com o artigo 37.º.

4. A eu-LISA deve realizar também tarefas relacionadas com a organização de formação sobre a utilização técnica dos componentes de interoperabilidade.

Artigo 54.º
Responsabilidades dos Estados-Membros

1. Cada Estado-Membro é responsável pela:

   (a) Ligação à infraestrutura de comunicação do portal europeu de pesquisa (ESP) e ao repositório comum de dados de identificação (CIR);

   (b) Integração dos sistemas e infraestruturas nacionais existentes com o ESP, o serviço partilhado de correspondências biométricas, o CIR e o detetor de identidades múltiplas;

   (c) Organização, gestão, funcionamento e manutenção da respetiva infraestrutura nacional existente e da sua ligação aos componentes de interoperabilidade;

   (d) Gestão e disponibilização do acesso por parte do pessoal devidamente autorizado e pelo pessoal devidamente habilitado das autoridades nacionais

competentes ao ESP, ao CIR e ao detetor de identidades múltiplas em conformidade com o presente regulamento, e criação e atualização periódica de uma lista dos membros do pessoal e respetivos perfis;

(e) Adoção das medidas legislativas referidas no artigo 20.º, n.º 3, a fim de aceder ao CIR para efeitos de identificação;

(f) Verificação manual das diferentes identidades referida no artigo 29.º;

(g) Aplicação de requisitos de qualidade dos dados nos sistemas de informação da UE e nos componentes de interoperabilidade;

(h) Correção de quaisquer deficiências identificadas no relatório de avaliação da Comissão sobre a qualidade dos dados a que se refere o artigo 37.º, n.º 5.

2. Cada Estado-Membro deve ligar as suas autoridades designadas referidas no artigo 4.º, n.º 24, ao CIR.

Artigo 55.º
Responsabilidades da unidade central do ETIAS

A unidade central do ETIAS é responsável pela:

(a) Verificação manual das diferentes identidades referida no artigo 29.º;

(b) Realização de uma deteção de identidades múltiplas entre os dados armazenados no VIS, Eurodac e SIS referidos no artigo 59.º.

CAPÍTULO IX
Alterações a outros instrumentos da União

Artigo 55.º-A
Alterações ao Regulamento (UE) 2016/399

O Regulamento (UE) 2016/399 é alterado do seguinte modo:

No artigo 8.º do Regulamento (UE) 2016/399, é aditado o n.º 4-A seguinte:

«4-A. Se, à entrada ou à saída, a consulta das bases de dados pertinentes, incluindo o detetor de identidades múltiplas através do portal europeu de pesquisa, referidos, respetivamente, no [artigo 4.º, n.º 36 e 33 do Regulamento n.º 2018/XX relativo à interoperabilidade] se traduzir numa ligação amarela ou numa ligação vermelha, a pessoa alvo da consulta deve ser submetida ao controlo de segunda linha.

O guarda de fronteira de segunda linha deve proceder à consulta do detetor de identidades múltiplas conjuntamente com o repositório comum de dados de identificação referido no [artigo 4.º, n.º 35 do Regulamento n.º 2018/XX relativo à interoperabilidade] ou do Sistema de Informação Schengen ou ambos para avaliar as diferenças nas identidades ligadas e deve efetuar qualquer verificação adicional necessária para tomar uma decisão sobre o estatuto e a

cor da ligação bem como tomar uma decisão sobre a entrada ou recusa de entrada da pessoa em questão.

Em conformidade com o [artigo 59.º, n.º 1 do Regulamento n.º 2018/XX], o presente número é aplicável unicamente a partir do início das operações do detetor de identidades múltiplas.»

Artigo 55.º-B
Alterações ao Regulamento (UE) 2017/2226

O Regulamento (UE) 2017/2226 é alterado do seguinte modo:

1) No artigo 1.º, é aditado o seguinte número:

«1-A. Através do armazenamento da identidade, de documentos de viagem e dados biométricos no repositório comum de dados de identificação (CIR) estabelecido pelo [artigo 17.º do Regulamento n.º 2018/XX relativo à interoperabilidade], o SES contribui para facilitar e apoiar a identificação correta das pessoas registadas no SES, nas condições e com os objetivos finais referidos no [artigo 20.º] do mesmo regulamento.»

2) No artigo 3.º, é aditado o seguinte ponto 21-A):

« «CIR», o repositório comum de dados de identificação tal como definido no [artigo 4.º, n.º 35 do Regulamento n.º 2018/XX relativo à interoperabilidade]»

3) O artigo 3.º, n.º 1, ponto 22) é substituído pelo seguinte:

«22) «Dados do SES», todos os dados armazenados no Sistema Central do SES e no CIR em conformidade com o artigo 14.º e os artigos 16.º a 20.º.»

4) No artigo 3.º, é aditado um novo ponto 22-A):

«22-A) «Dados de identidade», os dados a que se refere o artigo 16.º, n.º 1, alínea a);»

5) No artigo 6.º, n.º 1, é inserida a seguinte alínea:

«j) Garantir a identificação correta das pessoas.»

6) O artigo 7.º, n.º 1, alínea a) é substituído pelo seguinte:

«a) O repositório comum de dados de identificação (CIR) a que se refere o [artigo 17.º, n.º 2, alínea a), do Regulamento n.º 2018/XX relativo à interoperabilidade];

aa) Um sistema central (Sistema Central do SES);»

7) No artigo 7.º, n.º 1, a alínea f) é substituída pelo seguinte:

«f) Uma infraestrutura de comunicação segura entre o Sistema Central do SES e as infraestruturas centrais do portal europeu de pesquisa estabelecido pelo [artigo 6.º do Regulamento n.º 2018/XX, relativo à interoperabilidade], o serviço partilhado de correspondências biométricas estabelecido pelo [artigo 12.º do Regulamento n.º 2018/XX, relativo à interoperabilidade], o repositório comum de dados de identificação, estabelecido pelo [artigo 17.º do Regulamento n.º 2018/XX relativo à

interoperabilidade] e o detetor de identidades múltiplas estabelecido pelo [artigo 25.º do Regulamento n.º 2018/XX relativo à interoperabilidade]».

8) No artigo 7.º, é aditado o seguinte número:

«1-A. O CIR contem os dados referidos no artigo 16.º, n.º 1, alíneas a) a d) e no artigo 17.º, n.º 1, alíneas a) a c), sendo os restantes dados do SES armazenados no Sistema Central do SES.

9) No artigo 9.º, é aditado o seguinte número:

«3. O acesso à consulta dos dados do SES armazenados no CIR deve ser exclusivamente reservado ao pessoal devidamente autorizado das autoridades nacionais de cada Estado-Membro e ao pessoal devidamente autorizado dos organismos da UE que são competentes para os efeitos previstos no [artigo 20.º e artigo 21.º do Regulamento n.º 2018/XX relativo à interoperabilidade]. Este acesso deve ser limitado na medida do necessário para o desempenho das funções das autoridades nacionais e organismos da UE em conformidade com as finalidades, sendo proporcional aos objetivos prosseguidos.»

10) No artigo 21.º, n.º 1, a expressão «Sistema Central do SES» será substituída, em ambas as ocorrências, pela expressão «Sistema Central do SES ou do CIR».

11) No artigo 21.º, n.º 2, a expressão «tanto no sistema central do SES como na IUN» é substituída pela expressão «tanto no Sistema Central do SES e do CIR, por um lado, e na IUN, por outro».

12) No artigo 21.º, n.º 2, a expressão «são introduzidos no Sistema Central do SES» é substituída pela expressão «são introduzidos no Sistema Central do SES e do CIR».

13) É aditado um novo número 1-A) ao artigo 32.º:

«1-A. Nos casos em que as autoridades designadas lançaram uma consulta do CIR em conformidade com o [artigo 22.º do Regulamento n.º 2018/XX relativo à interoperabilidade], podem ter acesso ao SES para consulta quando a resposta recebida, tal como referido no n.º 3.º do [artigo 22.º do Regulamento n.º 2018/XX relativo à interoperabilidade] revelar que os dados estão armazenados no SES.»

14) O artigo 32.º, n.º 2 é substituído pelo seguinte:

«2. O acesso ao SES enquanto ferramenta para identificar um suspeito desconhecido, um autor desconhecido ou uma vítima presumível desconhecida de uma infração terrorista ou outra infração penal grave só é autorizado quando for lançada uma consulta ao CIR nos termos do [artigo 22.º do Regulamento 2018/XX relativo à interoperabilidade] e se estiverem reunidas todas as condições referidas no n.º 1 e no n.º 1-A.

Contudo, esta condição adicional não se aplica em caso de urgência se for necessário impedir um perigo iminente para a vida de uma pessoa associada a uma infração terrorista ou outra infração penal grave. Esses motivos razoáveis devem ser incluídos no pedido eletrónico ou escrito enviado pela unidade operacional da autoridade designada para o ponto de acesso central.»

15) O artigo 32.º, n.º 4, é suprimido.

16) É aditado um novo número 1-A) ao artigo 33.º:

«1-A. Nos casos em que a Europol lançar uma consulta ao CIR em conformidade com o [artigo 22.º do Regulamento n.º 2018/XX relativo à interoperabilidade], pode ter acesso ao SES para consulta quando a resposta recebida, tal como referido no n.º 3 do [artigo 22.º do Regulamento n.º 2018/XX relativo à interoperabilidade] revelar que os dados estão armazenados no SES.»

17) No artigo 33.º, o n.º 3 é substituído pelo seguinte:

«As condições estabelecidas no artigo 32.º, n.º 3 e n.º 5 são aplicáveis em conformidade.»

18) No artigo 34.º, n.º 1 e n.º 2, a expressão «no Sistema Central do SES» é substituída pela expressão «no CIR e no Sistema Central do SES, respetivamente».

19) No artigo 34.º, n.º 5, a expressão «do Sistema Central do SES» é substituída pela expressão «do Sistema Central do SES e do CIR».

20) No artigo 35.º, o n.º 7 é substituído pelo seguinte:

«O Sistema Central do SES e o CIR informam imediatamente todos os Estados-Membros do apagamento dos dados do SES e do CIR e, se for caso disso, retiram-nos da lista de pessoas identificadas referida no artigo 12.º, n.º 3.»

21) No artigo 36.º, a expressão «do Sistema Central do SES» é substituída pela expressão «do Sistema Central do SES e do CIR».

22) No artigo 37.º, n.º 1, a expressão «desenvolvimento do Sistema Central do SES» é substituída pela expressão «desenvolvimento do Sistema Central do SES e do CIR».

23) No do artigo 37.º, n.º 3, primeiro parágrafo, a expressão «do Sistema Central do SES» é substituída, na primeira e terceira ocorrência, pela expressão «do Sistema Central do SES e do CIR».

24) No artigo 46.º, n.º 1, é aditada a alínea f) seguinte:

«f) Sempre que adequado, uma referência à utilização do portal europeu de pesquisa para consultar o SES, tal como referido no [artigo 7.º, n.º 2, do Regulamento (UE) n.º 2018/XX relativo à interoperabilidade].»

25) O artigo 63.º, n.º 2, é substituído pelo seguinte:

«2. Para os efeitos do n.º 1 do presente artigo, a eu-LISA armazena os dados referidos no n.º 1 no repositório central para a elaboração de relatórios e estatísticas referido no [artigo 39.º do Regulamento n.º 2018/XX relativo à interoperabilidade].»

26) No artigo 63.º, n.º 4, é aditado um novo parágrafo:

«As estatísticas diárias devem ser conservadas no repositório central para a elaboração de relatórios e estatísticas.»

Artigo 55.º-C
Alterações à Decisão 2004/512/CE do Conselho

A Decisão 2004/512/CE do Conselho que estabelece o Sistema de Informação sobre Vistos (VIS) é alterada do seguinte modo:

O artigo 1.º, n.º 2, é alterado do seguinte modo:

«2. O Sistema de Informação sobre Vistos baseia-se numa arquitetura centralizada e consiste:

a) Num repositório comum de dados de identificação a que se refere o [artigo 17.º, n.º 2, alínea a), do Regulamento n.º 2018/XX relativo à interoperabilidade];

b) Num sistema central de informação, a seguir designado «Sistema Central de Informação sobre Vistos» (CS-VIS);

c) Numa interface em cada Estado-Membro, a seguir denominada «Interface Nacional» (NI-VIS), que assegura a conexão com a autoridade central nacional competente do respetivo Estado-Membro;

d) Numa infraestrutura de comunicação entre o Sistema Central de Informação sobre Vistos e as interfaces nacionais;

e) Num canal de comunicação seguro entre o Sistema Central do SES e o CS-VIS;

f) Numa infraestrutura de comunicação segura entre o Sistema Central do VIS e as infraestruturas centrais do portal europeu de pesquisa estabelecido pelo [artigo 6.º do Regulamento n.º 2018/XX relativo à interoperabilidade], o serviço partilhado de correspondências biométricas estabelecido pelo [artigo 12.º do Regulamento n.º 2018/XX relativo à interoperabilidade], o repositório comum de dados de identificação e o detetor de identidades múltiplas (MID) estabelecido pelo [artigo 25.º do Regulamento n.º 2018/XX relativo à interoperabilidade]».

Artigo 55.º-D
Alterações ao Regulamento (CE) n.º 767/2008

1) No artigo 1.º, é aditado o seguinte número:

«2. Mediante o armazenamento de identidade, documentos de viagem e dados biométricos no repositório comum de dados de identificação (CIR) estabelecido pelo [artigo 17.º do Regulamento n.º 2018/XX relativo à interoperabilidade], o VIS contribui para facilitar e apoiar a identificação correta das pessoas registadas no VIS nas condições e para os objetivos fundamentais estabelecidos no n.º 1 do presente artigo.»

2) No artigo 4.º, são aditados os seguintes pontos:

«12) «Dados VIS», todos os dados armazenados no Sistema Central do VIS e no CIR em conformidade com os artigos 9.º a 14.º.»

13) «Dados de identidade», os dados mencionados no artigo 9.º, n.º 4, alíneas a) a aa);

14) «Dados dactiloscópicos», os dados relativos às cinco impressões digitais dos dedos indicador, médio, anelar, mínimo e o polegar da mão direita, sempre que existentes, e da mão esquerda;

15) «Imagem facial», a imagem digitalizada do rosto;

16) «Dados biométricos», as impressões digitais e a imagem facial;»

3) No artigo 5.º, é aditado o seguinte número:

«1-A). O CIR contém os dados referidos no artigo 9.º, n.º 4, alínea a) a cc), artigo 9.º, n.º 5 e artigo 9.º, n.º 6, sendo os restantes dados VIS armazenados no Sistema Central do VIS.»

4) O artigo 6.º, n.º 2, é alterado do seguinte modo:

«2. O acesso ao VIS para efeitos de consulta dos dados é exclusivamente reservado ao pessoal devidamente autorizado das autoridades nacionais competentes, tendo em vista as finalidades referidas nos artigos 15.º a 22.º, e ao pessoal devidamente autorizado das autoridades nacionais e dos organismos da UE competentes para os efeitos previstos nos [artigos 20.º e 21.º do Regulamento n.º 2018/XX relativo à interoperabilidade], na medida em que estes dados sejam necessários para a execução das suas tarefas conformes com essas finalidades e proporcionais aos objetivos prosseguidos.»

5) O artigo 9.º, n.º 4, alíneas a) a c), é alterado do seguinte modo:

«a) Apelido; nome(s) próprio(s); data de nascimento; nacionalidade ou nacionalidades; sexo;

aa) Apelido de nascimento [apelido(s) anterior(es)]; local e país de nascimento; nacionalidade de nascimento;

b) Tipo e número do documento ou documentos de viagem e código de três letras do país emissor do documento ou documentos de viagem;

c) Data do termo de validade do documento ou documentos de viagem;

cc) Autoridade que emitiu o documento de viagem e a respetiva data de emissão;»

6) O artigo 9.º, n.º 5 é substituído pelo seguinte:

«Imagem facial, tal como definido no artigo 4.º, n.º 15».

7) No artigo 29.º, n.º 2, alínea a), o termo «VIS» é substituído pelo termo «VIS ou do CIR» em ambos os casos em que aparece.

Artigo 55.º-E
Alterações à Decisão 2008/633/JAI do Conselho

1) É aditado um novo número 1-A ao artigo 5.º:

«1-A. Nos casos em que as autoridades designadas tiverem lançado uma consulta do CIR em conformidade com o [artigo 22.º do Regulamento n.º 2018/XX relativo à interoperabilidade], podem aceder ao VIS para consulta quando a resposta recebida, tal como referido no n.º 3 do [artigo 22.º do Regulamento n.º 2018/XX relativo à interoperabilidade] revelar que os dados estão armazenados no VIS.»

2) É aditado um novo número 1-A ao artigo 7.º:

«1-A. Nos casos em que a Europol tiver lançado uma consulta do CIR em conformidade com o [artigo 22.º do Regulamento n.º 2018/XX relativo à interoperabilidade], pode aceder ao VIS para consulta quando a resposta recebida, tal como referido no n.º 3 do [artigo 22.º do Regulamento n.º 2018/XX relativo à interoperabilidade] revelar que os dados estão armazenados no VIS.»

CAPÍTULO X
Disposições finais

Artigo 56.º
Elaboração de relatórios e estatísticas

1. O pessoal devidamente autorizado das autoridades competentes dos Estados-Membros, da Comissão e da eu-LISA deve ter acesso ao sistema para consultar os seguintes dados relativos ao portal europeu de pesquisa (ESP), unicamente para efeitos da elaboração de relatórios e estatísticas, sem permitir a identificação individual:

   (a) Número de consultas por utilizador do perfil ESP;

   (b) Número de consultas efetuadas a cada uma das bases de dados da Interpol.

2. O pessoal devidamente autorizado das autoridades competentes dos Estados-Membros, da Comissão e da eu-LISA deve ter acesso ao sistema para consultar os seguintes dados relacionados com o repositório comum de dados de identificação, unicamente para efeitos da elaboração de relatórios e estatísticas, sem permitir a identificação individual:

   (a) Número de consultas para os efeitos dos artigos 20.º, 21.º e 22.º;

   (b) Nacionalidade, sexo e ano de nascimento da pessoa;

   (c) Tipo de documento de viagem e código de três letras do país emissor;

   (d) Número de consultas efetuadas com e sem dados biométricos.

3. O pessoal devidamente autorizado das autoridades competentes dos Estados-Membros, da Comissão e da eu-LISA deve ter acesso ao sistema para consultar os seguintes dados relativos ao detetor de identidades múltiplas, unicamente para efeitos da elaboração de relatórios e estatísticas, sem permitir a identificação individual:

   (a) Nacionalidade, sexo e ano de nascimento da pessoa;

(a) Tipo de documento de viagem e código de três letras do país emissor;

(b) Número de consultas efetuadas com e sem dados biométricos;

(c) Número de cada tipo de ligação.

4. O pessoal devidamente autorizado da Agência Europeia da Guarda de Fronteiras e Costeira, criada pelo Regulamento (UE) 2016/1624 do Parlamento Europeu e do Conselho[76] deve ter acesso ao sistema para consultar os dados referidos nos nºs 1, 2 e 3, para efeitos de realização de análises de risco e avaliações da vulnerabilidade, tal como referido nos artigos 11.º e 13.º do referido regulamento.

5. Para efeitos do n.º 1 do presente artigo, a eu-LISA deve conservar os dados referidos no n.º 1 do presente artigo no repositório central para a elaboração de relatórios e estatísticas, referido no capítulo VII do presente regulamento. Os dados incluídos no repositório não devem permitir a identificação de pessoas, mas devem permitir às autoridades enumeradas no n.º 1 do presente artigo obter relatórios e dados estatísticos adaptáveis para melhorar a eficiência do controlo de fronteiras, para ajudar as autoridades no tratamento dos pedidos de visto e para apoiar a definição de políticas fundamentadas em provas em matéria de migração e de segurança na União.

Artigo 57.º
Período transitório para a utilização do portal europeu de pesquisa

Durante um período de dois anos a contar da data da entrada em funcionamento do ESP, as obrigações referidas no artigo 7.º, n.º 2 e n.º 4 não são aplicáveis e a utilização dos ESP é facultativa.

Artigo 58.º

Período transitório aplicável às disposições relativas ao acesso ao repositório comum de dados de identificação para efeitos de aplicação da lei

O artigo 22.º, o artigo 55.º-B, pontos 13, 14, 15 e 16, e o artigo 55.º-E aplicam-se a partir da data de início das operações a que se refere o artigo 62.º, n.º 1.

Artigo 59.º
Período transitório para a deteção de identidades múltiplas

1. Por um período de um ano a contar da notificação pela eu-LISA da conclusão do teste referido no artigo 62.º, n.º 1, alínea b) relativo ao detetor de identidades múltiplas (MID) e antes do início do funcionamento do MID, a unidade central do ETIAS referida no [artigo 33.º, alínea a), do Regulamento (UE) 2016/1624] é responsável por efetuar uma deteção de identidades múltiplas entre os dados armazenados no VIS, no Eurodac e no SIS. As deteções de identidades múltiplas

[76] Regulamento (UE) 2016/1624 do Parlamento Europeu e do Conselho, de 14 de setembro de 2016, relativo à Guarda Europeia de Fronteiras e Costeira, que altera o Regulamento (UE) 2016/399 do Parlamento Europeu e do Conselho e revoga o Regulamento (CE) n.º 863/2007 do Parlamento Europeu e do Conselho, o Regulamento (CE) n.º 2007/2004 do Conselho e a Decisão 2005/267/CE do Conselho (JO L 251 de 16.9.2016, p. 1).

devem ser efetuadas utilizando apenas os dados biométricos em conformidade com o artigo 27.º, n.º 2, do presente regulamento.

2. Se a consulta detetar uma ou várias respostas positivas e os dados de identificação dos processos ligados forem idênticos ou similares deve ser criada uma ligação branca em conformidade com o artigo 33.º.

Se a consulta detetar uma ou várias respostas positivas e os dados de identificação dos processos ligados não puderem ser considerados similares, deve ser criada uma ligação amarela em conformidade com o artigo 30.º e aplicar-se o procedimento previsto no artigo 29.º.

Quando forem detetadas várias respostas positivas, deve ser criada uma ligação para cada elemento de dados que desencadeou a resposta positiva.

3. Sempre que for criada uma ligação amarela, o MID deve facultar acesso aos dados de identidade presentes nos diferentes sistemas de informação para a unidade central do ETIAS.

4. Quando for criada uma ligação a uma indicação no SIS, que não seja uma indicação de não admissão ou uma indicação relativa a um documento de viagem extraviado, roubado ou invalidado nos termos do artigo 24.º do Regulamento relativo ao SIS no domínio dos controlos de fronteira e do artigo 38.º do Regulamento relativo ao SIS no domínio da aplicação da lei, respetivamente, o MID deve facultar ao gabinete SIRENE do Estado-Membro que criou a indicação acesso aos dados de identidade presentes nos diferentes sistemas de informação.

5. A unidade central ETIAS ou o gabinete SIRENE do Estado-Membro que criou a indicação deve ter acesso aos dados constantes do processo de confirmação de identidade e avaliar as diferentes identidades, atualizando a ligação em conformidade com os artigos 31.º, 32.º e 33.º e adicionando-a ao processo de confirmação de identidade.

6. A eu-LISA deve apoiar, se for caso disso, a unidade central ETIAS na realização da deteção de identidades múltiplas referida no presente artigo.

Artigo 60.º
Custos

1. Os custos decorrentes da criação e funcionamento do ESP, do serviço partilhado de correspondências biométricas, do repositório comum de dados de identificação (CIR) e do MID são suportados pelo orçamento geral da União.

2. Os custos decorrentes da integração das infraestruturas nacionais existentes e respetiva ligação às interfaces uniformes nacionais, bem como decorrentes do alojamento das interfaces uniformes nacionais, são suportados pelo orçamento geral da União.

Estão excluídos os seguintes custos:

(a) Gabinete de gestão do projeto dos Estados-Membros (reuniões, missões,

gabinetes);

(b) Alojamento dos sistemas informáticos nacionais (espaço, implementação, eletricidade, refrigeração);

(c) Funcionamento dos sistemas informáticos nacionais (operadores e contratos de assistência);

(d) Conceção, desenvolvimento, implementação, funcionamento e manutenção de redes de comunicação nacionais.

3. Os custos incorridos pelas autoridades designadas referidas no artigo 4.º, n.º 24, são suportados, respetivamente, por cada Estado-Membro e pela Europol. Os custos da ligação das autoridades designadas ao CIR são suportados por cada Estado-Membro e pela Europol, respetivamente.

Artigo 61.º
Notificações

1. Os Estados-Membros devem comunicar à eu-LISA as autoridades referidas nos artigos 7.º, 20.º, 21.º e 26.º que podem utilizar ou ter acesso ao ESP, ao CIR e ao MID, respetivamente.

Deve ser publicada uma lista consolidada das referidas autoridades no *Jornal Oficial da União Europeia* dentro de um prazo de três meses a contar da data em que cada componente de interoperabilidade iniciou a sua atividade em conformidade com o artigo 62.º. Em caso de alterações à lista, a eu-LISA deve publicar uma lista consolidada e atualizada uma vez por ano.

2. A eu-LISA deve notificar à Comissão a conclusão com êxito do teste referido no artigo 62.º, n.º 1, alínea b).

3. A unidade central ETIAS deve notificar à Comissão a conclusão com êxito da medida transitória estabelecida no artigo 59.º.

4. A Comissão deve disponibilizar aos Estados-Membros e ao público, através de um sítio público constantemente atualizado, as informações comunicadas nos termos do n.º 1.

Artigo 62.º
Início das operações

1. A Comissão deve decidir a data a partir da qual cada componente de interoperabilidade entra em funcionamento, depois de estarem reunidas as seguintes condições:

(a) A adoção das medidas a que se referem o artigo 8.º, n.º 2, artigo 9.º, n.º 7, artigo 28.º, n.º 5 e n.º 6, artigo 37.º, n.º 4, artigo 38.º, n.º 4, artigo 39.º, n.º 5 e artigo 44.º, n.º 5;

(b) A eu-LISA tiver declarado a conclusão com êxito de um teste global do

componente de interoperabilidade, que deve ser efetuado pela eu-LISA em cooperação com os Estados-Membros;

(c) A eu-LISA tiver validado as disposições técnicas e jurídicas para a recolha e transmissão dos dados a que se referem os artigos 8.º, n.º 1, 13.º, 19.º, 34.º e 39.º e procedido à notificação da Comissão;

(d) Os Estados-Membros tiverem notificado a Comissão, em conformidade com o artigo 61.º, n.º 1;

(e) Para o detetor de identidades múltiplas, a unidade central ETIAS tiver notificado a Comissão, conforme referido no artigo 61.º, n.º 3.

2. A Comissão deve informar o Parlamento Europeu e o Conselho dos resultados do teste efetuado em conformidade com o n.º 1, alínea b).

3. A decisão da Comissão referida no n.º 1 é publicada no *Jornal Oficial da União Europeia*.

4. Os Estados-Membros e a Europol devem começar a utilizar os componentes de interoperabilidade a partir da data determinada pela Comissão em conformidade com o n.º 1.

Artigo 63.º
Exercício da delegação

1. É conferido à Comissão o poder de adotar atos delegados nas condições estabelecidas no presente artigo.

2. O poder de adotar os atos delegados referidos nos artigos 8.º, n.º 2 e artigo 9.º, n.º 7, é conferido à Comissão por um período de tempo indeterminado, a partir de [*data de entrada em vigor do presente regulamento*].

3. A delegação de poderes referida nos artigos 8.º, n.º 2 e artigo 9.º, n.º 7 pode ser revogada em qualquer momento pelo Parlamento Europeu ou pelo Conselho. A decisão de revogação põe termo à delegação dos poderes especificados nessa decisão. Produz efeitos no dia seguinte ao da publicação da decisão no *Jornal Oficial da União Europeia* ou numa data posterior especificada. A decisão de revogação não afeta a validade de quaisquer atos delegados já em vigor.

4. Antes de adotar um ato delegado, a Comissão deve consultar os peritos designados por cada Estado-Membro de acordo com os princípios estabelecidos no Acordo Interinstitucional «Legislar Melhor», de 13 de abril de 2016.

5. Assim que adotar um ato delegado, este deve ser simultaneamente notificado pela Comissão ao Parlamento Europeu e ao Conselho.

6. Um ato delegado adotado nos termos dos artigos 8.º, n.º 2 e 9.º, n.º 7 só entra em vigor se não tiverem sido formuladas objeções pelo Parlamento Europeu ou pelo Conselho no prazo de [dois meses] a contar da notificação desse ato ao Parlamento Europeu e ao Conselho ou se, antes do termo desse prazo, o Parlamento Europeu e o Conselho tiverem ambos informado a Comissão de que não têm objeções a formular.

O referido prazo é prorrogado por [dois meses] por iniciativa do Parlamento Europeu ou do Conselho.

Artigo 64.º
Procedimento de comité

1. A Comissão é assistida por um comité. Este comité deve ser entendido como um comité na aceção do Regulamento (UE) n.º 182/2011.

2. Sempre que se faça referência ao referido número, aplica-se o artigo 5.º do Regulamento (UE) n.º 182/2011.

Artigo 65.º
Grupo consultivo

A eu-LISA deve criar um grupo consultivo para lhe fornecer conhecimentos especializados relacionados com a interoperabilidade, em especial no contexto da elaboração do seu programa de trabalho anual e do relatório anual de atividades. Durante a fase de conceção e desenvolvimento dos instrumentos de interoperabilidade, deve aplicar-se o artigo 52.º, n.º 4 a n.º 6.

Artigo 66.º
Formação

A eu-LISA deve realizar tarefas relacionadas com a prestação de formação sobre a utilização técnica dos componentes de interoperabilidade em conformidade com o Regulamento (UE) n.º 1077/2011.

Artigo 67.º
Manual prático

A Comissão, em estreita cooperação com os Estados-Membros, com a eu-LISA e com outros organismos relevantes, deve disponibilizar um manual prático para a execução e a gestão dos componentes de interoperabilidade. O manual prático deve fornecer orientações técnicas e operacionais, recomendações e boas práticas. A Comissão deve adotar o manual prático sob a forma de recomendação.

Artigo 68.º
Acompanhamento e avaliação

1. A eu-LISA deve assegurar que são criados procedimentos para acompanhar o desenvolvimento de componentes de interoperabilidade à luz dos objetivos relacionados com o planeamento e custos e controlar o funcionamento dos componentes de interoperabilidade à luz dos objetivos fixados em termos de resultados técnicos, relação custo-eficácia, segurança e qualidade do serviço.

2. Até [*seis meses após a entrada em vigor do presente regulamento* — o OPOCE, queira por favor substituir pela data real] e, posteriormente, de seis em seis meses, durante a fase de desenvolvimento dos componentes de interoperabilidade, a eu-LISA deve apresentar um relatório ao Parlamento Europeu e ao Conselho sobre o ponto da situação do desenvolvimento dos componentes de interoperabilidade. Quando o desenvolvimento estiver concluído, deve ser apresentado um relatório ao Parlamento Europeu e ao Conselho a explicar em pormenor a forma como os objetivos, em especial os objetivos relacionados com o planeamento e custos, foram alcançados, justificando igualmente eventuais divergências.

3. Para efeitos de manutenção técnica, a eu-LISA deve ter acesso às informações necessárias respeitantes às operações de tratamento de dados efetuadas nos componentes de interoperabilidade.

4. Quatro anos após o início do funcionamento de cada componente de interoperabilidade e posteriormente de quatro em quatro anos, a eu-LISA deve apresentar ao Parlamento Europeu, ao Conselho e à Comissão um relatório sobre o funcionamento técnico dos componentes de interoperabilidade, incluindo sobre a sua segurança.

5. Além disso, um ano após cada relatório da eu-LISA, a Comissão deve apresentar uma avaliação global dos componentes, incluindo uma:

   (a) Avaliação da aplicação do presente regulamento;

   (b) Uma análise dos resultados obtidos comparativamente aos objetivos fixados e ao impacto nos direitos fundamentais;

   (c) Avaliação da continuidade da validade dos princípios subjacentes aos componentes de interoperabilidade;

   (d) Avaliação da segurança dos componentes de interoperabilidade;

   (e) Avaliação de quaisquer implicações, incluindo qualquer impacto desproporcionado no fluxo de tráfego nos pontos de passagem de fronteira e as implicações de um impacto orçamental sobre o orçamento da União.

   As avaliações devem incluir quaisquer recomendações necessárias. A Comissão deve transmitir o relatório de avaliação ao Parlamento Europeu, ao Conselho, à Autoridade Europeia para a Proteção de Dados e à Agência dos Direitos Fundamentais da União Europeia, criada pelo Regulamento (CE) n.º 168/2007 do Conselho[77].

6. Os Estados-Membros e a Europol devem fornecer à eu-LISA e à Comissão as informações necessárias para a elaboração dos relatórios referidos nos nºs 4 e 5. Estas informações não podem pôr em causa os métodos de trabalho, nem incluir informações que revelem fontes, membros do pessoal ou investigações das autoridades designadas.

[77] Regulamento (CE) n.º 168/2007 do Conselho, de 15 de fevereiro de 2007, que cria a Agência dos Direitos Fundamentais da União Europeia (JO L 53 de 22.2.2007, p. 1).

7. A eu-LISA deve comunicar à Comissão as informações necessárias à elaboração das avaliações referidas no n.º 5.

8. Respeitando as disposições de direito nacional sobre a publicação de informações sensíveis, cada Estado-Membro e a Europol devem elaborar relatórios anuais sobre a eficácia do acesso aos dados armazenados no repositório comum de dados de identificação para efeitos de aplicação da lei, contendo informações e estatísticas sobre:

   (a) A finalidade exata da consulta, incluindo o tipo de infração terrorista ou crime grave;

   (b) Motivos razoáveis apresentados de suspeita fundamentada de que o suspeito, autor ou vítima está abrangido pelo [Regulamento SES], o Regulamento VIS ou o [Regulamento ETIAS];

   (c) O número de pedidos de acesso ao repositório comum de dados de identificação para efeitos de aplicação da lei;

   (d) O número e tipo de casos que resultaram em identificações positivas;

   (e) A necessidade e utilização feitas dos casos de urgência excecional, incluindo os casos em que essa urgência não foi aceite pela verificação *ex post* realizada pelo ponto central de acesso.

   Os relatórios anuais dos Estados-Membros e da Europol devem ser transmitidos à Comissão até 30 de junho do ano seguinte.

Artigo 69.º
Entrada em vigor e aplicabilidade

O presente regulamento entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável nos Estados-Membros em conformidade com os Tratados.

Feito em Estrasburgo, em

Pelo Parlamento Europeu	*Pelo Conselho*
O Presidente	*O Presidente*

FICHA FINANCEIRA LEGISLATIVA

1. CONTEXTO DA PROPOSTA/INICIATIVA

1.1. Título da proposta/iniciativa

1.2. Domínio(s) de intervenção abrangido(s)

1.3. Natureza da proposta/iniciativa

1.4. Objetivo(s)

1.5. Justificação da proposta/iniciativa

1.6. Duração e impacto financeiro

1.7. Modalidade(s) de gestão prevista(s)

2. MEDIDAS DE GESTÃO

2.1. Regras de controlo e comunicação

2.2. Sistema de gestão e de controlo

2.3. Medidas de prevenção de fraudes e irregularidades

3. IMPACTO FINANCEIRO ESTIMADO DA PROPOSTA/INICIATIVA

3.1. Rubrica(s) do quadro financeiro plurianual e rubrica(s) orçamental(is) de despesas envolvida(s)

3.2. Impacto estimado nas despesas

3.2.1. Síntese do impacto estimado nas despesas

3.2.2. Impacto estimado nas dotações operacionais

3.2.3. Impacto estimado nas dotações de natureza administrativa

3.2.4. Compatibilidade com o atual quadro financeiro plurianual

3.2.5. Participação de terceiros no financiamento

3.3. Impacto estimado nas receitas

FICHA FINANCEIRA LEGISLATIVA

1. CONTEXTO DA PROPOSTA/INICIATIVA

1.1. Título da proposta/iniciativa

Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece a interoperabilidade entre os sistemas de informação da União Europeia para a segurança, a gestão das fronteiras e migrações.

1.2. Domínio(s) de intervenção abrangido(s)

Assuntos Internos (título 18)

1.3. Natureza da proposta/iniciativa

X A proposta/iniciativa refere-se a **uma nova ação**

☐ A proposta/iniciativa refere-se a **uma nova ação na sequência de um projeto-piloto/ação preparatória**[78]

☐ A proposta/iniciativa refere-se **à prorrogação de uma ação existente**

☐ A proposta/iniciativa refere-se a **uma ação reorientada para uma nova ação**

1.4. Objetivo(s)

1.4.1. Objetivo(s) estratégico(s) plurianual(is) da Comissão visado(s) pela proposta/iniciativa

Gestão das fronteiras — salvar vidas e garantir a segurança das fronteiras externas

Os componentes de interoperabilidade criam a oportunidade de melhor utilizar as informações contidas nos sistemas existentes da UE para a segurança e gestão das fronteiras e da migração. Estas medidas evitam sobretudo que a mesma pessoa seja registada em diferentes sistemas com diferentes identidades. Atualmente, a identificação única de uma pessoa é possível dentro de um determinado sistema, mas não entre os sistemas. Isto pode conduzir a decisões erradas tomadas pelas autoridades ou então pode ser aproveitado por viajantes de má fé para ocultar a sua verdadeira identidade.

Melhor intercâmbio de informações

As medidas propostas preveem igualmente um procedimento de acesso simplificado mas ainda assim delimitado dos serviços de aplicação da lei a estes dados. Mas, ao contrário do que acontece atualmente, existe um conjunto único de condições em vez de conjuntos diferentes para acesso a cada compilação de dados.

[78] Tal como referido no artigo 54.º, n.º 2, alínea a), ou b), do Regulamento Financeiro.

1.4.2. Objetivo(s) específico(s) e objetivo específico n.º [ ]

A criação de componentes de interoperabilidade tem os seguintes objetivos gerais:

(a) Melhorar a gestão das fronteiras externas;

(b) Contribuir para a prevenção e combate contra a migração irregular; e

(c) Contribuir para um elevado nível de segurança no espaço de liberdade, segurança e justiça da União, incluindo a manutenção da segurança pública e da ordem pública e a salvaguarda da segurança nos territórios dos Estados-Membros.

Os objetivos de interoperabilidade são alcançados mediante:

a) A garantia da identificação correta das pessoas;

b) O contributo para combater a fraude de identidade;

c) A melhoria e harmonização dos requisitos de qualidade dos dados dos respetivos sistemas de informação da UE;

d) A facilitação da aplicação, por parte dos Estados-Membros, dos aspetos técnicos e operacionais dos sistemas de informação da UE atuais e futuros;

e) O reforço, a simplificação e tornando mais uniformes as condições de segurança e de proteção dos dados que regem os respetivos sistemas de informação da UE;

f) A simplificação e uniformização das condições de acesso das autoridades responsáveis pela aplicação da lei ao SES, ao VIS, ao ETIAS e ao Eurodac;

g) O apoio aos objetivos dos sistemas SES, VIS, ETIAS, Eurodac, SIS e ECRIS-TCN.

Atividade(s) ABM/ABB em causa

Capítulo Segurança e Proteção das Liberdades: Segurança Interna

1.4.3. Resultados e impacto esperados

Especificar os efeitos que a proposta/iniciativa poderá ter nos beneficiários/na população visada.

Os objetivos gerais desta iniciativa resultam dos dois objetivos consagrados no Tratado:

1. Melhorar a gestão das fronteiras externas do espaço Schengen, tendo por base a Agenda Europeia da Migração e as comunicações subsequentes, incluindo a comunicação relativa à preservação e reforço do espaço Schengen.

2. Contribuir para a segurança interna da União Europeia, tendo por base a Agenda Europeia para a Segurança e o trabalho da Comissão rumo a uma União da Segurança genuína e eficaz.

Os objetivos políticos específicos desta iniciativa sobre interoperabilidade são os seguintes:

Os objetivos específicos da presente proposta consistem em:

1. Assegurar que os utilizadores finais, nomeadamente os guardas de fronteira, agentes com funções coercivas, agentes dos serviços de imigração e autoridades judiciais têm **acesso rápido, contínuo, sistemático e controlado** às informações de que necessitam para desempenhar as suas funções;

2. Encontrar uma solução para detetar identidades múltiplas ligadas ao mesmo conjunto de dados biométricos, com o duplo objetivo de garantir a identificação correta das pessoas de boa-fé e combater a fraude de identidade;

3. Facilitar os controlos de identidade de nacionais de países terceiros, no território de um Estado-Membro, por parte das autoridades policiais; e

4. Facilitar e agilizar o acesso das autoridades de aplicação da lei aos sistemas de informação com finalidades não coercivas a nível da UE, sempre que tal for necessário para efeitos de prevenção, investigação, deteção ou repressão de formas graves de criminalidade e terrorismo.

Para cumprir o objetivo específico 1, será desenvolvido o portal europeu de pesquisa (ESP).

Para cumprir o objetivo específico 2, será implementado o detetor de identidades múltiplas (MID), com o apoio do repositório comum de dados de identificação (CIR) e o serviço partilhado de correspondências biométricas (BMS).

Para cumprir o objetivo específico 3, funcionários autorizados terão acesso ao CIR para efeitos de identificação.

A fim de atingir o objetivo 4 o CIR conterá uma funcionalidade indicadora de resposta positiva, que irá permitir uma abordagem em duas fases para o acesso para fins de aplicação da lei aos sistemas de gestão das fronteiras.

Além destes quatro componentes de interoperabilidade, os objetivos descritos na secção 1.4.2 serão ainda apoiados pela criação e governação do Formato de Mensagem Universal (UMF) como uma norma da UE para o desenvolvimento dos sistemas de informação no domínio da justiça e dos assuntos internos, bem como a criação de um repositório comum para a elaboração de relatórios e estatísticas (CRRS).

1.4.4. Indicadores de resultados e impacto

Especificar os indicadores que permitem acompanhar a execução da proposta/iniciativa.

Cada uma das medidas propostas exige o desenvolvimento, seguido da manutenção e funcionamento desse componente.

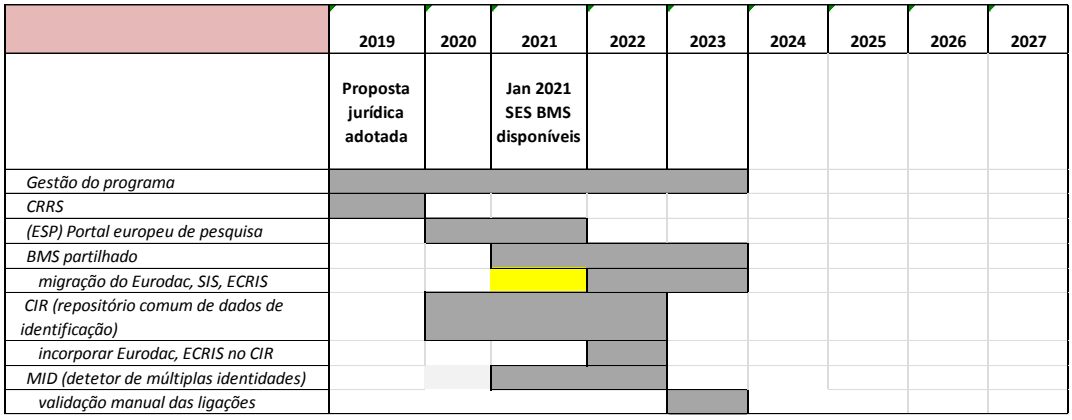
Durante a fase de desenvolvimento

O desenvolvimento de cada componente será feito logo que os pré-requisitos estejam preenchidos, ou seja, a proposta legislativa seja adotada pelos colegisladores e preenchidos os pré-requisitos técnicos, uma vez que alguns componentes só podem ser construídos depois de estar disponível outro componente.

Objetivo específico: apto a entrar em funcionamento até a data limite pretendida

Até ao final de 2017, a proposta é enviada aos colegisladores para a sua adoção. Presume-se que o processo de adoção esteja concluído durante 2018, por analogia com o tempo necessário para as outras propostas.

Com base neste pressuposto, o início do período de desenvolvimento fica definido no início de 2019 (= T0) a fim de dispor de um ponto de referência a partir do qual são contabilizados os períodos de tempo e não prazos absolutos. Se a adoção pelos colegisladores ocorrer em data posterior, todo o calendário varia em conformidade. Por outro lado, o BMS tem de estar disponível antes que o CIR e o MID possam estar concluídos. As durações de desenvolvimento estão indicadas no quadro infra:



(Bloco a amarelo refere-se a uma tarefa específica relacionada com o Eurodac.)

- Repositório comum para a elaboração de relatórios e estatísticas (CRRS): data prevista: T0 +12 meses (2019-2020)

- Portal europeu de pesquisa (ESP): data prevista: T0 +36 meses (2019-2021)

- Serviço partilhado de correspondências biométricas (BMS partilhado) é criado em primeiro lugar para fornecer o Sistema de Entrada/Saída (SES). Quando esta etapa é atingida, as aplicações que irão utilizar o BMS têm de ser atualizadas e os dados contidos no sistema automático de identificação dactiloscópica (AFIS) do SIS, o AFIS da Eurodac e os dados do ECRIS-TNS têm de migrar para o BMS. A data prevista de conclusão é o final de 2023.

- O repositório comum de dados de identificação (CIR) é criado primeiramente durante a implementação do SES. Depois de concluído o SES, os dados provenientes do Eurodac e ECRIS são incorporados no CIR. A data prevista de conclusão é o final de 2022 (disponibilidade do BMS partilhado +12 meses).

- O detetor de identidades múltiplas (MID) é criado depois de o CIR estar operacional. A data prevista de conclusão é o final de 2022 (disponibilidade do BMS +24 meses), mas existe um período com elevada ocupação de recursos para validação de ligações entre as identidades que são propostas pelo MID. Cada uma das ligações estimadas deve ser validada manualmente. Esta etapa estende-se até ao final de 2023.

O período operacional começa quando o período de desenvolvimento referido acima estiver concluído.

Operações

Os indicadores relacionados com cada objetivo específico referido no ponto 1.4.3 são as seguintes:

1. Objetivo específico: Acesso rápido, contínuo e sistemático a fontes de dados autorizadas

- Número de casos de utilização executados (= número de consultas que podem ser manuseadas pelo ESP) por período de tempo.

- Número de consultas manuseadas pelo ESP em comparação com o número total de consultas (através do ESP e sistemas diretamente) por período de tempo.

2. Objetivo específico: Deteção de identidades múltiplas

- O número de identidades ligado ao mesmo conjunto de dados biométricos em comparação com o número de identidades com dados biográficos por período de tempo.

- O número de casos detetados de fraude de identidade em comparação com o número de identidades ligadas e o número total das identidades por período de tempo.

3. Objetivo específico: Facilitar a identificação de nacionais de países terceiros

- O número de controlos de identidade realizados em comparação com o número total de operações por período.

4. Objetivo específico: Simplificar o acesso às fontes de dados autorizadas para efeitos de aplicação da lei

- O número de acessos «etapa 1» (= uma verificação da presença de dados) para efeitos de aplicação da lei por período de tempo.

- Número de acessos «etapa 2» (= consulta efetiva de dados dos sistemas da UE dentro do âmbito) para efeitos de aplicação da lei por período de tempo.

5. Objetivo transversal, suplementar: Melhorar a qualidade dos dados e a utilização de dados para uma melhor elaboração das políticas

— A emissão regular de relatórios de monitorização da qualidade dos dados.

— O número de pedidos de informação estatística *ad hoc* por período de tempo.

1.5. Justificação da proposta/iniciativa

1.5.1. Necessidade(s) a satisfazer a curto ou a longo prazo

Tal como demonstrado na avaliação de impacto que acompanha a presente proposta legislativa, os respetivos componentes propostos são necessários para alcançar a interoperabilidade:

• Para cumprir o objetivo de proporcionar aos utilizadores autorizados um acesso rápido, contínuo, sistemático e controlado aos sistemas de informação relevantes deve ser criado um portal europeu de pesquisa (ESP) assente num BMS para lidar com todas as bases de dados.

• Para cumprir o objetivo de facilitar os controlos de identidade de nacionais de países terceiros, no território de um Estado-Membro, por agentes autorizados, é necessário criar um repositório comum de dados de identificação (CIR), contendo o conjunto mínimo de dados de identificação e assente no mesmo BMS.

• Para cumprir o objetivo de deteção de identidades múltiplas ligadas ao mesmo conjunto de dados biométricos, com o duplo objetivo de facilitar os controlos de identidade para viajantes de boa-fé e combater a fraude de identidade, deve ser criado um detetor de identidades múltiplas (MID) com ligações entre identidades múltiplas entre os sistemas.

• Para cumprir o objetivo de facilitação e simplificação do acesso das autoridades de aplicação da lei aos sistemas de informação não relacionados com a aplicação da lei para efeitos de prevenção, investigação, deteção ou repressão de crimes graves e de terrorismo, deve ser incluída uma funcionalidade «hit-flagging» (indicadora de resposta positiva) no repositório comum de dados de identificação (CIR).

Uma vez que todos os objetivos devem ser cumpridos, a solução completa é a combinação do ESP, do CIR (com indicadores de respostas positivas) e do MID, todos assentes no BMS.

1.5.2. Valor acrescentado da intervenção da União (pode decorrer de diferentes fatores, nomeadamente ganhos em termos de coordenação, certeza jurídica, maior eficácia

ou complementaridades). Para efeitos do presente ponto, por «valor acrescentado da intervenção da União» é o valor resultante da intervenção da União, que se acrescenta ao valor que teria sido criado, de contrário, apenas pelos Estados-Membros individualmente.

É necessário intervir a nível europeu, porque os sistemas que se propõe tornar interoperáveis, são sistemas utilizados por vários Estados-Membros: seja por todos os Estados-Membros (no caso do Eurodac) ou todos os Estados-Membros que fazem parte do espaço Schengen (no caso do SES, VIS, ETIAS e SIS). Por definição, as ações não podem pura e simplesmente ser tomadas a outro nível.

O principal valor acrescentado esperado reside na eliminação dos casos de fraude de identidade, identificar os casos em que uma pessoa tenha utilizado diferentes identidades para entrar na UE e evitar que pessoas de boa-fé sejam confundidas com pessoas de má fé com o mesmo nome. Um valor acrescentado adicional reside na maior facilidade de implementação e manutenção de sistemas informáticos de grande escala permitida pela interoperabilidade presentemente proposta. Para os serviços de aplicação da lei, as medidas propostas deveriam resultar num acesso mais frequente e bem-sucedido a dados específicos no âmbito dos sistemas informáticos europeus de grande escala. A nível operacional, a qualidade dos dados só pode ser mantida e melhorada se for controlada. Além disso, para a elaboração de políticas e tomada de decisões, há a necessidade de fazer com que seja possível proceder a consultas *ad hoc* de dados anonimizados.

Uma análise dos custos-benefícios é parte integrante da avaliação de impacto e tendo apenas em conta os benefícios suscetíveis de ser quantificados, os benefícios esperados podem ser razoavelmente estimados em cerca de 77,5 milhões de euros por ano e beneficiam, principalmente, os Estados-Membros. Estes benefícios decorrem essencialmente de:

- Redução dos custos das alterações nas aplicações nacionais quando o sistema central esteja operacional (estimado em 6 milhões de euros por ano para os serviços informáticos de cada Estado-Membro);

- Redução de custos derivada da disponibilidade de um BMS central em vez de um BMS por sistema central contendo dados biométricos (estimado em 1,5 milhões de euros por ano, e uma poupança única de 8 milhões de euros para a eu-LISA).

- Custos poupados em identificação de identidades múltiplas comparativamente com a situação em que o mesmo resultado seria alcançado sem os meios propostos. Este fator representaria uma poupança de, pelo menos, 50 milhões de euros por ano para as administrações dos Estados-Membros, para a gestão das fronteiras, a migração e a aplicação da lei.

- Custos de formação poupados para um grande grupo de utilizadores finais em comparação com uma situação em que a formação é necessária numa base recorrente, estimados em 20 milhões de euros por ano para as administrações dos Estados-Membros para a gestão das fronteiras, migração e aplicação da lei.

1.5.3. Lições tiradas de experiências anteriores semelhantes

A experiência adquirida com o desenvolvimento de Schengen de segunda geração (SIS II) e do Sistema de Informação sobre Vistos (VIS) revelou os seguintes ensinamentos:

1. Como possível salvaguarda contra derrapagens orçamentais e atrasos resultantes da alteração dos requisitos, qualquer novo sistema de informação no domínio da liberdade, segurança e justiça, em especial se envolver um sistema informático de grande escala, não deve ser desenvolvido antes de definitivamente adotados os instrumentos jurídicos de base que definem o seu objeto, âmbito, funções e características técnicas.

2. Para o SIS II e o VIS, o desenvolvimento nacional nos Estados-Membros podia ser cofinanciado no âmbito do Fundo para as Fronteiras Externas (FFE), mas não seria obrigatório. Não foi possível ter uma visão geral do nível de progresso naqueles Estados-Membros que não tinham previsto as ações correspondentes na sua programação plurianual ou cuja programação não era suficientemente rigorosa. Por conseguinte, propõe-se agora que a Comissão reembolse todas as despesas de integração suportadas pelos Estados-Membros, a fim de poder supervisionar o progresso destes desenvolvimentos.

3. Tendo em vista facilitar a coordenação geral da execução, todas as propostas de intercâmbio de mensagens entre sistemas nacionais e centrais deve reutilizar as redes existentes e a interface uniforme nacional.

1.5.4. Compatibilidade e eventual sinergia com outros instrumentos adequados

Compatibilidade com o atual QFP

O Regulamento relativo ao FSI-Fronteiras é o instrumento financeiro no qual o orçamento destinado à implementação da iniciativa de interoperabilidade foi incluído.

No seu artigo 5.º, alínea b), prevê a aplicação de 791 milhões de EUR através de um programa para o desenvolvimento de sistemas informáticos, com base em sistemas informáticos existentes e/ou novos, de apoio à gestão dos fluxos migratórios nas fronteiras externas, sob reserva da adoção dos atos legislativos pertinentes da União e nos termos do artigo 15.º. Deste montante de 791 milhões de euros, 480,2 milhões de euros estão reservados ao desenvolvimento do SES, 210 milhões de euros para o ETIAS e 67,9 milhões de euros para a revisão do SIS II. O restante (32,9 milhões de euros) deverá ser reafetado através dos mecanismos do FSI-Fronteiras. A atual proposta prevê 32,1 milhões de euros para o atual período do quadro financeiro plurianual, coadunando-se com o orçamento restante.

A atual proposta prevê um orçamento total de 424,7 milhões de euros (rubrica 5) durante o período de 2019 a 2027. O atual QFP apenas abrange o período de dois anos de 2019 e 2020. Os custos foram, no entanto, estimados até 2027 inclusive para dar uma opinião informada sobre as consequências financeiras da presente proposta e sem prejuízo do próximo quadro financeiro plurianual.

O orçamento solicitado pelo período de nove anos ascende a 424,7 milhões de euros, sendo também focados os seguintes pontos:

1) 136,3 milhões de euros para os Estados-Membros cobrirem as alterações nos seus sistemas nacionais, a fim de utilizar os componentes de interoperabilidade, a IUN fornecida pela eu-LISA e um orçamento para a formação da comunidade de utilizadores finais substancial. Não haverá qualquer impacto sobre o financiamento do atual QFP já que o financiamento é concedido a partir de 2021.

2) 4,8 milhões de euros para a Agência GEFC, para acolher uma equipa de especialistas que, durante um ano (2023) validará as ligações entre identidades a partir do momento em que o MID entrar em ação. As atividades da equipa podem ser associadas à desambiguação da identidade conforme atribuído à Agência GEFC sob proposta do ETIAS. Não haverá qualquer impacto sobre o financiamento do atual QFP já que o financiamento é concedido a partir de 2021.

3) 48,9 milhões de euros para a Europol, para cobrir a atualização dos sistemas informáticos da Europol para o volume de mensagens a tratar e o reforço do seu nível de desempenho. Os componentes de interoperabilidade serão utilizados pelo ETIAS tendo em vista a consulta dos dados da Europol. No entanto, a capacidade atual de tratamento de informações da Europol não é conforme com os volumes substanciais (média de 100 000 pedidos de informações por dia) e menor tempo de resposta. 9,1 milhões de euros despendidos no atual QFP.

4) 2,0 milhões de euros para a CEPOL, para cobrir a preparação e realização de ações de formação para o pessoal operacional. 0,1 milhões de euros estão previstos em 2020.

5) 225,0 milhões de euros para a eu-LISA, que cobre o custo total do desenvolvimento do programa que fornece as cinco componentes de interoperabilidade (68,3 milhões de euros), os custos de manutenção a partir do momento em que os componentes sejam entregues até 2027 (56,1 milhões de euros), um orçamento específico de 25,0 milhões de euros para a migração dos dados dos sistemas existentes para o BMS e os custos adicionais para a atualização das IUN, rede, formação e reuniões. Um orçamento específico de 18,7 milhões de euros cobre o custo de modernização e de funcionamento do ECRIS-TNC em modo de alta disponibilidade a partir de 2022. Deste montante total, 23,0 milhões de euros são gastos no âmbito do atual QFP.

6) 7,7 milhões de euros para a DG Migração e Assuntos Internos, a fim de cobrir um aumento limitado do pessoal e custos conexos durante o período de desenvolvimento das diferentes componentes, dado que a Comissão também assumirá a responsabilidade pelo comité para o UMF (Formato de Mensagem Universal). Este orçamento, que se enquadra na rubrica 5, não é suportado pelo orçamento do FSI. A título informativo, são devidos 2,0 milhões de euros ao longo do período 2019-2020.

Compatibilidade com iniciativas anteriores

A presente iniciativa é compatível com as seguintes:

Em abril de 2016, a Comissão apresentou uma **Comunicação sobre *Sistemas de informação mais sólidos e mais inteligentes para controlar as fronteiras e garantir a segurança*** que aborda uma série de lacunas estruturais relacionadas com os sistemas de informação. Esta apresentação deu origem a três ações:

Em primeiro lugar, a Comissão **tomou medidas para reforçar e maximizar os benefícios dos sistemas de informação existentes**. Em dezembro de 2016, a Comissão adotou propostas para um maior reforço do atual Sistema de Informação Schengen (SIS). Entretanto, na sequência da proposta da Comissão de maio de 2016, foram aceleradas as negociações sobre a base jurídica revista para o Eurodac — a base de dados dactiloscópicos da UE para requerentes de asilo. Encontra-se igualmente em preparação uma nova base jurídica para o Sistema de Informação sobre Vistos (VIS), que será apresentada no segundo trimestre de 2018.

Em segundo lugar, a Comissão propôs **sistemas de informação adicionais para resolver lacunas identificadas** na arquitetura de gestão de dados da UE. As negociações sobre a proposta da Comissão de abril de 2016 no sentido de estabelecer um Sistema de Entrada/Saída (SES)[79] – para melhorar os procedimentos de controlo nas fronteiras para os nacionais de países terceiros que viajam para a UE — foram concluídas logo em julho de 2017, os colegisladores chegaram a um acordo político, confirmado pelo Parlamento Europeu em outubro de 2017 e formalmente adotado pelo Conselho em novembro de 2017. Em novembro de 2016, a Comissão também apresentou uma proposta para a criação de um Sistema Europeu de Informação e Autorização de Viagem (ETIAS)[80]. Esta proposta tem por objetivo reforçar os controlos de segurança aplicáveis aos viajantes isentos da obrigação de visto, permitindo controlos prévios em matéria de migração irregular e de segurança. Está atualmente em fase de negociação pelos colegisladores. Em junho de 2017, foi igualmente proposto o Serviço Europeu de Informação sobre os Registos Criminais de nacionais de países terceiros (sistema ECRIS-TCN)[81] para colmatar a lacuna identificada no que se refere à troca de informações entre os Estados-Membros sobre os nacionais de países terceiros condenados

Em terceiro lugar, a Comissão trabalhou **no sentido de assegurar a interoperabilidade dos sistemas de informação**, centrada nas seguintes quatro opções apresentadas na Comunicação de abril de 2016[82], com vista a concretizar a interoperabilidade. Três das quatro opções são precisamente o ESP, o CIR e o BMS. Posteriormente tornou-se clara a necessidade de efetuar uma distinção entre o CIR, enquanto base de dados de identidades e um novo elemento que identifica identidades múltiplas ligadas a um mesmo identificador biométrico (MID). Assim, os quatro componentes são agora: o ESP, o CIR, o MID e o BMS.

Sinergia

Neste contexto, sinergia é entendido como o benefício alcançado pela reutilização das soluções existentes e evitando novos investimentos em todo o sistema.

[79] COM(2016)194 de 6 de abril de 2016.
[80] COM(2016)731 de 16 de novembro de 2016.
[81] COM(2017)344 de 29 de junho de 2017.
[82] COM(2016)205 de 6 de abril de 2016.

Existe uma maior sinergia entre estas iniciativas e o desenvolvimento do SES e do ETIAS.

Para o funcionamento do SES, é criado um processo individual para todos os nacionais de países terceiros que entram no espaço Schengen para uma estada de curta duração. Para o efeito, o atual sistema de correspondências biométricas utilizadas para o VIS, que contêm os modelos de impressões digitais para todos os viajantes sujeitos a obrigação de visto, será alargado de modo a abranger igualmente os dados biométricos dos viajantes isentos da obrigação de visto. O BMS consiste assim, conceptualmente, numa generalização do dispositivo de busca de dados biométricos, que será elaborada enquanto parte do SES. Irá proceder-se à migração (este é o termo técnico quando os dados são transferidos de um regime para outro) dos modelos biométricos contidos no dispositivo de busca de dados biométricos do SIS e do Eurodac para o BMS. Segundo o fornecedor, o armazenamento em bases de dados separadas custa, em média, 1 EUR por conjunto biométrico (existem potencialmente 200 milhões de conjuntos de dados no total), enquanto o custo médio diminui para 0,35 EUR por conjunto biométrico quando é criada uma solução BMS. Os custos mais elevados sobre o «hardware» necessário para um elevado volume de dados compensa parcialmente estas prestações, mas, no final de contas, o custo do BMS é estimado em menos 30 % do que quando os mesmos dados são armazenados em múltiplos sistemas BMS mais pequenos.

Para o funcionamento do ETIAS, deve estar disponível um componente para consulta de um conjunto de sistemas da UE. Ou é utilizado o ESP ou é concebido um componente específico como parte do ESP. A proposta de interoperabilidade permite a construção de um componente, em vez de dois.

Gera-se também uma sinergia através da reutilização da mesma interface uniforme nacional (IUN) que é utilizada para o SES e para o ETIAS. A IUN terá de ser atualizada, mas continuará a ser utilizada.

1.6. Duração e impacto financeiro

☐ Proposta/iniciativa de **duração limitada**

– ☐ Proposta/iniciativa com efeitos entre [DD/MM] AAAA e [DD/MM] AAAA

– ☐ Impacto financeiro entre AAAA e AAAA

☒ Proposta/iniciativa de **duração ilimitada**

– Incluindo o período de desenvolvimento entre 2019 e 2023, seguido de um período de funcionamento em pleno.

– Por conseguinte, é apresentada a duração do impacto financeiro de 2019 a 2027.

1.7. Modalidade(s) de gestão prevista(s)[83]

☒ **Gestão direta** por parte da Comissão

– X por parte dos seus serviços, incluindo do seu pessoal nas delegações da União;

– ☐ por parte das agências de execução

☒ **Gestão partilhada** com os Estados-Membros

☒ **Gestão indireta** confiando tarefas de execução orçamental a:

– ☐ países terceiros ou a organismos por estes designados;

– ☐ organizações internacionais e respetivas agências (a especificar);

– ☐ao BEI e ao Fundo Europeu de Investimento;

– ☒ aos organismos referidos nos artigos 208.º e 209.º do Regulamento Financeiro;

– ☐ a organismos de direito público;

– ☐ a organismos regidos pelo direito privado com uma missão de serviço público na medida em que prestem garantias financeiras adequadas;

– ☐ organismos regidos pelo direito privado de um Estado-Membro a quem é confiada a implementação de uma parceria público-privada e que prestem garantias financeiras adequadas;

– ☐ pessoas encarregadas da implementação de ações específicas no quadro da PESC por força do título V do Tratado da União Europeia e identificadas no ato de base relevante.

– *Se for indicada mais de uma modalidade de gestão, queira especificar na secção «Observações».*

Observações

[83] Os pormenores sobre as modalidades de gestão e as referências ao Regulamento Financeiro estão disponíveis no sítio BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

Blocos	Fase de desenvolvimento	Fase de funcionamento	Modalidade de gestão	Ator
Desenvolvimento e manutenção (dos componentes de interoperabilidade para os sistemas centrais, formação para o sistema)	X	X	Indireta	eu-LISA Europol CEPOL
Migração de dados (migração de modelos biométricos para o BMS), custos de rede, atualização das IUN, reuniões e formação	X	X	Indireta	eu-LISA
Validação das ligações ao criar o MID	X	-	Indireta	GEFC
Adaptação das IUN, integração dos sistemas nacionais e formação dos utilizadores finais	X	X	Partilhada (ou direta) (1)	COM + Estados-Membros

(1) Não há montantes para a fase de funcionamento incluídos no presente instrumento.

O período de desenvolvimento tem início em 2019 e prolonga-se até à entrega de cada componente, decorrendo de 2019 a 2023 (ver ponto 1.4.4).

1. Gestão direta pela DG MIGRAÇÃO E ASSUNTOS INTERNOS: Durante o período de desenvolvimento, se necessário, as ações podem ser executadas diretamente pela Comissão. Tal poderia incluir, nomeadamente, o apoio financeiro da União a favor das atividades sob a forma de subvenções (incluindo subvenções às autoridades nacionais dos Estados-Membros), contratos públicos e/ou o reembolso dos custos incorridos por peritos externos.

2. Gestão partilhada: Durante a fase de desenvolvimento, os Estados-Membros serão obrigados a adaptar os seus sistemas nacionais para ter acesso ao ESP em vez de sistemas individuais (isto é para o envio de mensagens provenientes dos Estados-Membros) e alterações às respostas dos seus pedidos de consulta (as mensagens recebidas pelos Estados-Membros). Será também realizada uma atualização das IUN existentes, implementada para o SES e ETIAS.

3. Gestão indireta: A eu-LISA abrangerá a parte relativa ao desenvolvimento de todos os componentes do projeto informático, ou seja, os componentes de interoperabilidade, a atualização da interface uniforme nacional (IUN) em cada Estado-Membro, a atualização da infraestrutura de comunicações entre os sistemas centrais e as interfaces uniformes nacionais, a migração de modelos biométricos a partir dos atuais sistemas de busca de dados biométricos do SIS e Eurodac para o BMS e a atividade de limpeza de dados associada.

Durante o período de operações, a eu-LISA executa todas as atividades técnicas ligadas à manutenção dos componentes.

A Agência Europeia da Guarda de Fronteiras e Costeira (GEFC) integrará uma equipa suplementar dedicada à validação das ligações a partir do momento em que o MID é colocado em serviço. Trata-se de uma tarefa de duração limitada.

A Europol cobrirá o desenvolvimento e manutenção dos seus sistemas a fim de garantir a interoperabilidade com o ESP e o ETIAS.

A CEPOL prepara e presta formação aos serviços operacionais segundo uma abordagem de formação de formadores.

2. MEDIDAS DE GESTÃO

2.1. Regras de controlo e comunicação

Especificar a periodicidade e as condições.

As regras de controlo e de comunicação com vista ao desenvolvimento e manutenção de outros sistemas:

1. A eu-LISA deve assegurar que são criados procedimentos para acompanhar o desenvolvimento de componentes de interoperabilidade, tendo em conta os objetivos de planeamento e custos, bem como para acompanhar o funcionamento dos componentes tendo em conta os objetivos em termos de resultados técnicos, custo-eficácia, segurança e qualidade do serviço.

2. No prazo de seis meses a contar da data de entrada em vigor do presente regulamento e posteriormente de seis em seis meses, durante a fase de desenvolvimento dos componentes, a eu-LISA apresenta um relatório ao Parlamento Europeu e ao Conselho sobre o ponto da situação do desenvolvimento de cada componente. Quando o desenvolvimento estiver concluído, é apresentado um relatório ao Parlamento Europeu e ao Conselho a explicar em pormenor a forma como os objetivos, em especial de planeamento e de custos, foram alcançados, justificando igualmente eventuais divergências.

3. Para efeitos de manutenção técnica, a eu-LISA terá acesso às informações necessárias respeitantes às operações de tratamento de dados efetuadas nos componentes.

4. Quatro anos após o início das operações do último componente aplicado e posteriormente de quatro em quatro anos, a eu-LISA apresentará ao Parlamento Europeu, ao Conselho e à Comissão um relatório sobre o funcionamento técnico dos componentes.

5. Cinco anos após o início das operações do último componente implementado e posteriormente de quatro em quatro anos, a Comissão apresenta uma avaliação global e apresentará eventuais recomendações necessárias. Essa avaliação global deve incluir: os resultados alcançados pelos componentes tendo em conta os seus objetivos de interoperabilidade, facilidade de manutenção, o desempenho e as implicações financeiras, bem como do impacto sobre os direitos fundamentais.

A Comissão transmitirá o relatório de avaliação ao Parlamento Europeu e ao Conselho.

6. Os Estados-Membros e a Europol fornecerão à eu-LISA e à Comissão as informações necessárias para a elaboração dos relatórios referidos nos pontos 4 e 5, de acordo com os parâmetros quantitativos previamente definidos pela Comissão e/ou pela eu-LISA. Estas informações não podem em caso algum prejudicar os métodos de trabalho, nem incluir informações que revelem as fontes, identidades dos membros do pessoal ou as investigações das autoridades designadas.

7. A eu-LISA comunica à Comissão as informações necessárias à elaboração das avaliações globais referidas no ponto 5.

8. Respeitando as disposições de direito nacional sobre a publicação de informações sensíveis, cada Estado-Membro e a Europol devem elaborar relatórios anuais sobre a eficácia do acesso aos sistemas da UE para efeitos de aplicação da lei contendo informações e estatísticas sobre:

- a finalidade exata da consulta, incluindo o tipo de infração terrorista ou crime grave;

- motivos razoáveis de suspeita fundamentada de que o suspeito, autor ou vítima está abrangido pelo presente regulamento;

- o número de pedidos de acesso aos componentes para efeitos de aplicação da lei;

- o número e tipo de casos que resultaram em identificações positivas;

- a necessidade e utilização feitas dos casos de urgência excecional, incluindo os casos em que essa urgência não foi aceite pela verificação posterior realizada pelo ponto central de acesso.

Os relatórios anuais dos Estado-Membro e da Europol devem ser transmitidos à Comissão até 30 de junho do ano seguinte.

2.2. Sistema de gestão e de controlo

2.2.1. Risco(s) identificado(s)

Os riscos são os que estão relacionados com um desenvolvimento informático de cinco componentes por um contratante externo gerido pela eu-LISA. Estes são os riscos típicos dos projetos:

1. O risco de não concluir projeto dentro do prazo;

2. O risco de não concluir o projeto dentro dos limites do orçamento;

3. O risco de não se concretizar na íntegra o âmbito do projeto.

O primeiro risco é o mais importante uma vez que a ultrapassagem dos prazos acarreta custos mais elevados, dado que a maioria dos custos têm uma relação com a duração: custos de pessoal, custos de licença paga por ano, etc.

Estes riscos podem ser limitados através da aplicação de técnicas de gestão de projeto, incluindo medidas de emergência em projetos de desenvolvimento e pessoal suficiente, a fim de poderem absorver os picos de trabalho. A estimativa do esforço é normalmente feita com base numa carga de trabalho uniforme ao longo do tempo, muito embora na realidade os projetos estejam sujeitos a cargas de trabalho irregulares, que são absorvidas pelo aumento da afetação de recursos.

São vários os riscos ligados ao recurso a um contratante externo para estes trabalhos de desenvolvimento:

1. Em especial, o risco de que a empresa contratada não consiga afetar recursos suficientes ao projeto ou que conceba e desenvolva um sistema que não corresponda ao estado da técnica;

2. O risco de que as técnicas administrativas e métodos de gestão de projetos informáticos de grande escala não sejam plenamente respeitados como forma de o contratante reduzir os custos;

3. Por último, não pode ser completamente excluído o risco de a empresa contratada ser confrontada com dificuldades financeiras por razões externas a este projeto.

Estes riscos são atenuados através de contratos celebrados com base em critérios de qualidade sólidos e verificação das referências das empresas contratadas e manutenção de uma forte relação com estas. Por fim, como último recurso, podem ser incluídas e aplicadas sempre que necessário cláusulas penais e de rescisão.

2.2.2. Informações sobre o sistema de controlo interno criado

A eu-LISA destina-se a ser um centro de excelência no domínio do desenvolvimento e da gestão de sistemas informáticos de grande escala. Deve executar as atividades relacionadas com o desenvolvimento e as operações dos diferentes componentes de interoperabilidade, incluindo a manutenção da interface uniforme nacional nos Estados-Membros.

Durante a fase de desenvolvimento, o conjunto das atividades será executado pela eu-LISA. Esta abrange a parte do desenvolvimento de todas as vertentes do projeto. Os custos relacionados com a integração dos sistemas nos Estados-Membros durante o desenvolvimento, serão geridos pela Comissão através de gestão partilhada ou de subvenções.

Durante a fase operacional, a eu-LISA será responsável pela gestão técnica e financeira dos componentes utilizados a nível central, nomeadamente a adjudicação e a gestão dos contratos. A Comissão irá gerir os fundos destinados aos Estados-Membros para as despesas com as unidades nacionais através do FSI-Fronteiras (programas nacionais).

A fim de evitar atrasos a nível nacional deve ser prevista antes do início do desenvolvimento uma governação eficaz entre todas as partes interessadas. A Comissão pressupõe que será definida uma arquitetura interoperável no início do projeto, a fim de poder ser aplicada nos projetos SES e ETIAS, dado que estes projetos fornecem e usam o BMS, o repositório comum de dados de identificação e o portal europeu de pesquisa. Um membro da equipa de gestão do projeto de interoperabilidade deve fazer parte da estrutura de governação do projeto do SES e ETIAS.

2.2.3. Estimativa dos custos e benefícios dos controlos e avaliação do nível previsto de risco de erro

Não foi apresentada qualquer estimativa dado que o controlo e a minimização dos riscos é uma tarefa inerente à estrutura de governação do projeto.

2.3. Medidas de prevenção de fraudes e irregularidades

Especificar medidas de prevenção e proteção existentes ou previstas.

As medidas previstas para lutar contra a fraude estão previstas no artigo 35.º do Regulamento (UE) n.º 1077/2011, que determina o seguinte:

1. Tendo em vista a luta contra a fraude, a corrupção e outras atividades ilícitas, aplica-se o Regulamento (CE) n.º 1073/1999.

2. As agências devem aderir ao Acordo Interinstitucional relativo aos inquéritos internos efetuados pelo Organismo Europeu de Luta Antifraude (OLAF) e publicar sem demora as disposições relevantes aplicáveis a todo o pessoal das Agências.

3. As decisões de financiamento e os acordos de implementação e instrumentos delas decorrentes devem estipular expressamente que o Tribunal de Contas e o OLAF podem, se for necessário, proceder a controlos no terreno dos beneficiários dos fundos das Agências e dos agentes responsáveis pela sua atribuição.

Em conformidade com esta disposição, a decisão do Conselho de Administração da Agência europeia para a gestão operacional de sistemas informáticos de grande escala no espaço da liberdade, segurança e justiça relativa aos termos e condições dos inquéritos internos em matéria de luta contra a fraude, corrupção e todas as atividades ilegais lesivas dos interesses da União foi adotada em 28 de junho de 2012.

Será aplicável a estratégia de prevenção e de deteção de fraude da DG MIGRAÇÃO E ASSUNTOS INTERNOS.

3. IMPACTO FINANCEIRO ESTIMADO DA PROPOSTA/INICIATIVA

JUNTA-SE A ESTIMATIVA DO IMPACTO NAS DESPESAS E PESSOAL A PARTIR DE 2021 NA PRESENTE FICHA FINANCEIRA LEGISLATIVA EXCLUSIVAMENTE PARA FINS ILUSTRATIVOS, SEM PREJUÍZO DO PRÓXIMO QUADRO FINANCEIRO PLURIANUAL

3.1. Rubrica(s) do quadro financeiro plurianual e rubrica(s) orçamental(is) de despesas envolvida(s)

- Rubricas orçamentais existentes

Por ordem das rubricas do quadro financeiro plurianual e rubricas orçamentais.

Rubrica do quadro financeiro plurianual	Rubrica orçamental	Tipo de despesas	Contribuição			
	Número [Rubrica.....]	Dd/DND[84].	dos países EFTA[85]	dos países candidatos [86]	de países terceiros	na aceção do artigo 21.º, n.º 2, alínea b), do Regulamento Financeiro
3	18.02.01.03 — Fronteiras Inteligentes	Dd	Não	Não	Sim	Não
3	18.02.03 — Agência Europeia da Guarda Costeira e de Fronteiras (Frontex)	Dd	Não	Não	Sim	Não
3	18.02.04 — EUROPOL	Dd	Não	Não	Não	Não
3	18.02.05 — CEPOL	DND	Não	Não	Não	Não
3	18.02.07 — Agência europeia para a gestão operacional de sistemas informáticos de grande escala no espaço da liberdade, da segurança e da justiça (eu-LISA)	Dd	Não	Não	Sim	Não

[84] Dd = dotações diferenciadas / DND = dotações não diferenciadas.
[85] EFTA: Associação Europeia de Comércio Livre.
[86] Países candidatos e, se for caso disso, países candidatos potenciais dos Balcãs Ocidentais.

3.2. Impacto estimado nas despesas

[Esta parte deve ser preenchida na **folha de cálculo relativa aos dados orçamentais de natureza administrativa** (segundo documento no anexo da presente ficha financeira) e carregada para DECIDIR para efeitos de consulta interserviços.]

3.2.1. Síntese do impacto estimado nas despesas

Em milhões de EUR (até três casas decimais)

Rubrica do quadro financeiro plurianual	3	Segurança e cidadania

DG Migração e Assuntos Internos			Ano **2019**	Ano **2020**	Ano **2021**	Ano **2022**	Ano **2023**	Ano **2024**	Ano **2025**	Ano **2026**	Ano **2027**	**Ano 2028**	**TOTAL**
• Dotações operacionais													
18.02.01.03 — Fronteiras Inteligentes	Autorizações	1)	0	0	43,150	48,150	45,000	0	**0**	**0**	**0**	**0**	**136,300**
	Pagamentos	2)	0	0	34,520	47,150	45,630	9,000	**0**	**0**	**0**	**0**	136,300
Dotações de natureza administrativa financiadas a partir da dotação de programas específicos[87]													
Número da rubrica orçamental		3)											
Total das dotações para a DG Migração e Assuntos Internos	Autorizações	=1+1a +3)	0	0	43,150	48,150	45,000	0	**0**	**0**	**0**	**0**	**136,300**
	Pagamentos	=2+2a +3	0	0	34,520	47,150	45,630	9,000	**0**	**0**	**0**	**0**	136,300

As despesas cobrem os custos relacionados com:

[87] Assistência técnica e/ou administrativa e despesas de apoio à implementação de programas e/ou ações da UE (antigas rubricas «BA»), investigação direta e indireta.

– O custo para a adaptação da interface uniforme nacional (IUN), cujo desenvolvimento é financiado ao abrigo da proposta relativa ao SES, um montante orçamentado para as alterações aos sistemas existentes nos Estados-Membros a fim de ter em conta as alterações dos sistemas centrais e um montante orçamentado para a formação dos utilizadores finais.

18.0203 — GEFC			Ano **2019**	Ano **2020**	Ano **2021**	Ano **2022**	Ano **2023**	Ano **2024**	Ano **2025**	Ano **2026**	Ano **2027**	**TOTAL**
Título 1: Despesas de pessoal	Autorizações	1)	0	0	0	0,488	2,154	0,337	0	0	0	2,979
	Pagamentos	2)	0	0	0	0,488	2,154	0,337	0	0	0	2,979
Título 2: Infraestruturas e despesas de funcionamento	Autorizações	(1a)	0	0	0	0,105	0,390	0,065	0	0	0	0,560
	Pagamentos	(2a)	0	0	0	0,105	0,390	0,065	0	0	0	0,560
Título 3: Despesas operacionais	Autorizações	(3a)	0	0	0	0,183	2,200	0	0	0	0	2,383
	Pagamentos	(3b)	0	0	0	0,183	2,200	0	0	0	0	2,383
TOTAL de dotações para a GEFC	(total das autorizações = total dos pagamentos)	= 1 +1a +3a	**0**	**0**	**0**	**0,776**	**4,744**	**0,402**	**0**	**0**	**0**	**5,923**

– O orçamento para a GEFC abrange as despesas de uma equipa dedicada para a validação de ligações geradas pelo MID (detetor de identidades múltiplas) com base nos dados preexistentes (algo como 14 milhões de registos). O volume das ligações que requerem validação manual estima-se em cerca de 550 000.

A equipa dedicada criada para o efeito é adicionada à equipa da GEFC criada para o ETIAS, porque este é funcionalmente aproximado e evita os custos de criação de uma nova equipa. Prevê-se que os trabalhos decorram em 2023. Os agentes contratuais são assim recrutados com até 3 meses de antecedência e o seu contrato termina a partir de 2 meses após o termo da atividade migratória. Não se pressupõe o recrutamento de outra parte dos recursos necessários como agentes contratuais e estes serão contratados como consultores. Isto explica as despesas ao abrigo do título 3 para 2023. Pressupõe-se que serão contratados com um mês de antecedência. Mais pormenores sobre os níveis de pessoal serão apresentados posteriormente.

– O título 1 inclui, assim, o custo de 20 internos e as disposições para o reforço do pessoal de gestão e de apoio.

– O título 2 inclui o custo adicional para o acolhimento de 10 pessoas adicionais da empresa contratada.

– O título 3 inclui os honorários para 10 pessoas adicionais da empresa contratada. Não existem outros tipos de custos incluídos.

18.0204 — Europol			Ano **2019**	Ano **2020**	Ano **2021**	Ano **2022**	Ano **2023**	Ano **2024**	Ano **2025**	Ano **2026**	Ano **2027**	**TOTAL**
Título 1: Despesas de pessoal	Autorizações	1)	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
	Pagamentos	2)	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
Título 2: Infraestruturas e despesas de funcionamento	Autorizações	(1a)	0	0	0	0	0	0	0	0	0	0
	Pagamentos	(2a)	0	0	0	0	0	0	0	0	0	0
Título 3: Despesas operacionais	Autorizações	(3a)	0	6,380	6,380	2,408	2,408	7,758	7,758	7,758	2,408	37,908
	Pagamentos	(3b)	0	6,380	6,380	2,408	2,408	7,758	7,758	7,758	2,408	37,908
TOTAL de dotações para a Europol	(total das autorizações = total dos pagamentos)	= 1 +1a +3a	0,690	8,382	8,382	3,589	3,589	3,382	8,732	8,732	3,382	48,860

As despesas da Europol cobrirão a atualização das capacidades dos sistemas informáticos da Europol para tratar o volume de mensagens que vai ser necessário manusear e o aumento necessário dos níveis de desempenho (tempo de resposta).

Título 1 Despesas de pessoal abrange as despesas relacionadas com pessoal adicional a recrutar para as TIC, para reforçar os sistemas de informação da Europol pelas razões descritas supra. Informações mais pormenorizadas sobre a repartição de lugares entre agentes temporários e agentes contratuais e as respetivas competências são apresentados a seguir.

O título 3 inclui os custos para o hardware e o software necessários para reforçar os sistemas de informação da Europol. Neste momento, os sistemas informáticos da Europol servem uma comunidade limitada designada da Europol, os agentes de ligação da Europol e investigadores nos Estados-Membros que utilizam esses sistemas para efeitos de análise e investigação. Com a implementação do sistema QUEST (a interface do sistema que permitirá ao ESP consultar os dados da Europol) no nível básico de proteção (atualmente os sistemas de informação da Europol possuem acreditação até ao nível restrito UE e confidencial UE), os sistemas de informação da Europol serão disponibilizados para uma comunidade muito maior de forças policiais autorizadas. Para além destes aumentos, o ESP será utilizado pelo ETIAS para consultar automaticamente os dados da Europol para tratar autorizações de viagem. Aumenta assim o volume de consultas dos dados da Europol de cerca

de 107 000 consultas por mês, atualmente, para mais de 100 000 consultas por dia e exigirá igualmente a disponibilidade de 24 horas sobre 24, 7 dias da semana dos sistemas de informação da Europol e tempos de resposta muito curtos para responder às exigências impostas pelo Regulamento ETIAS. A maior parte dos custos são limitados ao período que precede o início do funcionamento dos componentes de interoperabilidade, mas são necessárias algumas dotações permanentes para assegurar uma disponibilidade elevada e contínua dos sistemas de informação da Europol. Além disso, são necessárias alguns trabalhos de desenvolvimento para implementar os componentes de interoperabilidade por parte da Europol enquanto utilizador.

18.0205 - CEPOL			Ano **2019**	Ano **2020**	Ano **2021**	Ano **2022**	Ano **2023**	Ano **2024**	Ano **2025**	Ano **2026**	Ano **2027**	**TOTAL**
Título 1: Despesas de pessoal	Autorizações	1)	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
	Pagamentos	2)	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
Título 2: Infraestruturas e despesas de funcionamento	Autorizações	(1a)	0	0	0	0	0	0	0	0	0	0
	Pagamentos	(2a)	0	0	0	0	0	0	0	0	0	0
Título 3: Despesas operacionais	Autorizações	(3a)	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
	Pagamentos	(3b)	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
TOTAL de dotações para a CEPOL	(total das autorizações = total dos pagamentos)	= 1 +1a +3a	0	0,144	0,384	0,482	0,208	0,208	0,208	0,208	0,208	2,050

Uma formação com coordenação centralizada a nível da UE melhora a implementação coerente dos cursos de formação a nível nacional e, consequentemente, assegura uma execução correta e uma implementação e utilização eficaz e bem sucedida dos componentes de interoperabilidade. A CEPOL, a Agência da União Europeia para a Formação Policial — está bem posicionada para dar formação centralizada a nível da UE. Estas despesas cobrem a preparação da «formação de formadores dos Estados-Membros» necessários para utilizar os sistemas centrais assim que estiverem interoperáveis. Os custos incluem os relativos a um pequeno aumento de pessoal da CEPOL para coordenar, gerir, organizar e atualizar os cursos e os custos de uma série de sessões de formação por ano e preparação do curso em linha. São apresentados pormenores sobre estes custos mais adiante. O esforço de formação é concentrado nos períodos imediatamente anteriores à entrada em serviço. Continua a ser necessário um esforço contínuo para além da ativação dado que os componentes interoperáveis são mantidos e os formadores não permanecem continuamente as mesmas pessoas, com base na experiência de formação existente no sistema de informação Schengen.

18.0207 - eu-LISA			Ano **2019**	Ano **2020**	Ano **2021**	Ano **2022**	Ano **2023**	Ano **2024**	Ano **2025**	Ano **2026**	Ano **2027**	**TOTAL**
Título 1: Despesas de pessoal	Autorizações	1)	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
	Pagamentos	2)	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
Título 2: Infraestruturas e despesas de funcionamento	Autorizações	(1a)	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
	Pagamentos	(2a)	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
Título 3: Despesas operacionais	Autorizações	(3a)	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
	Pagamentos	(3b)	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
TOTAL de dotações para a eu-LISA	(total das autorizações = total dos pagamentos)	= 1 +1a +3a	**5,830**	**17,031**	**51,743**	**44,749**	**29,653**	**20,370**	**18,609**	**18,529**	**18,529**	**225,041**

Estas despesas cobrem:

– O desenvolvimento e a manutenção dos quatro componentes de interoperabilidade (portal europeu de pesquisa (ESP), serviço partilhado de correspondências biométricas (BMS), repositório comum de dados de identificação (CIR) e detetor de identidades múltiplas (MID) incluídos nas propostas legislativas mais o repositório comum para a elaboração de relatórios e estatísticas (CRRS). A eu-LISA agirá na qualidade de representante do proprietário do projeto e utiliza o seu próprio pessoal para elaboração de especificações, a seleção de empresas contratadas, orientação do seu trabalho, submissão dos resultados a uma série de ensaios e aceitação do trabalho realizado.

– Os custos associados à migração de dados dos sistemas herdados para os novos componentes. Contudo, a eu-LISA não tem qualquer papel direto no carregamento inicial de dados no MID (validação de ligações), porque esta ação é exercida sobre o conteúdo dos dados propriamente dito. A migração dos dados biométricos de sistemas herdados prende-se com o formato e o rótulo dos dados e não com o conteúdo dos dados.

– Os custos de atualização e exploração do sistema ECRIS-TCN para um sistema de disponibilidade elevada a partir de 2022. O ECRIS-TCN é o sistema central que contém os registos criminais de nacionais de países terceiros. Está previsto que o sistema esteja disponível a partir de 2020. Está previsto que os componentes de interoperabilidade possam igualmente ter acesso a esse sistema que, por conseguinte, deve tornar-se também um sistema de elevado nível de disponibilidade. As despesas operacionais incluem o custo adicional para atingir essa elevada disponibilidade. Existe um custo de desenvolvimento significativo em 2021 seguido de um custo de manutenção e de exploração contínuo. Estes custos não são incluídos na ficha financeira legislativa da revisão do regulamento de base da eu-LISA[88], que inclui apenas os orçamentos de 2018 a 2020 e, por conseguinte, não se sobrepõe ao presente orçamento.

– O padrão das despesas é o resultado da sequenciação do projeto. Dado que os diferentes componentes não são independentes entre si, o período de desenvolvimento estende-se de 2019 a 2023. No entanto, a partir de 2020 tem já início a manutenção e exploração dos primeiros componentes já disponíveis. Explica-se assim por que razão as despesas começam lentamente, aumentam e depois diminuem para um valor constante.

– As despesas previstas no título 1 (despesas de pessoal) seguem a sequenciação do projeto: O aumento do pessoal é necessário para passar o projeto à empresa contratada (cujas despesas são previstas no título 3). Quando o projeto for entregue, parte da equipa responsável pela entrega é afetada aos trabalhos de evolução e de manutenção. Ao mesmo tempo, o pessoal para a exploração dos sistemas recém-entregues aumenta.

– As despesas previstas no título 2 (despesas de infraestruturas e de exploração) abrangem o espaço de escritórios adicional para acolher temporariamente as equipas da empresa contratada responsável pelas tarefas de desenvolvimento, manutenção e operacionais. O padrão de despesas ao longo do tempo segue assim também a evolução do quadro de pessoal. Os custos para albergar o equipamento adicional já foram incluídos no orçamento da eu-LISA. Não existem também custos adicionais para acolher o pessoal da eu-LISA dado estarem incluídos nos custos padrões com o pessoal.

– As despesas previstas no título 3 (despesas operacionais) incluem o custo de uma empresa contratada para desenvolver e manter o sistema, a aquisição de hardware e software específicos.
Os custos com a empresa contratada começam inicialmente com os estudos de especificação dos componentes e o desenvolvimento apenas para um componente (o CRRS). Durante o período 2020-2022, os custos aumentam à medida que mais componentes vão sendo desenvolvidos em paralelo. Os custos não diminuem após o pico porque as tarefas de migração são particularmente pesadas nesta carteira de projetos. Os custos com a empresa contratada diminuem depois à medida que os componentes são entregues e iniciam o modo operacional, que exige um

[88] COM 2017/0145 (COD) Proposta de regulamento do Parlamento Europeu e do Conselho sobre a Agência Europeia para a gestão operacional de sistemas informáticos de grande escala no domínio da liberdade, segurança e justiça, e que altera o Regulamento (CE) n.º 1987/2006 e a Decisão 2007/533/JHA do Conselho e que revoga o Regulamento (UE) n.º 1077/2011

padrão de recursos estáveis.
Em simultâneo com as despesas previstas no título 3, as despesas aumentam fortemente em 2020 em comparação com o ano anterior devido ao investimento inicial em equipamento informático e software necessários durante o desenvolvimento. As despesas previstas no título 3 (despesas operacionais) apresentam um aumento em 2021 e 2022 devido aos custos de investimento em equipamento informático e software para os ambientes informáticos operacionais (produção e pré-produção tanto para a unidade central e para a unidade central auxiliar) são incorridas no ano anterior à entrada em funcionamento, respetivamente para componentes de interoperabilidade (CIR e o MID) com um nível de exigência elevado quanto ao software e equipamento informático. Assim que entrarem em funcionamento, os custos com equipamento informático e software são essencialmente os custos de manutenção.

– Mais adiante serão apresentados mais detalhes.

Rubrica do quadro financeiro plurianual	**5**	«Despesas administrativas»

Em milhões de EUR (até três casas decimais)

		Ano **2019**	Ano **2020**	Ano **2021**	Ano **2022**	Ano **2023**	Ano **2024**	Ano **2025**	Ano **2026**	Ano **2027**	**TOTAL**
DG MIGRAÇÃO E ASSUNTOS INTERNOS											
• Recursos humanos Número da rubrica orçamental 18.01		0,690	0,690	0,690	0,690	0,690	0,690	0,276	0,276	0,276	4,968
Outros custos administrativos (reuniões, etc.)		0,323	0,323	0,323	0,323	0,323	0,323	0,263	0,263	0,263	2,727
TOTAL DG MIGRAÇÃO E ASSUNTOS INTERNOS	Dotações	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695

TOTAL de dotações fora da RUBRICA 5 do quadro financeiro plurianual	(total das autorizações = total dos pagamentos)	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**0,539**	**0,539**	**0,539**	**7,695**

Em milhões de EUR (até três casas decimais)

		Ano **2019**	Ano **2020**	Ano **2021**	Ano **2022**	Ano **2023**	Ano **2024**	Ano **2025**	Ano **2026**	Ano **2027**	Ano 2028	**TOTAL**
TOTAL de dotações ao abrigo das RUBRICAS 1 a 5 do quadro financeiro plurianual	Autorizações	**7,533**	**26,569**	**104,672**	**98,591**	**83,363**	**25,256**	**28,088**	**28,008**	**22,658**	**0**	**424,738**
	Pagamentos	**7,533**	**26,569**	**96,042**	**97,591**	**83,993**	**34,256**	**28,088**	**28,008**	**22,658**	**0**	**424,738**

3.2.2. Impacto estimado nas dotações operacionais

3.2.2.1. Impacto estimado nas dotações da Agência GEFC

– ☐ A proposta/iniciativa não implica a utilização de dotações operacionais

– ☒ A proposta/iniciativa implica a utilização de dotações operacionais, tal como explicitado seguidamente:

Dotações de autorização em milhões de EUR (três casas decimais)

Indicar os objetivos e os resultados			Ano **2019**		Ano **2020**		Ano **2021**		Ano **2022**		Ano **2023**		Ano **2024**		Ano **2025**		Ano **2026**		Ano **2027**		**TOTAL**	
Agência GEFC ⇩	Tipo[89]	Custo médio	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	N.º total	Custo total
OBJETIVO ESPECÍFICO N.º 1[90] Validação das ligações																						
Número de efetivos recrutados como peritos para validar as ligações	Despesas da empresa contratada		0	0	0	0	0	0	0,8	0,183	10	2,200	0	0	0	0	0	0	0	0		2,383
Subtotal para o objetivo específico n.º 1			**0**	**0**	**0**	**0**	**0**	**0**	**0,8**	**0,183**	**10**	**2,200**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**2,383**

[89] Os resultados dizem respeito aos produtos fornecidos e serviços prestados (exemplo: número de intercâmbios de estudantes financiados, número de quilómetros de estradas construídas, etc.).

[90] Tal como descrito no ponto 1.4.2. «Objetivo(s) específico(s)...»

Estas despesas cobrem:

- A contratação de mão de obra suplementar suficiente (estimativa de cerca de 10 peritos) a adicionar ao pessoal interno existente (estimado em cerca de 20 pessoas) que serão acolhidos na GEFC a fim de validar as ligações. Existe apenas um mês de recrutamento antes da data de início prevista para atingir os níveis de recursos humanos necessários.

- Não existem outras despesas estimadas relacionadas com a empresa contratada. O software exigido faz parte dos custos com a licença BMS. Não existe nenhuma capacidade de tratamento específica para o equipamento informático. Pressupõe-se que o pessoal da empresa contratada será acolhido pela GEFC. Por conseguinte, ao abrigo dos custos previstos no título 2, é adicionado o custo anual de 12 m² por pessoa, em média.

3.2.2.2. Impacto estimado nas dotações da Europol

– ☐ A proposta/iniciativa não implica a utilização de dotações operacionais

– ☒ A proposta/iniciativa implica a utilização de dotações operacionais, tal como explicitado seguidamente:

Dotações de autorização em milhões de EUR (três casas decimais)

Indicar os objetivos e os resultados **Europol** ⇩			Ano **2019**		Ano **2020**		Ano **2021**		Ano **2022**		Ano **2023**		Ano **2024**		Ano **2025**		Ano **2026**		Ano **2027**		**TOTAL**	
	Tipo[91]	Custo médio	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	N.º total	Custo total
OBJETIVO ESPECÍFICO N.º 1[92] Desenvolvimento e manutenção de sistemas (Europol)																						
Ambiente informático	Infraestrutura					1,840		1,840		0,736		0,736		0,736		0,736		0,736		0,736		8,096
Ambiente informático	Hardware					3,510		3,510		1,404		1,404		1,404		5,754		5,754		1,404		26,144

[91] Os resultados dizem respeito aos produtos fornecidos e serviços prestados (exemplo: número de intercâmbios de estudantes financiados, número de quilómetros de estradas construídas, etc.).

[92] Tal como descrito no ponto 1.4.2. «Objetivo(s) específico(s)...»

Ambiente informático	Software				0,670		0,670		0,268		0,268		0,268		0,268		0,268		2,948
Trabalhos de desenvolvimento	Empresa contratada				0,360		0,360												0,720
Subtotal			**0**		**6,380**		**6,380**		**2,408**		**2,408**		**2,408**		**7,758**		**7,758**		**2,408**		**37,908**

Estas despesas cobrem as necessidades de reforço dos sistemas de informação e infraestruturas da Europol para integrar o aumento de consultas. Estes custos incluem:

- Atualização da segurança e das infraestruturas de rede, equipamento informático (servidores, sistemas de armazenamento) e software (licenças). Estas atualizações têm de ser concluídas antes de o portal europeu de pesquisa e o sistema ETIAS se tornarem operacionais em 2021, os custos foram repartidos uniformemente entre 2020 e 2021. A partir de 2022, foi assumida uma taxa anual de manutenção de 20 % como base de cálculo dos custos de manutenção. Além disso, foi tido em consideração o ciclo quinquenal normal de substituição do equipamento informático obsoleto e da infraestrutura.
- Custos da empresa contratada para trabalhos de desenvolvimento destinados à implementação de QUEST no nível básico de proteção.

3.2.2.3. Impacto estimado nas dotações da CEPOL

– ☐ A proposta/iniciativa não implica a utilização de dotações operacionais

– ☒ A proposta/iniciativa implica a utilização de dotações operacionais, tal como explicitado seguidamente:

Dotações de autorização em milhões de EUR (três casas decimais)

Indicar os objetivos e os resultados			Ano **2019**		Ano **2020**		Ano **2021**		Ano **2022**		Ano **2023**		Ano **2024**		Ano **2025**		Ano **2026**		Ano **2027**		**TOTAL**	
CEPOL ⇩	Tipo[93]	Custo médio	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	N.º total	Custo total
OBJETIVO ESPECÍFICO N.º 1[94] Desenvolvimento e realização dos cursos de formação																						
Número de cursos residenciais	0,34 por curso		0		1	0,040	4	0,136	8	0,272	2	0,068	2	0,068	2	0,068	2	0,068	2	0,068		0,788
Formação em linha	0,02			0				0,040		0,002		0,002		0,002		0,002		0,002		0,002		0,052

[93] Os resultados dizem respeito aos produtos fornecidos e serviços prestados (exemplo: número de intercâmbios de estudantes financiados, número de quilómetros de estradas construídas, etc.).

[94] Tal como descrito no ponto 1.4.2. «Objetivo(s) específico(s)...»

Subtotal		**0**		**0,040**		**0,176**		**0,274**		**0,070**		**0,070**		**0,070**		**0,070**		**0,840**

A fim de assegurar a implementação uniforme e utilização das soluções de interoperabilidade, as ações de formação serão organizadas tanto centralmente a nível da UE pela CEPOL como pelos Estados-Membros. As despesas de formação a nível da UE incluem:

- desenvolvimento de curricula comuns a utilizar pelos Estados-Membros na implementação de ações de formação a nível nacional;

- atividades residenciais para formação dos docentes. Nos dois anos, imediatamente após as soluções de interoperabilidade se tornarem operacionais, prevê-se a implementação da formação em maior escala, sendo mais tarde mantida por dois cursos de formação presencial por ano.

- curso em linha para complementar as atividades residenciais a nível da UE e nos Estados-Membros.

3.2.2.4. Impacto estimado nas dotações da eu-LISA

– ☐ A proposta/iniciativa não implica a utilização de dotações operacionais

– ☒ A proposta/iniciativa implica a utilização de dotações operacionais, tal como explicitado seguidamente:

Dotações de autorização em milhões de EUR (três casas decimais)

Indicar os objetivos e os resultados			Ano **2019**		Ano **2020**		Ano **2021**		Ano **2022**		Ano **2023**		Ano **2024**		Ano **2025**		Ano **2026**		Ano **2027**		**TOTAL**	
Eu-LISA ⇩	Tipo[95]	Custo médio	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	N.º total	Custo total
OBJETIVO ESPECÍFICO N.º 1[96] Desenvolvimento de componentes de interoperabilidade																						
Sistemas criados	Empresa contratada			1,800		4,930		8,324		4,340		1,073		1,000		0,100		0,020		0,020		21,607
Produtos de software	Software			0,320		3,868		15,029		8,857		3,068		0,265		0,265		0,265		0,265		32,202

[95] Os resultados dizem respeito aos produtos fornecidos e serviços prestados (exemplo: número de intercâmbios de estudantes financiados, número de quilómetros de estradas construídas, etc.).

[96] Tal como descrito no ponto 1.4.2. «Objetivo(s) específico(s)...»

Produtos de hardware	Hardware		0,250		2,324		5,496		2,904		2,660		0,500		0		0		0		14,133
Formação em informática	Formação e outros		0,020		0,030		0,030		0,030		0,030		0,050		0,050		0,050		0,050		0,340
Subtotal para o objetivo específico n.º 1			**2,390**		**11,151**		**28,879**		**16,131**		**6,830**		**1,815**		**0,415**		**0,335**		**0,335**		**68,281**

– Este objetivo inclui apenas os custos para a realização de quatro componentes de interoperabilidade e o CRRS.

– Os custos relacionados com o BMS foram estimados tendo em conta o pressuposto de que o SES que está prestes a ser desenvolvido servirá de sistema principal para o desenvolvimento. Por conseguinte, está prevista a reutilização das licenças de software biométrico (36 milhões de EUR) incluída para o SES.

– Neste orçamento, o BMS é tratado em termos orçamentais como uma nova extensão do BMS para o SES. Por conseguinte, a ficha financeira atual inclui o custo marginal de licenças de software (6,8 milhões de EUR) para acrescentar os cerca de 20 milhões de conjuntos de dados biométricos contidos no SIS AFIS (o AFIS é o sistema automático de identificação dactiloscópica = o «BMS» do SIS), no AFIS do Eurodac e no futuro ECRIS-TCN (Sistema Europeu de Informação sobre os Registos Criminais de nacionais de países terceiros) ao BMS entregue para o SES. Os custos de integração dos diferentes sistemas (SIS, Eurodac, ECRIS-TCN) no BMS estão incluídos na presente ficha financeira.

– Como parte do trabalho ao longo de 2019 e 2020, a eu-LISA será convidada a definir a solução técnica exata, que não possa ser definida no momento da apresentação da proposta legislativa, e estimar as consequências de custos da implementação da melhor solução técnica. Este aspeto pode implicar uma alteração da estimativa de custos presentemente fornecida.

– Todos os componentes serão entregues até ao final de 2023, o que explica a razão pela qual as despesas com a empresa contratada descem para perto de zero nessa altura. Permanece apenas um montante residual de atualização contínua do CRSS.

– Durante o período de 2019 a 2021, as despesas com o software aumentam substancialmente, dado que se incorre em custos com licenças de software para diferentes ambientes necessários para a produção, pré-produção e ensaios, tanto a nível central como local, e o serviço de salvaguarda. Além disso, são indicados os preços de alguns componentes de software específicos e indispensáveis em função do número de

«objetos referenciados»(ou seja, o volume de dados). Já que a base de dados irá conter, em última análise, cerca de 220 milhões de identidades, o preço do software é proporcional a este valor.

Indicar os objetivos e os resultados **Eu-LISA** ⇩			Ano **2019**		Ano **2020**		Ano **2021**		Ano **2022**		Ano **2023**		Ano **2024**		Ano **2025**		Ano **2026**		Ano **2027**		**TOTAL**	
	Tipo[97]	Custo médio	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	N.º total	Custo total
OBJETIVO ESPECÍFICO N.º 2 Manutenção e funcionamento dos componentes de interoperabilidade																						
Sistemas mantidos operacionais	Empresa contratada			0		0		0		1,430		2,919		2,788		2,788		2,788		2,788		15,501
Produtos de software	Software			0		0,265		0,265		1,541		5,344		5,904		5,904		5,904		5,904		31,032
Produtos de hardware	Hardware			0		0,060		0,060		0,596		1,741		1,741		1,741		1,741		1,741		9,423
Formação em informática	Formação			0		0		0		0		0,030		0,030		0,030		0,030		0,030		0,150
Subtotal para o objetivo específico n.º 2				**0**		**0,325**		**0,325**		**3,567**		**10,034**		**10,464**		**10,464**		**10,464**		**10,464**		**56,105**

[97] Os resultados dizem respeito aos produtos fornecidos e serviços prestados (exemplo: número de intercâmbios de estudantes financiados, número de quilómetros de estradas construídas, etc.).

– A manutenção começa assim que forem entregues alguns componentes. Por conseguinte, está incluído o orçamento atribuído a uma empresa de manutenção a partir do momento em que é entregue o ESP (em 2021). O orçamento de manutenção aumenta à medida que vão sendo entregues mais componentes, atingindo então um valor mais ou menos constante, que representa uma percentagem (entre 15 e 22%) do investimento inicial

– A manutenção de equipamentos informáticos e de software começa a contar com o ano de entrada em funcionamento: a evolução dos custos é semelhante à utilizada para os custos a cargo da empresa contratada.

Indicar os objetivos e os resultados **Eu-LISA** ⇩			Ano **2019**		Ano **2020**		Ano **2021**		Ano **2022**		Ano **2023**		Ano **2024**		Ano **2025**		Ano **2026**		Ano **2027**		**TOTAL**	
	Tipo[98]	Custo médio	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	N.º total	Custo total
OBJETIVO ESPECÍFICO N.º 3[99] Migração de dados																						
Dados herdados do BMS sujeitos a migração	Para BMS			0		0		0		7,000		3,000		0		0		0		0		10,000
Dados herdados do EDAC com permissão para migração	Reformular e reconstruir EDAC			0		0		7,500		7,500				0		0		0		0		15,000
Subtotal para o objetivo específico n.º 3				**0**		**0**		**7,500**		**14,500**		**3,000**										**25,000**

[98] Os resultados dizem respeito aos produtos fornecidos e serviços prestados (exemplo: número de intercâmbios de estudantes financiados, número de quilómetros de estradas construídas, etc.).

[99] Tal como descrito no ponto 1.4.2. «Objetivo(s) específico(s)...»

– No caso do projeto BMS, é necessário proceder à migração de dados a partir de outros motores de busca biométricos para o BMS, dado que este sistema comum é mais eficaz em termos operacionais e ainda confere uma vantagem financeira comparativamente com uma situação em que vários pequenos sistemas BMS continuariam a ser mantidos.

– A lógica atual do Eurodac não está claramente separada do mecanismo de correspondência biométrica, como no caso do BMS em funcionamento com o VIS. O funcionamento interno do Eurodac e o mecanismo com que os serviços às empresas recorrem aos serviços de correspondências biométricas subjacentes é uma «caixa negra» para o espectador externo e baseia-se em tecnologias patenteadas. Não é possível proceder simplesmente a uma migração dos dados para o BMS e manter o atual nível de atividade. Por conseguinte, a migração dos dados é acompanhada de custos significativos derivados da alteração dos mecanismos de intercâmbio com a aplicação central do Eurodac.

Indicar os objetivos e os resultados **Eu-LISA** ⇩			Ano **2019**		Ano **2020**		Ano **2021**		Ano **2022**		Ano **2023**		Ano **2024**		Ano **2025**		Ano **2026**		Ano **2027**		**TOTAL**	
	Tipo 100	Custo médio	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	N.º total	Custo total
OBJETIVO ESPECÍFICO N.º 4[101] Rede																						
Ligações de rede	Configuração da rede			0		0		0		0,505										0		0,505
Tráfego de rede tratado	Operações de rede			0		0						0,246		0,246		0,246		0,246		0,246		1,230
Subtotal para o objetivo específico				**0**		**0**		**0**		**0,505**		**0,246**		**0,246**		**0,246**		**0,246**		**0,246**		**1,735**

[100] Os resultados dizem respeito aos produtos fornecidos e serviços prestados (exemplo: número de intercâmbios de estudantes financiados, número de quilómetros de estradas construídas, etc.).

[101] Tal como descrito no ponto 1.4.2. «Objetivo(s) específico(s)...»

n.º 7																						

– Os componentes de interoperabilidade têm apenas um efeito marginal sobre o tráfego de rede. Em termos de dados, são criadas apenas as ligações entre os dados já existentes, o que constitui um elemento de baixo volume. O custo incluído neste ponto consiste apenas no aumento marginal do orçamento necessário para além dos orçamentos do SES e do ETIAS para a configuração da rede e tráfego.

Indicar os objetivos e os resultados **Eu-LISA** ⇩			Ano **2019**		Ano **2020**		Ano **2021**		Ano **2022**		Ano **2023**		Ano **2024**		Ano **2025**		Ano **2026**		Ano **2027**		**TOTAL**	
	Tipo [102]	Custo médio	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	N.º total	Custo total
OBJETIVO ESPECÍFICO N.º 5[103] Atualização da IUN																						
IUN atualizada	Empresa contratada			0		0		0		0,505		0,505								0		1,010
Subtotal para o objetivo específico n.º 5				**0**		**0**		**0**		**0,505**		**0,505**										**1,010**

– A proposta do SES introduziu o conceito da interface uniforme nacional (IUN) a ser desenvolvida e mantida pela eu-LISA. O quadro acima inclui o orçamento para a atualização das IUN para um tipo de intercâmbio de informações adicional. Não há custos adicionais sobre o funcionamento das IUN que já tinham sido orçamentadas ao abrigo da proposta relativa ao SES.

[102] Os resultados dizem respeito aos produtos fornecidos e serviços prestados (exemplo: número de intercâmbios de estudantes financiados, número de quilómetros de estradas construídas, etc.).

[103] Tal como descrito no ponto 1.4.2. «Objetivo(s) específico(s)...»

Indicar os objetivos e os resultados **Eu-LISA** ⇩			Ano **2019**		Ano **2020**		Ano **2021**		Ano **2022**		Ano **2023**		Ano **2024**		Ano **2025**		Ano **2026**		Ano **2027**		**TOTAL**	
	Tipo 104	Custo médio	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	N.º total	Custo total
Objetivo ESPECÍFICO N.º 6: Reuniões e formação																						
Reuniões de progresso mensal (Desenvolvimento)	0,021 por reunião x 10 por ano		10	*0,210*	10	*0,210*	10	*0,210*	10	*0,210*											40	0,840
Reuniões trimestrais (operações)	0,021 x 4 por ano		4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	36	0,756
Grupos consultivos	0,021 x 4 por ano		4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	36	0,756
Formação Estados-Membros	0,025 por formação		2	0,050	4	0,100	4	0,100	6	0,150	6	0,150	6	0,150	6	0,150	6	0,150	6	0,150	24	1,150
Subtotal para o objetivo específico n.º 6			20	**0,428**	22	**0,478**	22	**0,478**	24	**0,528**	14	**0,318**	14	**0,318**	14	**0,318**	14	**0,318**	14	**0,318**		**3,502**

[104] Os resultados dizem respeito aos produtos fornecidos e serviços prestados (exemplo: número de intercâmbios de estudantes financiados, número de quilómetros de estradas construídas, etc.).

– O subtotal 6 inclui as despesas de organização de reuniões da Autoridade de Gestão (neste caso, a eu-LISA) para a governação dos projetos. Estes são os custos relacionados com reuniões suplementares para a entrega de componentes de interoperabilidade.

– O subtotal 6 inclui os custos para as reuniões da eu-LISA com pessoal dos Estados-Membros encarregado do desenvolvimento, manutenção e funcionamento dos componentes de interoperabilidade e com a organização e realização de cursos de formação para pessoal de informática dos Estados-Membros.

– Durante o desenvolvimento, o orçamento inclui 10 reuniões de projeto por ano. Uma vez iniciada a preparação das operações (e é este o caso a partir de 2019), são organizadas quatro reuniões por ano. A um nível superior, é criado um grupo consultivo desde o início para implementar as decisões de execução da Comissão. Estão planeadas quatro reuniões por ano, quanto aos grupos consultivos existentes. Além disso, a eu-LISA prepara e presta formação para o pessoal de informática nos Estados-Membros. Esta formação é focada em aspetos técnicos dos componentes de interoperabilidade.

Indicar os objetivos e os resultados Eu-LISA ⇩			Ano **2019**		Ano **2020**		Ano **2021**		Ano **2022**		Ano **2023**		Ano **2024**		Ano **2025**		Ano **2026**		Ano **2027**		**TOTAL**	
	Tipo 105	Custo médio	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	N.º total	Custo total
OBJETIVO ESPECÍFICO N.º 7[106] Elevada disponibilidade do ECRIS-TCN																						
Sistema de elevada disponibilidade	Configuração do sistema			0		0		8,067												0		8,067
Operações de alta disponibilidade	Manutenção e gestão do sistema			0		0		0		1,768		1,768		1,768		1,768		1,768		1,768		10,608
Subtotal para o objetivo específico n.º 7				**0**		**0**		**8,067**		**1,768**		**1,768**		**1,768**		**1,768**		**1,768**		**1,768**		**18,675**

– O objetivo 7 consiste em passar o ECRIS-TCN de um sistema com uma disponibilidade «padrão» para um sistema de elevada disponibilidade. Em 2021, o ECRIS-TCN será sujeito a uma atualização, a qual exige essencialmente a aquisição de equipamento informático adicional. Uma vez que está prevista a conclusão do ECRIS-TCN em 2020, é tentadora a ideia de criar este sistema como um sistema de elevada disponibilidade desde o início e integrado com os componentes de interoperabilidade. Contudo, uma vez que muitos projetos ficam

[105] Os resultados dizem respeito aos produtos fornecidos e serviços prestados (exemplo: número de intercâmbios de estudantes financiados, número de quilómetros de estradas construídas, etc.).

[106] Tal como descrito no ponto 1.4.2. «Objetivo(s) específico(s)...»

interdependentes uns dos outros, é prudente evitar esta hipótese e orçamentar ações distintas. Este orçamento é um orçamento adicional ao custo de desenvolvimento, manutenção ou funcionamento do ECRIS-TCN em 2019 e 2020.

3.2.2.5. Impacto estimado nas dotações da DG Migração e Assuntos Internos

– ☐ A proposta/iniciativa não implica a utilização de dotações operacionais

– ☒ A proposta/iniciativa implica a utilização de dotações operacionais, tal como explicitado seguidamente:

Dotações de autorização em milhões de EUR (três casas decimais)

Indicar os objetivos e os resultados			Ano **2019**		Ano **2020**		Ano **2021**		Ano **2022**		Ano **2023**		Ano **2024**		Ano **2025**		Ano **2026**		Ano **2027**		**TOTAL**	
DG Migração e Assuntos Internos ⇩	Tipo 107	Custo médio	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	Não	Custo	N.º total	Custo total
Objetivo ESPECÍFICO N.º 1: Integração dos sistemas nacionais (Estado-Membro)																						
IUN prontas para utilização	Personalização das IUN — desenvolvimentos						30	3,150	30	3,150											30	6,300

[107] Os resultados dizem respeito aos produtos fornecidos e serviços prestados (exemplo: número de intercâmbios de estudantes financiados, número de quilómetros de estradas construídas, etc.).

Sistemas dos Estados-Membros adaptados para a interoperabilidade	Custos de integração					30	40,000	30	40,000	30	40,000									30	120,000
Utilizadores finais com formação	Um total de 10 000 sessões de utilizadores finais @ 1 000 EUR por sessão							5000	5,000	5000	5,000									10,000	10,000
Subtotal para o objetivo específico n.º 1							**43,150**		**48,150**		**45,000**										**136,300**

– O objetivo específico n.º 1 prende-se com os fundos disponibilizados aos Estados-Membros para tirar partido dos sistemas centrais interoperáveis. A IUN é personalizada tanto aquando da implementação do ESP como quando o MID ficar operacional. Cada Estado-Membro tem então uma alteração relativamente modesta (estimado em 150 dias-homem) para se adaptar a estes intercâmbios de mensagens atualizados com os sistemas centrais. É mais substancial a alteração do conteúdo dos dados introduzida pela interoperabilidade e que está abrangida em «custos de integração». Estes fundos destinam-se a lidar com as alterações do tipo de mensagens enviadas para o sistema central e para o tratamento das respostas. Para estimar os custos dessas alterações, é atribuído um orçamento de 4 milhões de euros por Estado-Membro. Este montante é igual ao do SES na medida em que existe uma quantidade comparável de trabalhos necessários à adaptação da integração dos sistemas nacionais com as IUN.

– Os utilizadores finais devem receber formação sobre os sistemas. Esta formação destinada a uma grande população de utilizadores finais será financiada com base num montante de 1 000 euros por sessão, de 10 a 20 utilizadores finais para o número estimado de 10 000 sessões que serão organizadas por todos os Estados-Membros nas suas próprias instalações.

3.2.3. Impacto estimado nos recursos humanos

3.2.3.1. Resumo da Agência GEFC

☐ A proposta/iniciativa não implica a utilização de dotações de natureza administrativa

☒ A proposta/iniciativa implica a utilização de dotações de natureza administrativa, tal como explicitado seguidamente:

Em milhões de EUR (até três casas decimais)

	Ano **2019**	Ano **2020**	Ano **2021**	Ano **2022**	Ano **2023**	Ano **2024**	Ano **2025**	Ano **2026**	Ano **2027**	**TOTAL**
Funcionários (Grau AD)										
Funcionários (grau AST)	0									
Agentes contratuais	0	0	0	0,350	1,400	0,233	0	0	0	1,983
Agentes temporários	0	0	0	0	0	0	0	0	0	0
Peritos nacionais destacados										
TOTAL	**0,0**	**0,0**	**0,0**	**0,350**	**1,400**	**0,233**	**0,0**	**0,0**	**0,0**	**1,983**

O trabalho que está previsto ser executado por estes efetivos adicionais afetados à GEFC é limitado no tempo (2023), mais precisamente a partir de 24 meses a contar da data de disponibilização do motor de busca biométrico para o SES. No entanto, o pessoal deve ser recrutado antecipadamente (foi calculada uma média de três meses), que explica o valor em 2022. O trabalho realizado é seguido de tarefas recapitulativas/de conclusão durante dois meses, o que explica o nível de pessoal em 2024.

O próprio nível de pessoal está baseado em 20 pessoas necessárias para realizar o trabalho (mais 10 pessoas fornecidas por uma empresa contratada e que se reflete no Título 3). Parte-se também do princípio que as tarefas irão decorrer durante um horário de trabalho alargado, sem estar limitado ao expediente normal. Parte-se do princípio que se poderá contar com os recursos da Agência para o fornecimento do pessoal de apoio e de gestão.

O número de efetivos baseia-se no pressuposto de que aproximadamente 550.000 impressões digitais terão de ser avaliadas, demorando uma média de 5 a 10 minutos por caso (controlo de 17 000 impressões por ano)[108].

Números de pessoal	2019	2020	2021	2022	2023	2024	2025	2026	2027	Total
Pessoal encarregue do tratamento manual das ligações e decisões	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3
Total Título 1 – AC	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3
Total Título 1 – AT	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Total Título 1	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3

.

3.2.3.2. Síntese da Europol

☐ A proposta/iniciativa não implica a utilização de dotações de natureza administrativa

☒ A proposta/iniciativa implica a utilização de dotações de natureza administrativa, tal como explicitado seguidamente:

Em milhões de EUR (até três casas decimais)

	Ano **2019**	Ano **2020**	Ano **2021**	Ano **2022**	Ano **2023**	Ano **2024**	Ano **2025**	Ano **2026**	Ano **2027**	**TOTAL**
Funcionários (Grau AD)										
Funcionários (grau AST)	0									
Agentes contratuais	0,000	0,070	0,070	0,560	0,560	0,560	0,560	0,560	0,560	3,500
Agentes temporários	0,690	1,932	1,932	0,621	0,621	0,414	0,414	0,414	0,414	7,452
Peritos nacionais destacados										
TOTAL	**0,690**	**2,002**	**2,002**	**1,181**	**1,181**	**0,974**	**0,974**	**0,974**	**0,974**	**10,952**

Estes custos foram calculados em função dos seguintes níveis de efetivos:

Número de ETC para as TIC	**2019**	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**TOTAL**
Agentes contratuais	0,0	1,0	1,0	8,0	8,0	8,0	8,0	8,0	8,0	50,0

[108] O pessoal para 2020 e para os anos seguintes é indicativo e terá de ser determinado se excede ou não o previsto para o pessoal da GEFC definido no documento COM(2015)671

Agentes temporários	5,0	14,0	14,0	4,5	4,5	3,0	3,0	3,0	3,0	54,0
Total do pessoal (ETC)	**5,0**	**15,0**	**15,0**	**12,5**	**12,5**	**11,0**	**11,0**	**11,0**	**11,0**	**104,0**

Prevê-se pessoal adicional especializado nas TIC para o reforço dos sistemas de informação da Europol, a fim de acolher o número crescente de consultas por parte do ESP e do ETIAS e, posteriormente, para manter os sistemas operacionais em permanência (24 sobre 24 horas e durante os 7 dias da semana).

– Para a fase de implementação do ESP (em 2020 e 2021) há uma necessidade adicional de peritos técnicos (arquitetos, engenheiros, agentes de desenvolvimento e de ensaios). A partir de 2022 haverá uma redução do número de técnicos necessários para implementar o resto dos componentes de interoperabilidade e manter os sistemas.

– A partir do segundo semestre de 2021, será implementado um sistema de monitorização TIC em permanência (24 sobre 24 horas e durante os 7 dias da semana) para assegurar níveis de serviço do ESP e do ETIAS. Esta operação será efetuada através de 2 agentes contratuais a trabalhar em 4 turnos em permanência (24 sobre 24 horas e durante os 7 dias da semana).

– Na medida do possível, os perfis foram repartidos entre agentes temporários e agentes contratuais. É de assinalar, contudo, que devido aos elevados requisitos de segurança, em vários lugares só é possível utilizar agentes temporários. O pedido de agentes temporários terá em conta os resultados da conciliação sobre o orçamento de 2018.

3.2.3.3. Síntese da CEPOL

☐ A proposta/iniciativa não implica a utilização de dotações de natureza administrativa

☒ A proposta/iniciativa implica a utilização de dotações de natureza administrativa, tal como explicitado seguidamente:

Em milhões de EUR (até três casas decimais)

	Ano **2019**	Ano **2020**	Ano **2021**	Ano **2022**	Ano **2023**	Ano **2024**	Ano **2025**	Ano **2026**	Ano **2027**	**TOTAL**
Funcionários (Grau AD)										
Funcionários (grau AST)										
Agentes contratuais			0,070	0,070						**0,140**

Agentes temporários		0,104	0,138	0,138	0,138	0,138	0,138	0,138	0,138	1,070
Peritos nacionais destacados										

TOTAL		**0,104**	**0,208**	**0,208**	**0,138**	**0,138**	**0,138**	**0,138**	**0,138**	**1,210**

É necessário pessoal adicional já que a formação de formadores dos Estados-Membros tem de ser especificamente desenvolvida com vista à utilização dos componentes de interoperabilidade em condições operacionais.

- O desenvolvimento de curricula e módulos de formação deve ter início pelo menos 8 meses antes da data em que o sistema está operacional. A formação terá o seu pico de intensidade nos dois primeiros anos depois de se tornar operacional. No entanto, terá que ser mantida por mais tempo para assegurar a implementação coerente, com base na experiência obtida com o sistema de informação Schengen.

- O pessoal adicional é necessário para se preparar, coordenar e implementar programas curriculares, cursos residenciais e cursos em linha. Estes cursos só poderão ser implementados adicionalmente ao catálogo de formação existente da CEPOL e, por conseguinte, é necessário pessoal adicional.

- Está previsto um agente temporário como gestor de curso ao longo do período de desenvolvimento e de manutenção que será apoiado por um agente contratual no período da organização de formação mais intenso.

3.2.3.4. Síntese da eu-LISA

☐ A proposta/iniciativa não implica a utilização de dotações de natureza administrativa

☒ A proposta/iniciativa implica a utilização de dotações de natureza administrativa, tal como explicitado seguidamente:

Em milhões de EUR (até três casas decimais)

	Ano **2019**	Ano **2020**	Ano **2021**	Ano **2022**	Ano **2023**	Ano **2024**	Ano **2025**	Ano **2026**	Ano **2027**	**TOTAL**
Funcionários (Grau AD)										
Funcionários (grau AST)										
Agentes contratuais	0,875	1,400	1,855	2,555	2,415	2,170	2,100	2,100	2,100	17,570

Agentes temporários	2,001	3,450	4,347	4,347	4,209	3,312	3,036	3,036	3,036	30,774
Peritos nacionais destacados										

TOTAL	**2,876**	**4,850**	**6,202**	**6,902**	**6,624**	**5,482**	**5,136**	**5,136**	**5,136**	**48,344**

– As necessidades de pessoal têm em conta que os quatro componentes e o CRRS constituem uma carteira de projetos com ligações (isto é, um programa). Para gerir as ligações entre projetos, é criada uma equipa de gestão do programa que inclua gestores do programa e de projeto e os perfis (muitas vezes referidos como arquitetos) que devem definir os elementos comuns entre eles. A realização do programa/projeto exige igualmente os perfis de apoio a programas e projetos.

– As necessidades de pessoal por projeto foram estimadas por analogia com os projetos anteriores (Sistema de Informação sobre Vistos) e distinguindo entre a fase de conclusão do projeto e a fase de exploração.

– Os perfis que têm de continuar durante a fase de exploração são recrutados como agentes temporários. Os perfis necessários durante a execução do programa/projeto são recrutados como agentes contratuais. A fim de assegurar a continuidade prevista das tarefas e para manter os conhecimentos na Agência, o número de lugares é quase 50/50 entre agentes temporários e agentes contratuais.

– Parte-se do pressuposto de que não haverá necessidade de qualquer pessoal adicional para realizar o projeto de elevada disponibilidade ECRIS-TCN e que o recrutamento de efetivos afetos ao projeto para a eu-LISA é efetuado através da reutilização de pessoal existente de projetos que são concluídos no mesmo período de tempo.

Estas estimativas baseiam-se nos seguintes efetivos:

Agentes contratuais:

3.2.1. Produtos da EU-LISA (é igual ao T1) no número de pessoas	2019	2020	2021	2022	2023	2024	2025	2026	2027	Total (fórmula)
Agentes contratuais										-
Gestão de programa/projeto	4,0	5,0	5,5	5,5	4,5	3,0	3,0	3,0	3,0	36,5
GP CRRS	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*1,5*
MID	*0,0*	*0,5*	*0,5*	*0,5*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*2,0*
Gabinete do programa/projeto	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*1,0*	*1,0*	*1,0*	*1,0*	*14,0*
Garantia de qualidade	*1,0*	*2,0*	*3,0*	*3,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*19,0*
Financiamento e aquisições	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Gestão financeira										*0,0*
Planificação e controlo orçamental										*0,0*
Gestão das aquisições/contratos	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Peritos técnicos	7,0	7,0	7,0	7,0	6,0	5,0	5,0	5,0	5,0	54,0
CRRS	*3,0*	*3,0*	*3,0*	*3,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*22,0*
ESP	*4,0*	*4,0*	*4,0*	*4,0*	*4,0*	*3,0*	*3,0*	*3,0*	*3,0*	*32,0*
BMS partilhado	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Testes	1,5	3,0	4,0	4,0	4,0	3,0	2,0	2,0	2,0	25,5
CRRS	*1,0*	*1,0*	*1,0*	*0,5*	*0,5*	*0,5*	*0,5*	*0,5*	*0,5*	*6,0*
ESP	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
BMS partilhado	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,5*	*1,0*	*2,0*	*2,5*	*2,5*	*1,5*	*1,0*	*1,0*	*1,0*	*13,0*
MID	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*0,5*	*0,5*	*0,5*	*6,5*
Monitorização dos sistemas	0,0	5,0	10,0	20,0	20,0	20,0	20,0	20,0	20,0	135,0
Comum (24:7)	0,0	*5,0*	*10,0*	*20,0*	*20,0*	*20,0*	*20,0*	*20,0*	*20,0*	*135,0*
Coordenação geral	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Recursos humanos	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
RH	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	*0,0*
Subtotal de agentes contratuais	**12,5**	**20,0**	**26,5**	**36,5**	**34,5**	**31,0**	**30,0**	**30,0**	**30,0**	**251,0**

Agentes temporários:

Agentes temporários										
Gestão de programa/projeto	3,0	4,0	5,5	5,5	5,5	4,5	4,0	4,0	4,0	40,0
Gestão do programa	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*9,0*
Gestão do projeto	*0,0*	*0,0*	*1,0*	*1,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*12,0*
Gabinete do programa/projeto	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*9,0*
ESP	*0,5*	*1,0*	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*3,0*
BMS partilhado	*0,5*	*0,5*	*0,5*	*1,0*	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*4,0*
CIR	*0,0*	*0,5*	*1,0*	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*3,0*
MID	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Financiamento e aquisições	3,0	3,0	4,0	4,0	4,0	4,0	4,0	4,0	4,0	34,0
Gestão financeira	*0,0*	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*7,0*
Planificação e controlo orçamental	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*9,0*
Gestão das aquisições/contratos	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*18,0*
Peritos técnicos	6,0	14,0	17,0	17,0	15,0	11,0	10,0	10,0	10,0	110,0
CRRS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
ESP	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
BMS partilhado	*2,0*	*3,0*	*5,0*	*5,0*	*5,0*	*3,0*	*3,0*	*3,0*	*3,0*	*32,0*
CIR	*2,0*	*5,0*	*5,0*	*5,0*	*3,0*	*3,0*	*3,0*	*3,0*	*3,0*	*32,0*
Segurança	*1,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*17,0*
MID	*0,0*	*2,0*	*2,0*	*2,0*	*2,0*	*1,0*	*1,0*	*1,0*	*1,0*	*12,0*
Arquitetos	*1,0*	*2,0*	*3,0*	*3,0*	*3,0*	*2,0*	*1,0*	*1,0*	*1,0*	*17,0*
Testes	2,5	3,0	4,0	4,0	4,0	2,5	2,0	2,0	2,0	26,0
CRRS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
ESP	*0,5*	*1,0*	*1,0*	*1,0*	*1,0*	*0,5*	*0,5*	*0,5*	*0,5*	*6,5*
BMS partilhado	*2,0*	*2,0*	*3,0*	*3,0*	*3,0*	*2,0*	*1,5*	*1,5*	*1,5*	*19,5*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
MID	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Monitorização dos sistemas	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
CRRS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
ESP	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
BMS partilhado	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
MID	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Formação	0,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	8,0
Formação	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*8,0*
Recursos humanos	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
RH	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	*0,0*
Outros	0,0	0,0	0,0	0,0	1,0	1,0	1,0	1,0	1,0	5,0
Especialista em proteção de dados	0,0	0,0	0,0	0,0	1,0	1,0	1,0	1,0	1,0	*5,0*
Subtotal de agentes temporários	**14,5**	**25,0**	**31,5**	**31,5**	**30,5**	**24,0**	**22,0**	**22,0**	**22,0**	**223,0**
Total	**27,0**	**45,0**	**58,0**	**68,0**	**65,0**	**55,0**	**52,0**	**52,0**	**52,0**	**474,0**

3.2.4. Impacto estimado nas dotações de natureza administrativa

3.2.4.1. DG Migração e Assuntos Internos: Síntese

– ☐ A proposta/iniciativa não implica a utilização de dotações de natureza administrativa

– ☒ A proposta/iniciativa implica a utilização de dotações de natureza administrativa, tal como explicitado seguidamente:

Em milhões de EUR (até três casas decimais)

	Ano **2019**	Ano **2020**	Ano **2021**	Ano **2022**	Ano **2023**	Ano **2024**	Ano **2025**	Ano **2026**	Ano **2027**	**TOTAL**
RUBRICA 5 do quadro financeiro plurianual										
Recursos humanos da DG MIGRAÇÃO E ASSUNTOS INTERNOS	0,690	0,690	0,690	0,690	0,690	0,690	0,276	0,276	0,276	4,968
Outras despesas administrativas	0,323	0,323	0,323	0,323	0,323	0,323	0,263	0,263	0,263	2,727
Subtotal da RUBRICA 5 do quadro financeiro plurianual	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695

Fora da RUBRICA 5[109] **do quadro financeiro plurianual**	(não utilizado)									
Recursos humanos										
Outras despesas de natureza administrativa										
Subtotal fora da RUBRICA 5 do quadro financeiro plurianual										

[109] Assistência técnica e/ou administrativa e despesas de apoio à implementação de programas e/ou ações da UE (antigas rubricas «BA»), investigação direta e indireta.

TOTAL	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**0,539**	**0,539**	**0,539**	**7,695**

.

3.2.4.2. Necessidades estimadas de recursos humanos

– ☐ A proposta/iniciativa não implica a utilização de recursos humanos.

– ☒ A proposta/iniciativa implica a utilização de recursos humanos, tal como explicitado seguidamente:

As estimativas devem ser expressas em termos de equivalente a tempo completo

	Ano **2019**	Ano **2020**	Ano **2021**	Ano **2022**	Ano **2023**	Ano **2024**	Ano **2025**	Ano **2026**	Ano **2027**	**TOTAL**
• Lugares do quadro do pessoal (funcionários e agentes temporários)										
18 01 01 01 (na sede e nos gabinetes de representação da Comissão) DG MIGRAÇÃO E ASSUNTOS INTERNOS	5,0	5,0	5,0	5,0	5,0	5,0	2,0	2,0	2,0	36,0
XX 01 01 02 (nas delegações)										
XX 01 05 01 (investigação indireta)										
10 01 05 01 (investigação direta)										
•Pessoal externo (em equivalente a tempo completo: ETC)[110]										
XX 01 02 02 (AC, AL, PND, TT e JPD nas delegações)										
XX 01 04 **yy** [111] - na sede										
XX 01 04 **yy** [111] - nas delegações										
XX 01 05 02 (AC, PND e TT — investigação indireta)										
10 01 05 02 (AC, PND e TT — Investigação direta)										
Outras rubricas orçamentais (especificar)										
TOTAL	**5,0**	**5,0**	**5,0**	**5,0**	**5,0**	**5,0**	**2,0**	**2,0**	**2,0**	**36,0**

18 constitui o domínio de ação ou título orçamental em causa.

As necessidades de recursos humanos serão cobertas pelos efetivos da DG já afetados à gestão da ação e/ou reafetados internamente a nível da DG, complementados, caso necessário, por eventuais dotações adicionais que sejam atribuídas à DG gestora no quadro do processo anual de atribuição e no limite das disponibilidades orçamentais.

Descrição das tarefas a executar:

Acompanhamento e seguimento dos projetos. Três funcionários para o acompanhamento. O pessoal trata de assumir as obrigações da Comissão na execução do programa: verificação da conformidade com a proposta legislativa, abordando questões de conformidade, elaboração de relatórios para o Parlamento Europeu e o Conselho, avaliando os progressos dos Estados-Membros. Dado que o programa é uma atividade adicional em comparação com o volume de trabalho existente, são necessários efetivos suplementares. Este aumento de pessoal é limitado em termos de duração e abrange apenas o período de desenvolvimento.

Gestão do UMF

[110] AC = agente contratual; AL = agente local; PND = Perito Nacional Destacado; TT = trabalhador temporário; JPD = jovem perito nas delegações.

[111] Sublimite para o pessoal externo coberto pelas dotações operacionais (antigas rubricas «BA»).

A Comissão irá gerir a norma UMF diariamente. São necessários dois funcionários para este efeito: uma pessoa como perito em matéria da aplicação da lei e outra pessoa com conhecimentos sólidos de modelos de atividade, bem como conhecimentos de TIC.

O Formato de Mensagem Universal (UMF) estabelece uma norma para o intercâmbio estruturado de informações transfronteiras entre os sistemas de informação, autoridades e/ou organizações no domínio da Justiça e Assuntos Internos. O UMF define um vocabulário e estruturas lógicas comuns para informações trocadas habitualmente, com o objetivo de facilitar a interoperabilidade ao permitir a criação e a leitura dos conteúdos do intercâmbio de forma consistente e equivalente em termos semânticos.

A fim de assegurar condições uniformes para a implementação do Formato de Mensagem Universal, propõe-se a atribuição de competências de execução à Comissão. Propõe-se que estas competências sejam exercidas em conformidade com o Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho, de 16 de fevereiro de 2011, que estabelece as regras e os princípios gerais relativos aos mecanismos de controlo pelos Estados-Membros do exercício das competências de execução pela Comissão

3.2.5. Compatibilidade com o atual quadro financeiro plurianual

– ☐ A proposta/iniciativa é compatível com o atual quadro financeiro plurianual

– ☒ A proposta/iniciativa requer uma reprogramação da rubrica pertinente do quadro financeiro plurianual.

Explicitar a reprogramação que é necessária, especificando as rubricas orçamentais em causa e as quantias correspondentes.

O Regulamento relativo ao FSI-Fronteiras é o instrumento financeiro no qual foi incluído o orçamento para a implementação da iniciativa de interoperabilidade.

No seu artigo 5.º, alínea b), prevê a aplicação de 791 milhões de EUR através de um programa para o desenvolvimento de sistemas informáticos, com base em sistemas informáticos existentes e/ou novos, de apoio à gestão dos fluxos migratórios nas fronteiras externas, sob reserva da adoção dos atos legislativos pertinentes da União e nos termos do artigo 15.º. Deste montante de 791 milhões de euros, 480,2 milhões de euros estão reservados ao desenvolvimento do SES, 210 milhões de euros para o ETIAS e 67,9 milhões de euros para a revisão do SIS II. O restante (32,9 milhões de euros) deverá ser reafetado através dos mecanismos FSI-Fronteiras. **A atual proposta prevê 32,1 milhões de EUR para o atual período do QFP, o que se coaduna com o orçamento restante.**

A conclusão da caixa acima sobre o montante necessário de 32,1 milhões de euros resulta da folha de cálculo seguinte:

AUTORIZAÇÕES										
3.2. Impacto estimado nas despesas DG MIGRAÇÃO E ASSUNTOS INTERNOS										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total (horiz)**
18 02 01 03 – Fronteiras inteligentes (abrange o apoio a Estados-Membros)	0	0	43,150	48,150	45,000	0	0	0	0	136,300
Total (1)	**0**	**0**	**43,150**	**48,150**	**45,000**	**0**	**0**	**0**	**0**	**136,300**
18.0207 -3.2. eu-LISA										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total (formula)**
T1: Despesas de pessoal	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
T2: Infraestruturas e despesas de funcionamento	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
T3: Despesas operacionais	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
Total (2)	**5,830**	**17,031**	**51,743**	**44,749**	**29,653**	**20,370**	**18,609**	**18,529**	**18,529**	**225,041**
		22,861							**202,181**	**225,041**
18.02.04 -3.2. Europol										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total(formula)**
T1: Despesas de pessoal	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
T2: Infraestruturas e despesas de funcionamento	0	0	0	0	0	0	0	0	0	0
T3: Despesas operacionais	0	6,380	6,380	2,408	2,408	2,408	7,758	7,758	2,408	37,908
Total (3)	**0,690**	**8,382**	**8,382**	**3,589**	**3,589**	**3,382**	**8,732**	**8,732**	**3,382**	**48,860**
		9,072							39,788	48,860
18/02/2005 -3.2. CEPOL										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total(formula)**
T1: Despesas de pessoal	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
T2: Infraestruturas e despesas de funcionamento	0	0	0	0	0	0	0	0	0	0
T3: Despesas operacionais	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
Total (4)	**0**	**0,144**	**0,384**	**0,482**	**0,208**	**0,208**	**0,208**	**0,208**	**0,208**	**2,050**
		0,144							**1,906**	**2,050**
18.02.0 -3.2. Frontex – GEFC										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total(formula)**
T1: Despesas de pessoal	0	0	0	0,350	1,400	0,233	0	0	0	1,983
T2: Infraestruturas e despesas de funcionamento	0	0	0	0,075	0,300	0,050	0	0	0	0,425
T3: Despesas operacionais	0	0	0	0,183	2,200	0	0	0	0	2,383
Total (5)	**0**	**0**	**0**	**0,608**	**3,900**	**0,283**	**0**	**0**	**0**	**4,792**
		0							**4,792**	**4,792**
TOTAL (1)+(2)+(3) +(4) +(5)	6,520	25,556	103,659	97,578	82,350	24,243	27,549	27,469	22,119	417,043
		32,076							384,966	
3.2. DG MIGRAÇÃO E ASSUNTOS INTERNOS Rubrica 5 «Despesas administrativas»										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total**
Total (6)	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695
TOTAL (1)+(2)+(3)+(4)+(5)+(6)	7,533	26,569	104,672	98,591	83,363	25,256	28,088	28,008	22,658	424,738

– ☐ A proposta/iniciativa requer a mobilização do Instrumento de Flexibilidade ou a revisão do quadro financeiro plurianual.

3.2.6. Participação de terceiros no financiamento

– A proposta/iniciativa **não** prevê o cofinanciamento por terceiros.

3.3. Impacto estimado nas receitas

– ☐ A proposta/iniciativa não tem impacto financeiro nas receitas.

– ☒ A proposta/iniciativa tem o impacto financeiro a seguir descrito:

– ☐ nos recursos próprios

– ☒ nas receitas diversas

Em milhões de EUR (até três casas decimais)

Rubrica orçamental das receitas:	Dotações disponíveis para o exercício em curso	Impacto da proposta/iniciativa[112]								
		Ano **2019**	Ano **2020**	Ano **2021**	Ano **2022**	Ano **2023**	Ano **2024**	Ano **2025**	Ano **2026**	Ano **2027**
Artigo 6313 - Contribuição de países associados de Schengen (Suíça, Noruega, Liechtenstein, Islândia).....		pm	pm	pm	pm	pm	pm	pm	pm	pm

Relativamente às receitas «afetadas» como diversas, especificar a(s) rubrica(s) orçamental(is) de despesas envolvida(s).

18.0207

Especificar o método de cálculo do impacto nas receitas.

O orçamento incluirá uma contribuição dos países associados à implementação, à aplicação e ao desenvolvimento do acervo de Schengen e às medidas relativas ao Eurodac, em conformidade com as condições estabelecidas nos respetivos acordos.

[112] No que respeita aos recursos próprios tradicionais (direitos aduaneiros e quotizações sobre o açúcar), as quantias indicadas devem ser apresentadas em termos líquidos, isto é, quantias brutas após dedução de 25 % a título de despesas de cobrança.