Jornal Oficial da União Europeia

L 135

Edição em língua portuguesa

Legislação

62.º ano

22 de maio de 2019

Índice

PT

Os atos cujos títulos são impressos em tipo fino são atos de gestão corrente adotados no âmbito da política agrícola e que têm, em geral, um período de validade limitado.

Os atos cujos títulos são impressos em tipo negro e precedidos de um asterisco são todos os restantes.

I

(Atos legislativos)

REGULAMENTOS

REGULAMENTO (UE) 2019/816 DO PARLAMENTO EUROPEU E DO CONSELHO

de 17 de abril de 2019

que cria um sistema centralizado para a determinação dos Estados-Membros que possuem informações sobre condenações de nacionais de países terceiros e de apátridas (ECRIS-TCN) tendo em vista completar o Sistema Europeu de Informação sobre Registos Criminais e que altera o Regulamento (UE) 2018/1726

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 82.º, n.º 1, segundo parágrafo, alínea d),

Tendo em conta a proposta da Comissão Europeia,

Após a transmissão do projeto de ato legislativo aos parlamentos nacionais,

Deliberando de acordo com o processo legislativo ordinário ([1]),

Considerando o seguinte:

(1) A União estabeleceu como objetivo proporcionar aos seus cidadãos um espaço de liberdade, segurança e justiça sem fronteiras internas, no qual esteja assegurada a livre circulação de pessoas. Esse objetivo deverá ser atingido, nomeadamente, através de medidas adequadas para prevenir e combater a criminalidade, incluindo a criminalidade organizada e o terrorismo.

(2) Esse objetivo exige que as informações relativas às decisões de condenação proferidas nos Estados-Membros sejam tomadas em consideração fora do Estado-Membro de condenação, tanto por ocasião de um novo processo penal, conforme previsto na Decisão-Quadro 2008/675/JAI do Conselho ([2]), como para prevenir novas infrações.

(3) Esse objetivo pressupõe o intercâmbio de informações extraídas dos registos criminais entre as autoridades competentes dos Estados-Membros. Tal intercâmbio de informações é organizado e facilitado pelas regras estabelecidas na Decisão-Quadro 2009/315/JAI do Conselho ([3]) e pelo sistema europeu de informação sobre os registos criminais (ECRIS), criado pela Decisão 2009/316/JAI do Conselho ([4]).

(4) Porém, o atual regime jurídico do ECRIS não tem suficientemente em conta as particularidades dos pedidos relativos a nacionais de países terceiros. Apesar de já ser possível o intercâmbio de informações sobre nacionais de países terceiros através do ECRIS, não existe na UE um procedimento ou mecanismo comum para o fazer com eficácia, rapidez e precisão.

(5) No interior da União, as informações sobre nacionais de países terceiros não são compiladas como acontece relativamente aos nacionais dos Estados-Membros no interior do Estado-Membro de nacionalidade, encontrando-se armazenadas apenas nos Estados-Membros onde foram proferidas as condenações. Por conseguinte, o quadro completo dos antecedentes criminais de nacionais de países terceiros só pode ser verificado se forem solicitadas informações a todos os Estados-Membros.

([1]) Posição do Parlamento Europeu de 12 de março de 2019 (ainda não publicada no Jornal Oficial) e decisão do Conselho de 9 de abril de 2019.

([2]) Decisão-Quadro 2008/675/JAI do Conselho, de 24 de julho de 2008, relativa à tomada em consideração das decisões de condenação nos Estados-Membros da União Europeia por ocasião de um novo procedimento penal (JO L 220 de 15.8.2008, p. 32).

([3]) Decisão-Quadro 2009/315/JAI do Conselho, de 26 de fevereiro de 2009, relativa à organização e ao conteúdo do intercâmbio de informações extraídas do registo criminal entre os Estados-Membros (JO L 93 de 7.4.2009, p. 23).

([4]) Decisão 2009/316/JAI do Conselho, de 6 de abril de 2009, relativa à criação do sistema europeu de informação sobre os registos criminais (ECRIS) em aplicação do artigo 11.º da Decisão-Quadro 2009/315/JAI (JO L 93 de 7.4.2009, p. 33).

(6) Tais pedidos genéricos implicam um encargo administrativo desproporcionado para todos os Estados-Membros, incluindo aqueles que não possuem informações sobre o nacional de um país terceiro em causa. Na prática, esse encargo dissuade os Estados-Membros de solicitarem a outros Estados-Membros informações sobre nacionais de países terceiros, o que resulta numa importante restrição ao intercâmbio de informações entre si, limitando o seu acesso a informações sobre o registo criminal às informações armazenadas nos seus registos nacionais. Em consequência, aumenta o risco de o intercâmbio de informações entre os Estados-Membros ser ineficaz e incompleto, o que, por sua vez, afeta o nível de segurança proporcionado aos cidadãos da União e às pessoas que nela residem.

(7) Para corrigir esta situação, deverá ser criado um sistema que permita às autoridades centrais dos Estados-Membros determinar com rapidez e eficácia que outros Estados-Membros possuem informações sobre registos criminais de nacionais de países terceiros (o «ECRIS-TCN»). Poderá então ser utilizado o regime atual do ECRIS para solicitar as informações do registo criminal desses Estados-Membros, nos termos da Decisão-Quadro 2009/315/JAI.

(8) O presente regulamento deverá, por conseguinte, estabelecer regras para a criação de um sistema centralizado a nível da União que contenha dados pessoais, e prever regras para a repartição de responsabilidades entre o Estado-Membro e o organismo responsável pelo seu desenvolvimento e gestão do sistema centralizado, bem como disposições específicas em matéria de proteção de dados que sejam necessárias para completar as disposições vigentes em matéria de proteção de dados e para prever um nível global adequado de proteção e segurança dos dados, e a defesa dos direitos fundamentais das pessoas em causa.

(9) O objetivo de proporcionar aos cidadãos da União um espaço de liberdade, segurança e justiça sem fronteiras internas, em que esteja assegurada a livre circulação de pessoas, exige também a posse de informações completas sobre condenações de cidadãos da União que tenham também a nacionalidade de um país terceiro. Dada a possibilidade de essas pessoas se apresentarem como tendo uma ou várias nacionalidades, e de poderem estar registadas diferentes condenações no Estado-Membro em que foram proferidas ou no Estado-Membro da nacionalidade, é necessário que o âmbito de aplicação do presente regulamento abranja os cidadãos da União que têm a nacionalidade de um país terceiro. A exclusão de tais pessoas levaria a que as informações armazenadas no ECRIS-TCN fossem incompletas e isso comprometeria a fiabilidade do sistema. No entanto, uma vez que tais pessoas têm a cidadania da União, as condições em que os dados dactiloscópicos relativos a essas pessoas podem ser inseridos no ECRIS-TCN deverão ser comparáveis às condições em que os dados dactiloscópicos dos cidadãos da União são trocados entre os Estados-Membros no âmbito do ECRIS, criado pela Decisão-Quadro 2009/315/JAI e pela Decisão 2009/316/JAI. Por conseguinte, no que diz respeito aos cidadãos da União que têm também a nacionalidade de um país terceiro, os dados datiloscópicos só deverão ser inseridos no ECRIS-TCN quando tenham sido recolhidos em conformidade com o direito nacional no decurso de processos penais, entendendo-se que, para tal inserção, os Estados-Membros deverão poder utilizar os dados datiloscópicos recolhidos para fins que não sejam o processo penal, se essa utilização for permitida nos termos do direito nacional.

(10) O ECRIS-TCN deverá permitir o tratamento de dados dactiloscópicos, a fim de determinar quais os Estados-Membros que possuem informações sobre os registos criminais de nacionais de países terceiros. Deverá permitir igualmente o tratamento de imagens faciais, a fim de confirmar a respetiva identidade. É essencial que a introdução e utilização de dados dactiloscópicos e de imagens faciais não exceda o estritamente necessário para alcançar o objetivo pretendido, devendo respeitar os direitos fundamentais, bem como o superior interesse da criança, e estar em conformidade com as regras da União aplicáveis em matéria de proteção de dados.

(11) A Agência da União Europeia para a Gestão Operacional de Sistemas Informáticos de Grande Escala no Espaço de Liberdade, Segurança e Justiça (eu-LISA), criada pelo Regulamento (UE) 2018/1726 do Parlamento Europeu e do Conselho ([5]), deverá ser incumbida da tarefa de desenvolver e gerir o ECRIS-TCN, tendo em conta a sua experiência na gestão de outros sistemas de grande escala no domínio da justiça e dos assuntos internos. O seu mandato deverá ser alterado de modo que reflita essas novas atribuições.

(12) A eu-LISA deverá ser dotada dos fundos e do pessoal necessários para cumprir as suas responsabilidades ao abrigo do presente regulamento.

(13) Tendo em conta a necessidade de criar ligações técnicas estreitas entre o ECRIS-TCN e o ECRIS, a eu-LISA deverá ser igualmente incumbida da tarefa de desenvolver e manter em condições de funcionamento a aplicação de referência do ECRIS, devendo o seu mandato ser alterado de modo que reflita essas alterações.

(14) Quatro Estados-Membros desenvolveram o seu próprio *software* nacional de aplicação do ECRIS, nos termos da Decisão 2009/316/JAI, e têm utilizado esse *software* em vez da aplicação de referência do ECRIS para o intercâmbio de informações sobre os registos criminais. Tendo em conta as características específicas que introduziram nos seus sistemas para uso nacional, bem como os investimentos que fizeram, esses Estados-Membros deverão poder utilizar o seu *software* nacional de aplicação do ECRIS também para efeitos do ECRIS-TCN, desde que respeitem as condições estabelecidas no presente regulamento.

([5]) Regulamento (UE) 2018/1726 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo à Agência da União Europeia para a Gestão Operacional de Sistemas Informáticos de Grande Escala no Espaço de Liberdade, Segurança e Justiça (eu-LISA), que altera o Regulamento (CE) n.º 1987/2006 e a Decisão 2007/533/JAI do Conselho, e que revoga o Regulamento (UE) n.º 1077/2011 (JO L 295 de 21.11.2018, p. 99).

(15) O ECRIS-TCN deverá conter apenas informações sobre a identidade de nacionais de países terceiros objeto de condenação por um tribunal penal da União. Essas informações relativas à identidade deverão incluir dados alfanuméricos e dactiloscópicos. Deverá ser possível inserir imagens faciais, na medida em que o direito do Estado-Membro em que a condenação é proferida permita a recolha e o armazenamento de imagens faciais de pessoas objeto de condenação.

(16) Os dados alfanuméricos a inserir pelos Estados-Membros no sistema central deverão incluir os apelidos, os nomes próprios da pessoa objeto de condenação, bem como, se a autoridade central dispuser dessas informações, os pseudónimos ou alcunhas da pessoa. Se o Estado-Membro em causa tiver conhecimento de dados pessoais divergentes – como um nome com uma ortografia diferente num outro alfabeto –, deverá ser possível inserir esses dados no sistema central a título de informação adicional.

(17) Os dados alfanuméricos deverão igualmente incluir, a título de informação adicional, o número de identificação ou o tipo e o número dos documentos de identificação da pessoa, bem como a designação da autoridade que emite esses documentos, se a autoridade central dispuser dessas informações. O Estado-Membro deverá procurar verificar a autenticidade dos documentos de identificação antes de introduzir as informações pertinentes no sistema central. Em todo o caso, uma vez que tais informações poderão não ser fiáveis, deverão ser tratadas com prudência.

(18) As autoridades centrais deverão utilizar o ECRIS-TCN para determinar o Estado-Membro ou Estados-Membros que possuem informações sobre os registos criminais de nacionais de países terceiros, quando forem solicitadas no Estado-Membro em causa informações dos registos criminais dessas pessoas para efeitos de processos penais contra elas instaurados, ou para os efeitos a que se refere o presente regulamento. Embora o ECRIS-TCN deva, em princípio, ser utilizado em todos estes casos, a autoridade responsável pelo processo penal deverá poder decidir não utilizar o ECRIS-TCN se essa utilização não for adequada, dadas as circunstâncias do processo, por exemplo, em certos tipos de processo penal urgente, em casos de trânsito, se a informação sobre o registo criminal tiver sido obtida recentemente através do ECRIS, ou em caso de infrações menores, especialmente infrações menores ao código da estrada, à regulamentação municipal geral ou à ordem pública.

(19) Se o direito nacional assim o previr, os Estados-Membros deverão ter também a possibilidade de utilizar o ECRIS-TCN para quaisquer outros fins não estabelecidos no presente regulamento nos termos do direito nacional e se este assim o previr. No entanto, a fim de aumentar a transparência da utilização do ECRIS-TCN, os Estados-Membros deverão notificar esses outros fins à Comissão, a qual deverá assegurar a publicação de todas as notificações no *Jornal Oficial da União Europeia*.

(20) Deverá igualmente ser possível que quaisquer outras autoridades que requeiram informações dos registos criminais determinem que o ECRIS-TCN não seja utilizado quando tal não for adequado dadas as circunstâncias do processo, por exemplo, quando for necessário verificar as qualificações profissionais de uma pessoa através de determinados controlos administrativos normalizados, especialmente se se souber que não irão ser solicitadas informações sobre registos criminais a outros Estados-Membros, independentemente do resultado da pesquisa no ECRIS-TCN. No entanto, o ECRIS-TCN deverá ser sempre utilizado se o pedido de informações do registo criminal tiver sido apresentado por uma pessoa que solicite informações sobre o seu próprio registo criminal, em conformidade com a Decisão-Quadro 2009/315/JAI, ou se o pedido for feito para obter informações constantes do registo criminal em conformidade com a Diretiva 2011/93/UE do Parlamento Europeu e do Conselho ([6]).

(21) Os nacionais de países terceiros deverão ter direito a obter informações por escrito sobre o seu próprio registo criminal nos termos do direito do Estado-Membro no qual solicitam o fornecimento dessas informações e nos termos da Decisão-Quadro 2009/315/JAI. Antes de fornecer essas informações a nacionais de países terceiros, o Estado-Membro em causa deverá consultar o ECRIS-TCN.

(22) Os cidadãos da União que tenham também a nacionalidade de um país terceiro só serão inseridos no sistema ECRIS-TCN se as autoridades competentes tiverem conhecimento de que essas pessoas têm a nacionalidade de um país terceiro. Pode acontecer que cidadãos da União tenham sido anteriormente condenados como nacionais de um país terceiro, sem que as autoridades competentes tenham conhecimento de que esses cidadãos têm também a nacionalidade de um país terceiro. A fim de assegurar que as autoridades competentes tenham uma visão completa dos registos criminais, deverá ser possível consultar o sistema ECRIS-TCN para verificar se, no que diz respeito a um cidadão da União, algum Estado-Membro possui informações sobre o seu registo criminal como nacional de um país terceiro.

(23) No caso de haver correspondência entre os dados registados no sistema central e os utilizados para a pesquisa por um Estado-Membro (resposta positiva), as informações sobre a identidade para as quais se registou «resposta positiva» deverão acompanhar a resposta positiva. O resultado das pesquisas deverá ser utilizado pelas autoridades centrais, apenas para fazer pedidos através do ECRIS ou, pela Agência da União Europeia para

([6]) Diretiva 2011/93/UE do Parlamento Europeu e do Conselho, de 13 de dezembro de 2011, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, e que substitui a Decisão-Quadro 2004/68/JAI do Conselho (JO L 335 de 17.12.2011, p. 1).

a Cooperação Judiciária Penal (Eurojust), criada pelo Regulamento (UE) 2018/1727 do Parlamento Europeu e do Conselho ([7]), à pela Agência da União Europeia para a Cooperação Policial (Europol), criada pelo Regulamento (UE) 2016/794 do Parlamento Europeu e do Conselho ([8]) e pela Procuradoria Europeia (a «EPPO»), criada pelo Regulamento (UE) 2017/1939 ([9]), apenas para apresentar um pedido de informações sobre condenações, conforme referido no presente regulamento.

(24) Numa primeira fase, as imagens faciais inseridas no ECRIS-TCN só deverão ser utilizadas para efeitos de confirmação da identidade de um nacional de um país terceiro a fim de identificar o Estado-Membro ou Estados-Membros que possuem informações sobre condenações anteriores desse nacional de um país terceiro. No futuro, deverá ser possível que as imagens faciais possam ser utilizadas para fins de correspondência biométrica automatizada, desde que sejam cumpridos os requisitos técnicos e estratégicos para esse efeito. Tendo em conta a necessidade e a proporcionalidade, bem como a evolução técnica no domínio do *software* de reconhecimento facial, a Comissão deverá avaliar a disponibilidade e o grau de preparação da tecnologia exigida antes de adotar um ato delegado relativo à utilização de imagens faciais para efeitos de identificação de nacionais de países terceiros, a fim de identificar o Estado-Membro ou Estados-Membros que possuem informações sobre condenações anteriores relativas a essas pessoas.

(25) A utilização de dados biométricos é necessária, pois é o método mais fiável de identificação de nacionais de países terceiros no território dos Estados-Membros, que, muitas vezes, não possuem documentos nem quaisquer outros meios de identificação, permitindo também estabelecer uma correspondência mais fiável entre os dados relativos a nacionais de países terceiros.

(26) Os Estados-Membros deverão inserir no sistema central os dados datiloscópicos de nacionais de países terceiros objeto de condenação que tenham sido recolhidos em processos penais nos termos do direito nacional. Para que o sistema central contenha informações sobre a identidade tão completas quanto possível, os Estados-Membros deverão também poder inserir no sistema central os dados datiloscópicos que tenham sido recolhidos para outros fins que não sejam o processo penal, se esses os dados datiloscópicos puderem ser utilizados em processos penais em conformidade com o direito nacional.

(27) O presente regulamento deverá estabelecer critérios mínimos no que respeita aos os dados datiloscópicos que os Estados-Membros deverão inserir no sistema central. Os Estados-Membros deverão poder escolher entre a introdução de os dados datiloscópicos de nacionais de países terceiros que tenham sido condenados a uma pena de prisão de pelo menos seis meses, e a introdução de os dados datiloscópicos de nacionais de países terceiros que tenham sido condenados por um crime punível, ao abrigo da legislação do Estado-Membro em causa, com pena de prisão máxima de pelo menos 12 meses.

(28) Os Estados-Membros deverão criar no ECRIS-TCN registos relativos a nacionais de países terceiros objeto de condenação, devendo fazê-lo de forma automática, quando possível, e sem demora injustificada após a sua condenação ter sido inscrita no registo criminal nacional. Os Estados-Membros deverão, em conformidade com o presente regulamento, inserir no sistema central dados alfanuméricos e dactiloscópicos relativos a condenações proferidas após a data de início da introdução de dados no ECRIS-TCN. A partir da mesma data, e depois em qualquer altura, os Estados-Membros deverão poder inserir imagens faciais no sistema central.

(29) Os Estados-Membros deverão igualmente, nos termos do presente regulamento, criar no ECRIS-TCN registos relativos a nacionais de países terceiros objeto de condenação antes da data de início da introdução de dados, a fim de assegurar a máxima eficácia do sistema. No entanto, para esse efeito, os Estados-Membros não deverão ser obrigados a recolher informações que não estejam ainda nos respetivos registos criminais antes da data de início da introdução de dados. As os dados datiloscópicos de nacionais de países terceiros recolhidos e relativos a essas condenações anteriores só deverão ser inseridas se tiverem sido recolhidas em processos penais e se o Estado-Membro em causa considerar que é possível estabelecer uma correspondência clara com outras informações sobre a identidade que constem do registo criminal.

(30) A melhoria do intercâmbio das informações sobre as condenações penais deverá ajudar os Estados-Membros na aplicação da Decisão-Quadro 2008/675/JAI, a qual obriga os Estados-Membros a tomarem em consideração as condenações anteriores proferidas noutros Estados-Membros por ocasião de um novo processo penal, na medida em que as condenações nacionais anteriores sejam tomadas em consideração nos termos do direito nacional.

([7]) Regulamento (UE) 2018/1727 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, que cria a Agência da União Europeia para a Cooperação Judiciária Penal (Eurojust), e que substitui e revoga a Decisão 2002/187/JAI do Conselho (JO L 295 de 21.11.2018, p. 138).

([8]) Regulamento (UE) 2016/794 do Parlamento Europeu e do Conselho, de 11 de maio de 2016, que cria a Agência da União Europeia para a Cooperação Policial (Europol) e que substitui e revoga as Decisões 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI e 2009/968/JAI do Conselho (JO L 135 de 24.5.2016, p. 53).

([9]) Regulamento (UE) 2017/1939 do Conselho, de 12 de outubro de 2017, que dá execução a uma cooperação reforçada para a instituição da Procuradoria Europeia (JO L 283 de 31.10.2017, p. 1).

(31) Uma resposta positiva indicada pelo ECRIS-TCN não deverá, por si só, ser interpretada como prova de que o nacional do país terceiro em causa tenha sido condenado nos Estados-Membros indicados. A existência de condenações anteriores só deverá ser confirmada com base nas informações recebidas dos registos criminais dos Estados-Membros em causa.

(32) Não obstante a possibilidade de recorrer a programas financeiros da União de acordo com as regras aplicáveis, cada Estado-Membro deverá suportar as suas próprias despesas decorrentes da execução, gestão, utilização e manutenção da sua base de dados dos registos criminais e das bases nacionais de dados dactiloscópicos, e da execução, gestão, utilização e manutenção das adaptações técnicas necessárias para poder utilizar o ECRIS-TCN, incluindo as conexões ao ponto de acesso central nacional.

(33) A Eurojust, a Europol e a EPPO deverão ter acesso ao ECRIS-TCN com vista a determinar o Estado-Membro ou Estados-Membros que possuem informações sobre os registos criminais de nacionais de países terceiros, em apoio ao exercício das suas funções legais. A Eurojust deverá também ter acesso direto ao ECRIS-TCN com vista ao exercício da sua função, ao abrigo do presente regulamento, de funcionar como ponto de contacto para os países terceiros e as organizações internacionais, sem prejuízo da aplicação dos princípios da cooperação judiciária em matéria penal, nomeadamente as regras aplicáveis ao auxílio judiciário mútuo. Embora deva ser tida em conta a posição dos Estados-Membros que não participam na cooperação reforçada para a criação da EPPO, não deverá ser recusado à EPPO o acesso às informações sobre condenações com o único fundamento de que o Estado-Membro em causa não participa na cooperação reforçada.

(34) O presente regulamento estabelece regras rigorosas de acesso ao ECRIS-TCN e as salvaguardas necessárias, incluindo a responsabilidade dos Estados-Membros no domínio da recolha e utilização de dados. Estabelece igualmente a forma como cada um pode exercer os seus direitos a indemnização, acesso, retificação, supressão e recurso, nomeadamente o direito a um recurso judicial efetivo e a supervisão das operações de tratamento por autoridades públicas independentes. Por conseguinte, o regulamento respeita os direitos e as liberdades fundamentais e observa os princípios consagrados, em especial, na Carta dos Direitos Fundamentais da União Europeia, incluindo o direito à proteção dos dados pessoais, o princípio da igualdade perante a lei e a proibição geral de discriminação. Neste sentido, o regulamento tem também em conta a Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais, o Pacto Internacional sobre os Direitos Civis e Políticos e outras obrigações em matéria de direitos humanos em conformidade com o direito internacional.

(35) A Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho ([10]) deverá aplicar-se ao tratamento de dados pessoais por parte das autoridades nacionais competentes com vista à prevenção, investigação, deteção ou instauração de processo penal contra infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública. O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ([11]) deverá ser aplicável ao tratamento de dados pessoais por autoridades nacionais quando tal tratamento não seja abrangido pelo âmbito de aplicação da Diretiva (UE) 2016/680. A supervisão coordenada deverá ser assegurada em conformidade com o Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho ([12]), o qual deverá também ser aplicável ao tratamento de dados pessoais pela eu-LISA.

(36) Relativamente às condenações anteriores, as autoridades centrais deverão inserir os dados alfanuméricos até ao final do prazo para a introdução de dados ao abrigo do presente regulamento, e os dados dactiloscópicos no prazo de dois anos após a data de entrada em funcionamento do ECRIS-TCN. Os Estados-Membros deverão poder inserir todos os dados em simultâneo, desde que esses prazos sejam cumpridos.

(37) Deverão ser estabelecidas regras relativas à responsabilidade dos Estados-Membros, da Eurojust, da Europol, da EPPO e da eu-LISA por danos resultantes do incumprimento do presente regulamento.

(38) A fim de melhorar a determinação do Estado-Membro ou Estados-Membros que possuem informações sobre condenações anteriores de nacionais de países terceiros, o poder de adotar atos nos termos do artigo 290.º do Tratado sobre o Funcionamento da União Europeia (TFUE) deverá ser delegado na Comissão no que respeita à complementação do presente regulamento com disposições sobre a utilização de imagens faciais para efeitos de identificação de nacionais de países terceiros com vista a identificar o Estado-Membro ou Estados-Membros que possuem informações sobre condenações anteriores. É particularmente importante que a Comissão proceda às consultas adequadas durante os trabalhos preparatórios, inclusive ao nível de peritos, e que essas consultas sejam

([10]) 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 e repressão de infrações penais ou de 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).

([11]) 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).

([12]) Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais por parte das instituições, órgãos, organismos e agências da União e à livre circulação desses dados e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (JO L 295 de 21.11.2018, p. 39).

conduzidas de acordo com os princípios estabelecidos no Acordo Interinstitucional, de 13 de abril de 2016, sobre legislar melhor ([13]). Em especial, a fim de assegurar a igualdade de participação na preparação dos atos delegados, o Parlamento Europeu e o Conselho recebem todos os documentos ao mesmo tempo que os peritos dos Estados-Membros e os respetivos peritos têm sistematicamente acesso às reuniões dos grupos de peritos da Comissão que tratem da preparação dos atos delegados.

(39) A fim de assegurar condições uniformes para a criação e gestão operacional do ECRIS-TCN, deverão ser atribuídas competências de execução à Comissão. Essas competências deverão ser exercidas nos termos do Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho ([14]).

(40) Os Estados-Membros deverão tomar as medidas necessárias para dar cumprimento ao presente regulamento o mais rapidamente possível, a fim de assegurar o bom funcionamento do ECRIS-TCN, tendo em conta o tempo de que a eu-LISA precisa para desenvolver e implementar o ECRIS-TCN. No entanto, os Estados-Membros deverão dispor de pelo menos 36 meses a contar da entrada em vigor do presente regulamento para tomar as medidas necessárias para lhe dar cumprimento.

(41) Atendendo a que o objetivo do presente regulamento, a saber o intercâmbio rápido e eficaz de informações precisas sobre registos criminais de nacionais de países terceiros, não pode ser suficientemente alcançado pelos Estados-Membros, mas pode, mediante a definição de regras comuns, ser mais bem alcançado ao nível da União, esta pode tomar medidas em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do Tratado da União Europeia. De acordo com o princípio da proporcionalidade consagrado no mesmo artigo, o presente regulamento não excede o necessário para alcançar aquele objetivo.

(42) Nos termos dos artigos 1.º e 2.º do Protocolo n.º 22 relativo à posição da Dinamarca, anexo ao TUE e ao TFUE, a Dinamarca não participa na adoção do presente regulamento e não fica a ele vinculada nem sujeita à sua aplicação.

(43) Nos termos dos artigos 1.º e 2.º e do artigo 4.º-A, n.º 1, do Protocolo n.º 21 relativo à posição do Reino Unido e da Irlanda em relação ao espaço de liberdade, segurança e justiça, anexo ao TUE e ao TFUE, e sem prejuízo do artigo 4.º do referido protocolo, a Irlanda não participa na adoção do presente regulamento e não fica a ele vinculada nem sujeita à sua aplicação.

(44) Nos termos do artigo 3.º e do artigo 4.º-A, n.º 1, do Protocolo n.º 21, o Reino Unido notificou a sua intenção de participar na adoção e na aplicação do presente regulamento.

(45) A Autoridade Europeia para a Proteção de Dados foi consultada em conformidade com o artigo 28.º, n.º 2, do Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho ([15]), tendo emitido o seu parecer em 12 de dezembro de 2017 ([16]),

ADOTARAM O PRESENTE REGULAMENTO:

CAPÍTULO I

Disposições gerais

Artigo 1.º

Objeto

O presente regulamento estabelece:

a) Um sistema que permite determinar o Estado-Membro ou Estados-Membros que possuem informações sobre condenações anteriores de nacionais de países terceiros (o «ECRIS-TCN»);

b) As condições em que o ECRIS-TCN deve ser utilizado pelas autoridades centrais para obterem informações sobre as condenações anteriores através do sistema europeu de informação sobre registos criminais (ECRIS), criado pela Decisão 2009/316/JAI, e as condições em que a Eurojust, a Europol e a EPPO devem utilizar o ECRIS-TCN.

([13]) JO L 123 de 12.5.2016, p. 1.
([14]) 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).
([15]) 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).
([16]) JO C 55 de 14.2.2018, p. 4.

Artigo 2.º

Âmbito de aplicação

O presente regulamento aplica-se ao tratamento de informações sobre a identidade de nacionais de países terceiros que tenham sido objeto de condenações nos Estados-Membros, a fim de determinar os Estados-Membros onde essas condenações foram proferidas. Com exceção do artigo 5.º, n.º 1, alínea b), subalínea ii), as disposições do presente regulamento aplicáveis aos nacionais de países terceiros aplicam-se igualmente aos cidadãos da União que também tenham a nacionalidade de um país terceiro e que tenham sido objeto de condenações nos Estados-Membros.

Artigo 3.º

Definições

Para efeitos do presente regulamento, entende-se por:

1) «Condenação», qualquer decisão definitiva de um tribunal penal contra uma pessoa singular devido a uma infração penal, na medida em que a decisão conste do registo criminal do Estado-Membro de condenação;

2) «Processo penal», a fase anterior ao julgamento, a fase do julgamento e a fase de execução da condenação;

3) «Registo criminal», o registo ou registos nacionais em que estão inscritas as condenações nos termos do direito nacional;

4) «Estado-Membro de condenação», o Estado-Membro em que é pronunciada uma condenação;

5) «Autoridade central», uma autoridade designada em conformidade com o artigo 3.º, n.º 1, da Decisão-Quadro 2009/315/JAI;

6) «Autoridades competentes», as autoridades centrais e a Eurojust, a Europol e EPPO), que são competentes para, em conformidade com o presente regulamento, aceder ao ECRIS-TCN ou consultá-lo;

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

8) «Sistema central», a base ou bases de dados, desenvolvidas e geridas pela eu-LISA, que contêm informações sobre a identidade de nacionais de países terceiros que tenham sido objeto de condenações nos Estados-Membros;

9) «*Software* de interface», o *software* utilizado pelas autoridades competentes que lhes permite aceder ao sistema central através da infraestrutura de comunicação referida no artigo 4.º, n.º 1, alínea d);

10) «Informações sobre a identidade», os dados alfanuméricos, os dados dactiloscópicos e as imagens faciais utilizadas para estabelecer a correspondência entre esses dados e uma pessoa singular;

11) «Dados alfanuméricos», os dados representados por letras, dígitos, carateres especiais, espaços e sinais de pontuação;

12) «Dados dactiloscópicos», os dados relativos às impressões digitais planas e roladas de todos os dedos de uma pessoa;

13) «Imagem facial», a imagem digital do rosto de uma pessoa;

14) «Resposta positiva», a concordância ou concordâncias determinadas pela comparação entre as informações sobre a identidade registadas no sistema central e as informações sobre a identidade utilizadas numa pesquisa;

15) «Ponto de acesso central nacional», o ponto nacional de ligação à infraestrutura de comunicação referida no artigo 4.º, n.º 1, alínea d);

16) «Aplicação de referência do ECRIS», o *software* desenvolvido pela Comissão e disponibilizado aos Estados-Membros para o intercâmbio de informações sobre registos criminais através do ECRIS.

17) «Autoridade nacional de controlo», uma autoridade pública independente criada por um Estado-Membro nos termos das regras da União aplicáveis em matéria de proteção de dados;

18) «Autoridades de controlo», a Autoridade Europeia para a Proteção de Dados e as autoridades nacionais de controlo.

Artigo 4.º

Arquitetura técnica do ECRIS-TCN

1. O ECRIS-TCN é composto por:

a) Um sistema central em que são armazenadas informações sobre a identidade de nacionais de países terceiros objeto de condenação;

b) Um ponto de acesso central nacional em cada Estado-Membro;

c) Um *software* de interface que permite a conexão das autoridades competentes ao sistema central através do ponto de acesso central nacional e da infraestrutura de comunicação referida na alínea d);

d) Uma infraestrutura de comunicação entre o sistema central e os pontos de acesso central nacional.

2. O sistema central é acolhido pela eu-LISA nas suas instalações técnicas.

3. O *software* de interface é integrado na aplicação de referência do ECRIS. Os Estados-Membros utilizam a aplicação de referência do ECRIS ou, na situação e nas condições descritas nos n.os 4 a 8, o *software* nacional de aplicação do ECRIS, para consultar o ECRIS-TCN e para enviar pedidos posteriores de informações sobre registos criminais.

4. Os Estados-Membros que utilizem o seu *software* nacional de aplicação do ECRIS são responsáveis por assegurar que este permita que as autoridades responsáveis pelo registo criminal nacional utilizem o ECRIS-TCN, com exceção do *software* de interface, em conformidade com o presente regulamento. Para esse efeito, antes da data da entrada em funcionamento do ECRIS-TCN e em conformidade com o artigo 35.º, n.º 4, esses Estados-Membros asseguram que o seu *software* nacional de aplicação do ECRIS funcione em conformidade com os protocolos e as especificações técnicas estabelecidas nos atos de execução a que se refere o artigo 10.º, e com quaisquer outros requisitos técnicos adicionais definidos pela eu-LISA nos temos do presente regulamento e baseados nesses atos de execução.

5. Enquanto não utilizarem a aplicação de referência do ECRIS, os Estados-Membros que utilizem o seu *software* nacional de aplicação do ECRIS garantem também, sem demora injustificada, que sejam aplicadas ao seu *software* nacional de aplicação do ECRIS eventuais adaptações técnicas subsequentes exigidas por qualquer alteração às especificações técnicas introduzida nos atos de execução a que se refere o artigo 10.º, ou a alterações a quaisquer outros requisitos técnicos adicionais definidos pela eu-LISA nos temos do presente regulamento e baseados nesses atos de execução.

6. Os Estados-Membros que utilizem o seu *software* nacional de aplicação do ECRIS suportam todas as despesas decorrentes da implementação, manutenção e desenvolvimento desse *software* e da sua interligação ao ECRIS-TCN, com exceção do *software* de interface.

7. Se um Estado-Membro que utilize o seu *software* nacional de aplicação do ECRIS não puder cumprir as obrigações que lhe incumbem por força do presente artigo, é obrigado a utilizar a aplicação de referência do ECRIS, incluindo o *software* de interface integrado para utilizar o ECRIS-TCN.

8. Tendo em conta a avaliação a realizar pela Comissão nos termos do artigo 36.º, n.º 10, alínea b), os Estados-Membros em causa fornecem à Comissão todas as informações necessárias.

CAPÍTULO II

Introdução e utilização de dados pelas autoridades centrais

Artigo 5.º

Introdução de dados no ECRIS-TCN

1. Para cada nacional de país terceiro objeto de condenação, a autoridade central do Estado-Membro de condenação cria um ficheiro correspondente no sistema central. Esse ficheiro inclui:

a) No que respeita a dados alfanuméricos:

i) informações a incluir a menos que, em casos individuais, essas informações não sejam do conhecimento da autoridade central (informações obrigatórias):

— apelidos;

— nomes próprios;

— data de nascimento;

— local de nascimento (localidade e país);

— nacionalidade ou nacionalidades;

— sexo;

— nomes anteriores, se aplicável;

— o código do Estado-Membro de condenação,

ii) informações a incluir se tiverem sido inscritas no registo criminal (informações facultativas):

— filiação,

iii) informações a incluir se a autoridade central delas dispuser (informações adicionais):

— número de identificação ou tipo e número dos documentos de identificação da pessoa, bem como a designação da entidade emissora;

— pseudónimos ou alcunhas;

b) No que respeita a dados dactiloscópicos:

i) dados dactiloscópicos de nacionais de países terceiros que tenham sido recolhidos nos termos do direito nacional em processo penal;

ii) no mínimo, dados dactiloscópicos recolhidos com base em qualquer dos seguintes critérios:

— quando o nacional de país terceiro tiver sido condenado a uma pena de prisão de pelo menos seis meses;

ou

— quando o nacional de país terceiro tiver sido condenado por um crime punível nos termos do direito do Estado-Membro com pena de prisão máxima de pelo menos 12 meses;

2. Os dados dactiloscópicos a que se refere o n.º 1, alínea b), do presente artigo devem ter especificações técnicas relativas à qualidade, resolução e tratamento de dados dactiloscópicos previstos no ato de execução a que se refere o artigo 10.º, n.º 1, alínea b). O número de referência dos dados dactiloscópicos da pessoa objeto de condenação deve incluir o código do Estado-Membro de condenação.

3. O ficheiro pode igualmente incluir imagens faciais do nacional de país terceiro objeto de condenação quando a legislação do Estado-Membro de condenação permita a recolha e o armazenamento de imagens faciais de pessoas objeto de condenação.

4. O Estado-Membro de condenação cria o ficheiro automaticamente, se possível, e sem demora injustificada, após o averbamento da condenação no registo criminal.

5. Os Estados-Membros de condenação criam também ficheiros relativos às condenações proferidas antes da data da introdução dos dados em conformidade com o artigo 35.º, n.º 1, na medida em que dados relativos a pessoas objeto de condenação estejam armazenados nas suas bases de dados nacionais. Nesses casos, os dados dactiloscópicos apenas são inseridos se tiverem sido recolhidos em processo penal nos termos do direito nacional e se puder ser claramente determinada a sua concordância com outras informações sobre a identidade constantes dos registos criminais.

6. A fim de cumprir as obrigações previstas no n.º 1, alínea b), subalíneas i) e ii), e no n.º 5, os Estados-Membros podem utilizar dados dactiloscópicos recolhidos para fins que não sejam o processo penal, se essa utilização for permitida nos termos do direito nacional.

Artigo 6.º

Imagens faciais

1. Até à entrada em vigor do ato delegado previsto no n.º 2, as imagens faciais podem ser utilizadas exclusivamente para confirmar a identidade do nacional de país terceiro que tenha sido identificado em resultado de uma pesquisa alfanumérica ou de uma pesquisa com recurso a dados dactiloscópicos.

2. A Comissão fica habilitada a adotar atos delegados em conformidade com o artigo 37.º que completem o presente regulamento no que respeita à utilização de imagens faciais para efeitos da identificação de cidadãos de países terceiros, a fim de identificar o Estado-Membro ou Estados-Membros que possuem informações sobre condenações anteriores no que respeita a essas pessoas quando se tornar tecnicamente possível. Antes de exercer esta competência delegada, a Comissão, tendo em conta a necessidade e a proporcionalidade, bem como a evolução técnica no domínio do *software* de reconhecimento facial, avalia a disponibilidade e o estado de desenvolvimento da tecnologia necessária.

Artigo 7.º

Utilização do ECRIS-TCN para determinar o Estado-Membro ou Estados-Membros que possuem informações sobre registos criminais

1. As autoridades centrais utilizam o ECRIS-TCN para determinar os Estados-Membros que possuem informações sobre os registos criminais de um nacional de país terceiro, de modo que obtenha informações sobre anteriores condenações através do ECRIS, caso sejam exigidas no Estado-Membro em causa informações sobre o registo criminal da referida pessoa para efeitos de processo penal contra ela instaurado ou para qualquer uma das seguintes finalidades, nos termos do direito nacional e se este assim o previr:

— verificação do registo criminal dessa pessoa, efetuada a seu pedido;

— credenciações de segurança;

— obtenção de licenças ou autorizações;

— verificações para efeitos de emprego;

— verificações para atividades de voluntariado que impliquem contactos diretos e regulares com crianças ou pessoas vulneráveis;

— procedimentos ligados a vistos, à aquisição de cidadania e à migração, incluindo os procedimentos de asilo; e

— verificações relacionadas com contratos públicos e concursos públicos.

No entanto, em casos específicos, para além dos casos em que o nacional de país terceiro peça à autoridade central informações sobre o seu próprio registo criminal, ou em que o pedido seja feito para obter informações sobre registos criminais nos termos do artigo 10.º, n.º 2, da Diretiva 2011/93/UE, a autoridade que requer as informações sobre os registos criminais pode determinar que essa utilização do ECRIS-TCN não é adequada.

2. Os Estados-Membros que decidam, nos termos do direito nacional e se este assim o previr, utilizar o ECRIS-TCN para eventuais finalidades diferentes das enunciadas no n.º 1, a fim de obter informações sobre condenações anteriores através do ECRIS, notificam a Comissão Europeia até à data da entrada em funcionamento referida no artigo 35.º, n.º 4, ou a qualquer momento subsequente, dessas outras finalidades e de eventuais alterações às mesmas. A Comissão publica tais notificações no *Jornal Oficial da União Europeia* no prazo de 30 dias após a receção das notificações.

3. A Eurojust, a Europol e a EPPO estão habilitadas a consultar o ECRIS-TCN para identificar o Estado-Membro ou Estados-Membros que possuem informações sobre os registos criminais de um nacional de um país terceiro, em conformidade com os artigos 14.º a 18.º. Todavia não introduzem, retificam nem apagam nenhuns dados do ECRIS--TCN.

4. Para os efeitos referidos nos n.ºs 1, 2 e 3, as autoridades competentes também podem consultar o ECRIS-TCN para verificar se, relativamente a um cidadão da União, algum Estado-Membro possui informações sobre os registos criminais relativos a essa pessoa enquanto nacional de um país terceiro.

5. Quando consultam o ECRIS-TCN, as autoridades competentes podem utilizar todos ou apenas alguns dos dados a que se refere o artigo 5.º, n.º 1. O conjunto mínimo de dados que é exigido para consultar o sistema é especificado num ato de execução adotado nos termos do artigo 10.º, n.º 1, alínea g).

6. As autoridades competentes também podem consultar o ECRIS-TCN utilizando imagens faciais, desde que esta funcionalidade tenha sido implementada em conformidade com o artigo 6.º, n.º 2.

7. Em caso de resposta positiva, o sistema central transmite automaticamente à autoridade competente informações sobre os Estados-Membros que possuem informações sobre o registo criminal do nacional de país terceiro, juntamente com o número ou números de referência associados e qualquer dado de identificação correspondente. Estas informações sobre a identificação são utilizadas exclusivamente para efeitos de verificação da identidade do nacional de país terceiro em causa. O resultado de consultas ao sistema central só pode ser utilizado para efeitos de apresentação de pedidos nos termos do artigo 6.º da Decisão-Quadro 2009/315/JAI ou de pedidos referidos no artigo 17.º, n.º 3, do presente regulamento.

8. Em caso de resposta negativa, o sistema central informa automaticamente deste facto a autoridade competente.

CAPÍTULO III

Conservação e alteração dos dados

Artigo 8.º

Período de conservação dos dados armazenados

1. Cada ficheiro é armazenado no sistema central enquanto os dados relativos às condenações da pessoa em causa constarem do registo criminal.

2. Após o termo do período de conservação referido no n.º 1, a autoridade central do Estado-Membro de condenação apaga o ficheiro do sistema central, incluindo quaisquer dados dactiloscópicos ou imagens faciais. O apagamento é feito automaticamente, quando tal for possível, e em qualquer caso o mais tardar um mês após o fim do período de conservação.

Artigo 9.º

Alteração e apagamento de dados

1. Os Estados-Membros podem alterar ou apagar os dados que tenham introduzido no sistema ECRIS-TCN.

2. Qualquer alteração das informações constantes dos registos criminais que tenha levado à criação de um ficheiro em conformidade com o artigo 5.º deve incluir uma alteração idêntica, efetuada sem demora injustificada, pelo Estado-Membro de condenação, das informações conservadas no ficheiro em causa no sistema central.

3. Se um Estado-Membro de condenação tiver razões para crer que os dados que registou no sistema central estão incorretos ou que o seu tratamento no sistema central é contrário ao presente regulamento:

a) Aciona imediatamente o procedimento de verificação da exatidão dos dados em causa ou a legalidade do seu tratamento, conforme adequado;

b) Se necessário, procede sem demora injustificada à sua retificação ou apagamento do sistema central.

4. Se um Estado-Membro diferente do Estado-Membro de condenação que introduziu os dados tiver motivos para crer que os dados registados no sistema central estão incorretos ou que o seu tratamento no sistema central é contrário ao presente regulamento, contacta sem demora injustificada a autoridade central do Estado-Membro de condenação.

O Estado-Membro de condenação:

a) Aciona imediatamente o procedimento de verificação da exatidão dos dados em causa ou da legalidade do seu tratamento, conforme adequado;

b) Se necessário, retifica os dados ou apaga-os do sistema central sem demora injustificada;

c) Informa sem demora injustificada o outro Estado-Membro de que os dados foram retificados ou apagados ou das razões pelas quais os dados não foram retificados nem apagados.

CAPÍTULO IV

Desenvolvimento, funcionamento e responsabilidades

Artigo 10.º

Adoção de atos de execução pela Comissão

1. A Comissão adota o mais rapidamente possível os atos de execução necessários ao desenvolvimento técnico e à execução técnica do ECRIS-TCN e, em especial, os atos sobre:

a) As especificações técnicas para o tratamento dos dados alfanuméricos;

b) As especificações técnicas para a qualidade, resolução e tratamento dos dados datiloscópicos;

c) As especificações técnicas do *software* de interface;

d) As especificações técnicas para a qualidade, resolução e tratamento das imagens faciais para efeitos do artigo 6.º e nas condições nele previstas;

e) A qualidade dos dados, incluindo um mecanismo e procedimentos de controlo da qualidade dos dados;

f) A introdução de dados, em conformidade com o artigo 5.º;

g) O acesso e a consulta ao ECRIS-TCN, em conformidade com o artigo 7.º;

h) A alteração e o apagamento de dados, em conformidade com os artigos 8.º e 9.º;

i) A conservação de registos e o acesso aos mesmos, em conformidade com o artigo 31.º;

j) funcionamento do repositório central e das regras de proteção e segurança dos dados aplicáveis ao repositório, em conformidade com o artigo 32.º;

k) A disponibilização de estatísticas, em conformidade com o artigo 32.º;

l) Os requisitos de funcionamento e de disponibilidade do ECRIS-TCN, incluindo as especificações e requisitos mínimos para o desempenho biométrico do ECRIS-TCN, particularmente no que se refere às taxas exigidas de identificação de falsos positivos e de identificação de falsos negativos.

2. Os atos de execução referidos no n.º 1 são adotados pelo procedimento de exame a que se refere o artigo 38.º, n.º 2.

Artigo 11.º

Desenvolvimento e gestão operacional do ECRIS-TCN

1. A eu-LISA é responsável pelo desenvolvimento do ECRIS-TCN, de acordo com o princípio da proteção de dados, desde a conceção e por defeito. Além disso, a eu-LISA é responsável pela gestão operacional do ECRIS-TCN. O desenvolvimento consiste na elaboração e implementação das especificações técnicas, na realização de testes e na coordenação global do projeto.

2. A eu-LISA é igualmente responsável pela continuação do desenvolvimento e da manutenção da aplicação de referência do ECRIS.

3. A eu-LISA define a conceção da arquitetura física do ECRIS-TCN, incluindo as suas especificações técnicas e a sua evolução em relação ao sistema central, ao ponto de acesso central nacional, e ao *software* de interface. Essa conceção é adotada pelo seu Conselho de Administração, sob condição de parecer favorável da Comissão.

4. A eu-LISA desenvolve e executa o ECRIS-TCN o mais rapidamente possível após a entrada em vigor do presente regulamento e após a adoção, pela Comissão, dos atos de execução previstos no artigo 10.º.

5. Previamente à fase de conceção e de desenvolvimento do ECRIS-TCN, o Conselho de Administração da eu-LISA cria um Comité de Gestão do Programa composto por dez membros.

O Comité de Gestão do Programa é composto por oito membros nomeados pelo Conselho de Administração, pelo presidente do Grupo Consultivo referido no artigo 39.º, e por um membro nomeado pela Comissão. Os membros nomeados pelo Conselho de Administração só são eleitos de entre os Estados-Membros que estejam plenamente vinculados, nos termos do direito da União, pelos instrumentos legislativos que regem o sistema ECRIS e que participem no ECRIS-TCN. O Conselho de Administração assegura que os membros que designa para o Comité de Gestão do Programa disponham da experiência e dos conhecimentos necessários em matéria de desenvolvimento e de gestão de sistemas informáticos utilizados pelas autoridades judiciárias e as autoridades que gerem os registos criminais.

A eu-LISA participa nos trabalhos do Comité de Gestão do Programa. Para o efeito, os representantes da eu-LISA participam nas reuniões do Comité de Gestão do Programa, a fim de apresentar relatórios sobre os trabalhos relativos à conceção e ao desenvolvimento do ECRIS-TCN e sobre quaisquer outros trabalhos e atividades conexas.

O Comité de Gestão do Programa reúne-se pelo menos uma vez de três em três meses, ou com maior frequência, se necessário. O Comité de Gestão do Programa garante a gestão adequada da fase de conceção e desenvolvimento do ECRIS-TCN e assegura a coerência entre o projeto ECRIS-TCN central e os projetos ECRIS nacionais e com o *software* nacional de aplicação. O Comité de Gestão do Programa apresenta regularmente e, se possível mensalmente, por escrito, ao Conselho de Administração da eu-LISA relatórios sobre os progressos do projeto. O Comité de Gestão do Programa não tem poder de decisão nem de mandato para representar os membros do Conselho de Administração.

6. O Comité de Gestão do Programa estabelece o seu regulamento interno, que inclui, em particular, regras sobre:

a) O exercício da presidência;

b) Os locais de reunião;

c) A preparação das reuniões;

d) A admissão de peritos nas reuniões;

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

7. A presidência do Comité de Gestão do Programa é exercida por um Estado-Membro que esteja plenamente vinculado, nos termos do direito da União, pelos instrumentos legislativos que regem o ECRIS e pelos que regem o desenvolvimento, a criação, o funcionamento e a utilização de todos os sistemas informáticos de grande escala geridos pela eu-LISA.

8. Todas as despesas de viagem e de estadia incorridas pelos membros do Comité de Gestão do Programa são suportadas pela eu-LISA, aplicando-se o artigo 10.º do regulamento interno da eu-LISA *mutatis mutandis*. O secretariado do Comité de Gestão do Programa é assegurado pela eu-LISA.

9. Durante a fase de conceção e de desenvolvimento, o Grupo Consultivo referido no artigo 39.º é composto por gestores de projeto nacionais do ECRIS-TCN e presidido pela eu-LISA. Durante a fase de conceção e de desenvolvimento, o grupo reúne-se regularmente, se possível pelo menos uma vez por mês, até à entrada em funcionamento do ECRIS--TCN. O grupo apresenta um relatório após cada reunião do Comité de Gestão do Programa. O grupo fornece ainda os conhecimentos técnicos necessários para apoiar as atividades do Comité de Gestão do Programa e assegura o acompanhamento do nível de preparação dos Estados-Membros.

10. A fim de assegurar a confidencialidade e a integridade dos dados armazenados no ECRIS-TCN a todo o tempo, a eu-LISA prevê, em cooperação com os Estados-Membros, as medidas técnicas e organizativas adequadas, tendo em conta o estado da arte, os custos de execução e os riscos colocados pelo tratamento.

11. A eu-LISA é igualmente responsável pelas funções seguintes relacionadas com a infraestrutura de comunicação a que se refere o artigo 4.º, n.º 1, alínea d):

a) Supervisão;

b) Segurança;

c) Coordenação das relações entre os Estados-Membros e o fornecedor da infraestrutura de comunicação.

12. A Comissão é responsável por todas as outras funções relacionadas com a infraestrutura de comunicação a que se refere o artigo 4.º, n.º 1, alínea d), em especial:

a) As relativas à execução do orçamento;

b) Aquisição e renovação;

c) Questões contratuais.

13. A eu-LISA desenvolve e mantém um mecanismo e procedimentos de controlo da qualidade dos dados no ECRIS--TCN, apresentando relatórios periódicos aos Estados-Membros. A eu-LISA apresenta periodicamente à Comissão relatórios sobre os problemas encontrados e os Estados-Membros afetados.

14. A gestão operacional do ECRIS-TCN engloba todas as tarefas necessárias para assegurar o seu funcionamento, em conformidade com o presente regulamento, em especial o trabalho de manutenção e as adaptações técnicas necessárias para garantir o funcionamento do ECRIS-TCN com um nível satisfatório de acordo com as especificações técnicas.

15. A eu-LISA realiza tarefas relacionadas com a prestação de formação sobre a utilização técnica do ECRIS-TCN e da aplicação de referência do ECRIS.

16. Sem prejuízo do disposto no artigo 17.º do Estatuto dos Funcionários da União Europeia, estabelecido no Regulamento (CEE, Euratom, CECA) n.º 259/68 do Conselho ([17]), a eu-LISA aplica as normas de sigilo profissional adequadas, ou outros deveres de confidencialidade equivalentes, a todos os elementos do seu pessoal que tenham de trabalhar com os dados registados no sistema central. Tal dever continua a aplicar-se depois de esses elementos do pessoal cessarem funções ou após a cessação da sua relação contratual ou atividade.

Artigo 12.º

Responsabilidades dos Estados-Membros

1. Cada Estado-Membro é responsável:

a) Por assegurar uma ligação segura entre as suas bases nacionais de dados dos registos criminais e de dados dactiloscópicos e o respetivo ponto de acesso central nacional;

b) Pelo desenvolvimento, funcionamento e manutenção da ligação a que se refere a alínea a);

c) Por assegurar a ligação entre os respetivos sistemas nacionais e a aplicação de referência do ECRIS;

([17]) JO L 56 de 4.3.1968, p. 1.

d) Pela gestão e pelas modalidades de acesso ao ECRIS-TCN pelo pessoal devidamente autorizado das autoridades centrais, em conformidade com o presente regulamento, bem como pela criação e atualização regular de uma lista desse pessoal e os perfis referidos no artigo 19.º, n.º 3, alínea g).

2. Cada Estado-Membro presta ao pessoal das suas autoridades centrais que tenham direito de acesso ao ECRIS-TCN a formação adequada, em especial sobre segurança de dados, normas de proteção de dados e direitos fundamentais aplicáveis, antes de autorizar que procedam ao tratamento dos dados armazenados no sistema central.

Artigo 13.º

Responsabilidade pela utilização dos dados

1. Em conformidade com a legislação da União aplicável em matéria de proteção de dados, cada Estado-Membro assegura que os dados registados no ECRIS-TCN sejam tratados de forma lícita e, em especial, que:

a) Apenas o pessoal devidamente autorizado tenha acesso aos dados para efeitos de desempenho das suas funções;

b) Os dados sejam recolhidos de forma lícita no pleno respeito pela dignidade e dos direitos fundamentais do nacional de país terceiro;

c) Os dados sejam introduzidos de forma lícita no ECRIS-TCN;

d) Os dados sejam exatos e atualizados aquando da sua introdução no ECRIS-TCN.

2. A eu-LISA assegura que o ECRIS-TCN seja gerido em conformidade com o presente regulamento, com o ato delegado a que se refere o artigo 6.º, n.º 2, e com os atos de execução a que se refere o artigo 10.º, bem como em conformidade com o Regulamento (UE) 2018/1725. A eu-LISA toma, em especial, as medidas necessárias para garantir a segurança do sistema central e da infraestrutura de comunicação a que se refere o artigo 4.º, n. 1, alínea d), sem prejuízo das responsabilidades de cada Estado-Membro.

3. A eu-LISA informa o Parlamento Europeu, o Conselho e a Comissão, bem como a Autoridade Europeia para a Proteção de Dados, o mais rapidamente possível, das medidas que adotar em aplicação do n.º 2 com vista à entrada em funcionamento do ECRIS-TCN.

4. A Comissão coloca as informações referidas no n.º 3 à disposição dos Estados-Membros e do público, através de um sítio Web regularmente atualizado.

Artigo 14.º

Acesso da Eurojust, da Europol e da EPPO

1. A Eurojust tem acesso direto ao ECRIS-TCN para efeitos da aplicação do artigo 17.º, bem como do exercício das suas atribuições, nos termos do artigo 2.º do Regulamento (UE) 2018/1727 do Parlamento Europeu e do Conselho, com vista a determinar os Estados-Membros que possuem informações sobre condenações anteriores de nacionais de países terceiros.

2. A Europol tem acesso direto ao ECRIS-TCN para efeitos do exercício das suas atribuições legais, nos termos do artigo 4.º, n.º 1, alíneas a) a e) e h), do Regulamento (UE) 2016/794, com vista a determinar os Estados-Membros que possuem informações sobre condenações anteriores de nacionais de países terceiros.

3. A EPPO tem acesso direto ao ECRIS-TCN para efeitos do exercício das suas atribuições, nos termos do artigo 4.º do Regulamento (UE) 2017/1939, com vista a determinar os Estados-Membros que possuem informações sobre condenações anteriores de nacionais de países terceiros.

4. Na sequência de uma resposta positiva que indique os Estados-Membros que possuem informações sobre o registo criminal de um nacional de país terceiro, a Eurojust, a Europol e a EPPO podem contactar as autoridades nacionais desses Estados-Membros para solicitar as informações do registo criminal do modo previsto nos seus respetivos atos de instituição.

Artigo 15.º

Acesso do pessoal autorizado da Eurojust, da Europol e da EPPO

A Eurojust, a Europol e a EPPO são responsáveis pela gestão e pelas modalidades de acesso ao ECRIS-TCN pelo pessoal devidamente autorizado, em conformidade com o presente regulamento, e ela criação e atualização regular de uma lista do referido pessoal e dos respetivos perfis.

Artigo 16.º

Responsabilidades da Eurojust, da Europol e da EPPO

A Eurojust, a Europol e a EPPO devem:

a) Estabelecer os meios técnicos que permitam a ligação ao ECRIS-TCN, sendo responsáveis pela manutenção da ligação;

b) Prestar formação adequada abrangendo, em particular, a segurança de dados, as regras de proteção de dados e os direitos fundamentais aplicáveis aos elementos do seu pessoal com direito de acesso ao ECRIS-TCN antes de autorizar que procedam ao tratamento dos dados armazenados no sistema central;

c) Assegurar que os dados pessoais tratados pelo referido pessoal ao abrigo do presente regulamento sejam protegidos em conformidade com as regras aplicáveis em matéria de proteção de dados.

Artigo 17.º

Ponto de contacto para os países terceiros e as organizações internacionais

1. Os países terceiros e as organizações internacionais podem, para efeitos de processo penal, dirigir à Eurojust os pedidos de informações relativas aos Estados-Membros, se algum houver, que possuam informações sobre registos criminais de nacionais de países terceiros. Para o efeito, devem utilizar o formulário normalizado constante do anexo ao presente regulamento.

2. Sempre que receba um pedido nos termos do n.º 1, a Eurojust utiliza o ECRIS-TCN para identificar os Estados-Membros, se algum houver, que possuam informações sobre o nacional de país terceiro em causa.

3. Se a resposta for positiva, a Eurojust deve indagar junto dos Estados-Membros que possuem informações sobre os registos criminais do nacional de país terceiro em causa se consentem que a Eurojust informe o país terceiro ou a organização internacional de qual o Estado-Membro em causa. Se esse Estado-Membro der o seu consentimento, a Eurojust informa o país terceiro ou a organização internacional de qual é esse Estado-Membro, e informa o país terceiro ou a organização internacional da forma como pode solicitar extratos do registo criminal junto desse Estado-Membro em conformidade com os procedimentos aplicáveis.

4. Nos casos em que a resposta seja negativa, ou sempre que a Eurojust não possa fornecer uma resposta em conformidade com o n.º 3 aos pedidos apresentados nos termos do presente artigo, informa o país terceiro ou a organização internacional em causa de que concluiu o procedimento, sem de modo nenhum indicar se algum dos Estados-Membros possui ou não informações sobre o registo criminal da pessoa em causa.

Artigo 18.º

Prestação de informações a países terceiros, organizações internacionais ou entidades privadas

Nem a Eurojust, nem a Europol, nem a EPPO, nem qualquer autoridade central podem transferir ou disponibilizar a um país terceiro, organização internacional ou entidade privada, as informações obtidas a partir do ECRIS-TCN sobre um nacional de país terceiro. O presente artigo não prejudica o disposto no artigo 17.º, n.º 3.

Artigo 19.º

Segurança dos dados

1. A eu-LISA toma as medidas necessárias para garantir a segurança do ECRIS-TCN, sem prejuízo das responsabilidades que incumbem a cada Estado-Membro, tendo em conta as medidas de segurança especificadas no n.º 3.

2. No que diz respeito ao funcionamento do ECRIS-TCN, a eu-LISA adota as medidas necessárias para alcançar os objetivos mencionados no n.º 3, incluindo a adoção de um plano de segurança e de um plano de retoma de atividades e de recuperação na sequência de catástrofes, e para assegurar que os sistemas instalados possam ser reestabelecidos em caso de interrupção.

3. Os Estados-Membros garantem a segurança dos dados antes e durante a sua transmissão ao ponto de acesso central nacional. Em especial, cada Estado-Membro deve:

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

b) Impedir o acesso de pessoas não autorizadas às instalações nacionais em que são realizadas as operações que incumbem ao Estado-Membro para fins do ECRIS-TCN;

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

d) Impedir a introdução não autorizada de dados, bem como qualquer inspeção, alteração ou apagamento não autorizados de dados pessoais armazenados;

e) Impedir o tratamento não autorizado de dados contidos no ECRIS-TCN e qualquer alteração ou apagamento não autorizados dos dados tratados no ECRIS-TCN;

f) Assegurar que as pessoas autorizadas a aceder ao ECRIS-TCN tenham acesso aos dados abrangidos pela respetiva autorização de acesso unicamente através de nomes de utilizador individuais e de modos de acesso confidenciais;

g) Assegurar que todas as autoridades com direito de acesso ao ECRIS-TCN criem perfis que descrevam as funções e responsabilidades das pessoas autorizadas a aceder, retificar, apagar, consultar e pesquisar dados, e que disponibilizem sem demora injustificada esses perfis às autoridades nacionais de controlo, a pedido destas;

h) Assegurar a possibilidade de verificar e determinar as entidades, serviços e agências da União às quais podem ser transmitidos os dados pessoais através de equipamentos de comunicação de dados;

i) Assegurar a possibilidade de verificar e determinar que tipos de dados foram tratados no ECRIS-TCN, em que momento, por quem e com que finalidade;

j) Impedir a leitura, a cópia, a alteração ou o apagamento não autorizados de dados pessoais durante a sua transmissão de e para o ECRIS-TCN, ou durante o transporte dos suportes de dados, em especial através de técnicas de cifragem adequadas;

k) Fiscalizar a eficácia das medidas de segurança referidas no presente número e adota as medidas organizativas necessárias relacionadas com o autocontrolo e a supervisão, de forma a assegurar a conformidade com o presente regulamento.

4. A eu-LISA e os Estados-Membros cooperam para garantir uma abordagem coerente da segurança dos dados, com base num processo de gestão dos riscos de segurança que englobe todo o ECRIS-TCN.

Artigo 20.º

Responsabilidade

1. Qualquer pessoa ou Estado-Membro que tenha sofrido um dano patrimonial ou não-patrimonial em razão de um tratamento ilícito ou de qualquer outro ato incompatível com o presente regulamento tem direito a ser indemnizado:

a) Pelo Estado-Membro responsável por esse dano; ou

b) Pela eu-LISA, quando esta não tiver cumprido as obrigações estabelecidas no presente regulamento ou no Regulamento (UE) 2018/1725.

O Estado-Membro responsável pelo dano sofrido ou a eu-LISA, respetivamente, são total ou parcialmente exonerados dessa responsabilidade se provarem que o facto que deu origem ao dano não lhes é imputável.

2. Se o incumprimento, por parte de um Estado-Membro, da Eurojust, da Europol ou da EPPO, das obrigações que lhes incumbem por força do presente regulamento causar danos ao ECRIS-TCN, esse Estado-Membro, a Eurojust, a Europol ou a EPPO, respetivamente, são considerados responsáveis pelos danos na medida em que a eu-LISA ou outro Estado-Membro participante no ECRIS-TCN não tenha tomado medidas razoáveis para prevenir os danos ou minimizar o seu impacto.

3. Os pedidos de indemnização a um Estado-Membro pelos danos referidos nos n.os 1 e 2 são regulados pelo direito do Estado-Membro requerido. Os pedidos de indemnização à eu-LISA, à Eurojust, à Europol ou à EPPO pelos danos referidos nos n.os 1 e 2 são regulados pelos respetivos atos de instituição.

Artigo 21.º

Autocontrolo

Os Estados-Membros asseguram que cada autoridade central tome as medidas necessárias para dar cumprimento ao disposto no presente regulamento e coopere, se necessário, com as autoridades de controlo.

Artigo 22.º

Sanções

Em conformidade com o direito nacional ou da União, qualquer utilização abusiva dos dados introduzidos no ECRIS-TCN é passível de sanções ou de medidas disciplinares efetivas, proporcionadas e dissuasivas.

CAPÍTULO V

Direitos e fiscalização em matéria de proteção de dados

Artigo 23.º

Responsável pelo tratamento de dados e subcontratante

1. Cada autoridade central é considerada responsável, em conformidade com as regras da União aplicáveis em matéria de proteção de dados, pelo tratamento de dados pessoais pelo Estado-Membro dessa autoridade central ao abrigo do presente regulamento.

2. A eu-LISA é considerada subcontratante, em conformidade com o Regulamento (UE) 2018/1725, no que diz respeito aos dados pessoais introduzidos no sistema central pelos Estados-Membros.

Artigo 24.º

Finalidade do tratamento de dados pessoais

1. Os dados introduzidos no sistema central só podem ser tratados para efeitos da determinação dos Estados-Membros que possuem informações sobre os registos criminais de nacionais de países terceiros.

2. Com exceção do pessoal devidamente autorizado da Eurojust, da Europol e da EPPO que tem acesso ao ECRIS-TCN para efeitos do presente regulamento, o acesso ao ECRIS-TCN está exclusivamente reservado ao pessoal devidamente autorizado das autoridades centrais. O acesso é limitado na medida necessária à execução de funções conformes com a finalidade a que se refere o n.º 1, e ao que é necessário e proporcional aos objetivos pretendidos.

Artigo 25.º

Direito de acesso, retificação, apagamento e limitação do tratamento

1. Os pedidos de nacionais de países terceiros relativos aos direitos de acesso a dados pessoais, à retificação, ao apagamento e à limitação do tratamento de dados pessoais, que estão previstos nas regras da União aplicáveis em matéria de proteção de dados, podem ser dirigidos à autoridade central de qualquer Estado-Membro.

2. Se for apresentado um pedido a um Estado-Membro diferente do Estado-Membro de condenação, o Estado-Membro ao qual tiver sido apresentado o pedido reencaminha-o para o Estado-Membro de condenação sem demora injustificada, e, em qualquer caso, no prazo de dez dias a contar da receção do pedido. Ao receber o pedido, o Estado-Membro de condenação deve:

a) Iniciar imediatamente um procedimento de verificação da exatidão dos dados em causa ou da licitude do seu tratamento no ECRIS-TCN; e

b) Responder sem demora injustificada ao Estado-Membro que tiver reencaminhado o pedido.

3. Se os dados registados no ECRIS-TCN forem inexatos ou tiverem sido tratados de forma ilícita, o Estado-Membro de condenação procede à sua retificação ou apagamento, em conformidade com o artigo 9.º. O Estado-Membro de condenação ou, se aplicável, o Estado-Membro ao qual tiver sido apresentado o pedido, confirma por escrito e sem demora injustificada à pessoa em causa que tomou as medidas necessárias para proceder à retificação ou ao apagamento de tais dados. O Estado-Membro de condenação comunica também sem demora injustificada a qualquer outro Estado-Membro que tenha sido destinatário das informações sobre condenações obtidas na sequência de uma consulta ao ECRIS-TCN quais as medidas que foram tomadas.

4. Se o Estado-Membro de condenação não considerar que os dados registados no sistema ECRIS-TCN são inexatos ou foram tratados de forma ilícita, adota uma decisão administrativa ou judicial, explicando por escrito à pessoa em causa as razões pelas quais não está disposto a retificar ou a apagar tais dados. Se for adequado, tais casos podem ser comunicados à autoridade nacional de supervisão.

5. O Estado-Membro que tiver adotado a decisão nos termos do n.º 4 faculta igualmente à pessoa em causa informações sobre as medidas que esta pode tomar caso não considere aceitável a explicação dada nos termos do n.º 4. Tais informações incluem a forma de intentar uma ação ou apresentar uma reclamação às autoridades competentes ou aos tribunais desse Estado-Membro, bem como a eventual assistência de que pode beneficiar por parte das autoridades nacionais de controlo, em conformidade com o direito nacional desse Estado-Membro.

6. Qualquer pedido apresentado nos termos do n.º 1 deve incluir as informações necessárias para identificar a pessoa em causa. Essas informações são utilizadas exclusivamente para efeitos do exercício dos direitos referidos no n.º 1, após o que serão imediatamente apagadas.

7. Se o n.º 2 for aplicável, a autoridade central a quem o pedido foi dirigido conserva um registo escrito de que esse pedido foi feito, acerca da forma como ele foi tratado e com indicação da autoridade para a qual foi reencaminhado. A pedido da autoridade nacional de controlo, a autoridade central disponibiliza esse registo sem demora a essa autoridade nacional de controlo. A autoridade central e a autoridade nacional de controlo suprimem tais registos após três anos a contar da sua criação.

Artigo 26.º

Cooperação com vista a garantir os direitos em matéria de proteção de dados

1. As autoridades centrais cooperam entre si, a fim de assegurar o respeito pelos direitos estabelecidos no artigo 25.º.

2. Em cada Estado-Membro, a autoridade nacional de controlo presta, a pedido do interessado, informações sobre o modo de exercer o seu direito a obter a retificação ou o apagamento dos dados que lhe digam respeito, em conformidade com as regras da União aplicáveis em matéria de proteção de dados.

3. Para efeitos do presente artigo, a autoridade nacional de controlo do Estado-Membro que transmitiu os dados e a autoridade nacional de controlo dos Estados-Membros à qual o pedido foi apresentado cooperam entre si.

Artigo 27.º

Vias de recurso

Qualquer pessoa tem o direito de apresentar queixa e o direito de recurso no Estado-Membro de condenação que lhe tiver recusado o direito de acesso, de retificação ou de apagamento dos dados que lhe digam respeito, referido no artigo 25.º, em conformidade com o direito nacional ou da União.

Artigo 28.º

Supervisão pelas autoridades nacionais de controlo

1. Cada Estado-Membro assegura que as autoridades nacionais de controlo, designadas nos termos das regras da União aplicáveis em matéria de proteção de dados, supervisionam a licitude do tratamento dos dados pessoais a que se referem os artigos 5.º e 6.º, pelo Estado-Membro em causa, incluindo a sua transmissão ao ECRIS-TCN e a partir do mesmo.

2. A autoridade nacional de controlo assegura que seja efetuada, no mínimo de três em três anos, uma auditoria das operações de tratamento de dados nos registos criminais e nas bases de dados dactiloscópicos nacionais relacionadas com o intercâmbio de dados entre esses sistemas e o ECRIS-TCN, em conformidade com as normas internacionais de auditoria aplicáveis a contar da entrada em funcionamento do ECRIS-TCN.

3. Os Estados-Membros asseguram que as autoridades nacionais de controlo dispõem dos meios necessários para desempenhar as funções que lhe são confiadas nos termos do presente regulamento.

4. Cada Estado-Membro presta todas as informações solicitadas pelas suas autoridades nacionais de controlo e, em especial, informa-as das atividades desenvolvidas em conformidade com os artigos 12.º, 13.º e 19.º. Cada Estado-Membro faculta às suas autoridades nacionais de controlo o acesso aos respetivos registos mencionados no artigo 25.º, n.º 7, e no artigo 31.º, n.º 6, bem como o acesso, a qualquer momento, a todas as suas instalações relacionadas com o ECRIS-TCN.

Artigo 29.º

Supervisão pela Autoridade Europeia para a Proteção de Dados

1. A Autoridade Europeia para a Proteção de Dados deve velar por que as atividades de tratamento de dados pessoais efetuadas pela eu-LISA no âmbito do ECRIS-TCN sejam realizadas em conformidade com o presente regulamento.

2. A Autoridade Europeia para a Proteção de Dados deve assegurar que, no mínimo de três em três anos, é efetuada uma auditoria das atividades de tratamento de dados pessoais realizadas pela eu-LISA, em conformidade com as normas internacionais de auditoria aplicáveis. O relatório dessa auditoria é enviado ao Parlamento Europeu, ao Conselho, à Comissão, à eu-LISA e às autoridades de supervisão. A eu-LISA tem a possibilidade de apresentar observações antes da aprovação do relatório.

3. A eu-LISA deve fornecer as informações solicitadas pela Autoridade Europeia para a Proteção de Dados, conceder-lhe o acesso a todos os documentos e aos registos referidos no artigo 31.º e permitir-lhe o acesso, a qualquer momento, a todas as suas instalações.

Artigo 30.º

Cooperação entre as autoridades nacionais de controlo e a Autoridade Europeia para a Proteção de Dados

A supervisão coordenada do ECRIS-TCN é assegurada em conformidade com o artigo 62.º do Regulamento (UE) 2018/1725.

Artigo 31.º

Conservação de registos

1. A eu-LISA e as autoridades competentes asseguram, em conformidade com as respetivas responsabilidades, que todas as operações de tratamento de dados no ECRIS-TCN sejam registadas nos termos do n.º 2 para fins de verificação da admissibilidade do pedido, de controlo da integridade e da segurança, e da licitude do tratamento dos dados, bem como para fins de autocontrolo.

2. O registo deve indicar:

a) A finalidade do pedido de acesso aos dados do ECRIS-TCN;

b) Os dados transmitidos, como referido no artigo 5.º;

c) A referência do ficheiro nacional;

d) A data e a hora exata da operação;

e) Os dados utilizados para a consulta;

f) Os dados de identificação do funcionário que efetuou a consulta.

3. O registo das consultas e dos resultados deve permitir determinar o motivo de tais operações.

4. Os registos só podem ser utilizados para controlar a licitude do tratamento de dados e assegurar a integridade e a segurança destes últimos. Só os registos que contenham dados de caráter não pessoal podem ser utilizados para o controlo e avaliação previstos no artigo 36.º. Os referidos registos são protegidos por medidas adequadas contra o acesso não autorizado e apagados no termo de um período de três anos, se já não forem necessários para procedimentos de controlo entretanto iniciados.

5. A eu-LISA disponibiliza sem demora injustificada às autoridades centrais, a pedido destas, os registos das suas operações de tratamento.

6. As autoridades nacionais de controlo responsáveis pela verificação da admissibilidade do pedido e pelo controlo da licitude do tratamento dos dados e da integridade e segurança dos mesmos, têm acesso aos registos, a seu pedido, para efeitos do exercício das suas funções. As autoridades centrais disponibilizam sem demora injustificada às autoridades nacionais de controlo competentes, a pedido destas, os registos das suas operações de tratamento.

CAPÍTULO VI

Disposições finais

Artigo 32.º

Utilização de dados para a elaboração de relatórios e estatísticas

1. O pessoal devidamente autorizado da eu-LISA, das autoridades competentes e da Comissão apenas têm acesso aos dados tratados no âmbito do ECRIS-TCN para fins de elaboração de relatórios e estatísticas, sem permitir uma identificação individual.

2. Para efeitos do n.º 1, a eu-LISA cria, implementa e acolhe um repositório central nas suas instalações técnicas que contenha os dados a que se refere o n.º 1, que, sem permitir uma identificação individual, permita elaborar relatórios e estatísticas adaptáveis. O acesso ao repositório central é concedido por meio de um controlo de acesso seguro e de perfis de utilizador específicos utilizados exclusivamente para fins de elaboração de relatórios e estatísticas.

3. Os procedimentos instaurados pela eu-LISA para acompanhar o funcionamento do ECRIS-TCN, referidos no artigo 36.º, bem como a aplicação de referência do ECRIS, devem incluir a possibilidade de elaborar regularmente estatísticas para fins de acompanhamento.

A eu-LISA apresenta à Comissão estatísticas mensais sobre o registo, armazenamento e intercâmbio de informações extraídas dos registos criminais através do ECRIS-TCN e da aplicação de referência do ECRIS. A eu-LISA deve garantir que não é possível a identificação de indivíduos com base nessas estatísticas. A pedido da Comissão, a eu-LISA deve facultar-lhe estatísticas sobre certos aspetos específicos relacionados com a aplicação do presente regulamento.

4. Os Estados-Membros devem facultar à eu-LISA as estatísticas necessárias ao cumprimento das suas obrigações nos termos do presente artigo. Devem facultar à Comissão estatísticas sobre o número de nacionais de países terceiros objeto de condenação e o número de condenações de nacionais de países terceiros no seu território.

Artigo 33.º

Custos

1. Os custos decorrentes da criação e do funcionamento do sistema central, da infraestrutura de comunicação referida no artigo 4.º, n.º 1, alínea d), do *software* de interface e da aplicação de referência do ECRIS são suportados pelo orçamento geral da União.

2. Os custos de ligação da Eurojust, da Europol e da EPPO ao ECRIS-TCN ficam a cargo dos respetivos orçamentos.

3. Outros custos ficam a cargo dos Estados-Membros, em especial os custos decorrentes da ligação dos registos criminais nacionais existentes, das bases de dados dactiloscópicos e das autoridades centrais ao ECRIS-TCN, bem como os custos decorrentes do acolhimento da aplicação de referência do ECRIS.

Artigo 34.º

Notificações

1. Cada Estado-Membro notifica a eu-LISA quanto à respetiva autoridade central ou autoridades centrais que têm acesso para introduzir, retificar, apagar, consultar ou pesquisar dados, bem como qualquer alteração a este respeito.

2. A eu-LISA assegura a publicação da lista das autoridades centrais notificadas pelos Estados-Membros, tanto no *Jornal Oficial da União Europeia* como no seu sítio Web. Quando seja notificada da mudança de uma autoridade central de um Estado-Membro, a eu-LISA atualiza essa lista sem demora injustificada.

Artigo 35.º

Introdução de dados e entrada em funcionamento

1. A Comissão determina a data a partir da qual os Estados-Membros introduzem os dados referidos no artigo 5.º no ECRIS-TCN assim que considerar que estão reunidas as seguintes condições:

a) Tiverem sido adotados os atos de execução pertinentes previstos no artigo 10.º;

b) Os Estados-Membros tiverem validado as disposições técnicas e jurídicas necessárias para recolher e transmitir os dados referidos no artigo 5.º ao ECRIS-TCN e procedido à sua comunicação à Comissão;

c) A eu-LISA tiver realizado um teste global do ECRIS-TCN, em cooperação com os Estados-Membros, utilizando dados de teste anónimos.

2. Quando a Comissão tiver fixado a data de início da introdução de dados nos termos do n.º 1, informa disso os Estados-Membros. Num prazo de dois meses a contar da referida data, os Estados-Membros introduzem no ECRIS-TCN os dados referidos no artigo 5.º, tendo em conta o artigo 41.º, n.º 2.

3. Após o fim do prazo referido no n.º 2, a eu-LISA realiza um teste final do ECRIS-TCN, em cooperação com os Estados-Membros.

4. Quando o teste referido no n.º 3 tiver sido concluído com resultados positivos e a eu-LISA considerar que o ECRIS-TCN está pronto para entrar em funcionamento, notifica a Comissão. A Comissão informa o Parlamento Europeu e o Conselho dos resultados do teste e decide em que data o ECRIS-TCN entra em funcionamento.

5. A decisão da Comissão sobre a data de entrada em funcionamento do ECRIS-TCN referida no n.º 4 é publicada no *Jornal Oficial da União Europeia*.

6. Os Estados-Membros começam a utilizar o ECRIS-TCN a partir da data determinada pela Comissão em conformidade com o n.º 4.

7. Ao tomar as decisões referidas no presente artigo, a Comissão pode especificar diferentes datas para a introdução dos dados alfanuméricos e dos dados dactiloscópicos a que se refere o artigo 5.º no ECRIS-TCN e para a entrada em funcionamento no que diz respeito a essas diferentes categorias de dados.

Artigo 36.º

Acompanhamento e avaliação

1. A eu-LISA assegura a criação de procedimentos para acompanhar o desenvolvimento do ECRIS-TCN, tendo em conta os objetivos fixados em termos de planeamento e de custos, e para acompanhar o funcionamento do ECRIS-TCN e da aplicação de referência do ECRIS tendo em conta os objetivos fixados em termos de resultados técnicos, custo-eficácia, segurança e qualidade do serviço.

2. Para efeitos do acompanhamento do funcionamento do ECRIS-TCN e da sua manutenção técnica, a eu-LISA tem acesso às informações necessárias respeitantes às operações de tratamento de dados efetuadas no ECRIS-TCN e na aplicação de referência do ECRIS.

3. Até 12 de dezembro de 2019 e, posteriormente, de seis em seis meses durante a fase de conceção e desenvolvimento, a eu-LISA apresenta ao Parlamento Europeu e ao Conselho um relatório sobre o desenvolvimento do ECRIS-TCN e da aplicação de referência do ECRIS.

4. O relatório a que se refere o n.º 3 deve incluir uma panorâmica geral das despesas correntes e da evolução do projeto, uma avaliação do impacto financeiro e informações sobre eventuais problemas técnicos e riscos suscetíveis de afetar os custos globais do ECRIS-TCN a suportar pelo orçamento geral da União nos termos do artigo 33.º.

5. Em caso de atrasos substanciais no processo de desenvolvimento, eu-LISA informa o Parlamento Europeu e o Conselho, o mais rapidamente possível, das causas desses atrasos e do seu impacto no calendário e a nível financeiro.

6. Uma vez concluída a fase de desenvolvimento do ECRIS-TCN e da aplicação de referência do ECRIS, a eu-LISA apresenta ao Parlamento Europeu e ao Conselho um relatório que explica a forma como os objetivos, em especial de planeamento e de custos, foram alcançados, justificando igualmente as eventuais divergências.

7. Caso se proceda a uma atualização técnica do ECRIS-TCN suscetível de gerar custos substanciais, a eu-LISA informa o Parlamento Europeu e o Conselho.

8. Dois anos após a entrada em funcionamento do ECRIS-TCN e, posteriormente, todos os anos, a eu-LISA apresenta à Comissão um relatório sobre o funcionamento técnico do ECRIS-TCN e da aplicação de referência do ECRIS, incluindo a respetiva segurança, baseado nomeadamente nas estatísticas sobre o funcionamento e a utilização do ECRIS-TCN, bem como sobre o intercâmbio, através da aplicação de referência do ECRIS, de informações extraídas dos registos criminais.

9. Quatro anos após a entrada em funcionamento do ECRIS-TCN e, posteriormente, de quatro em quatro anos, a Comissão realiza uma avaliação global do ECRIS-TCN e da aplicação de referência do ECRIS. O relatório da avaliação global elaborado nesta base deve incluir uma avaliação da aplicação do presente regulamento e uma análise dos resultados obtidos relativamente aos objetivos fixados e do impacto sobre os direitos fundamentais. O relatório deve incluir também uma avaliação relativa à valia dos princípios subjacentes ao funcionamento do ECRIS-TCN, à adequação do uso de dados biométricos para os fins do ECRIS-TCN, bem como uma avaliação da segurança do ECRIS-TCN e de possíveis implicações, em termos de segurança, para o seu funcionamento futuro. A avaliação deve incluir as eventuais recomendações consideradas necessárias. A Comissão envia o relatório ao Parlamento Europeu, ao Conselho, à Autoridade Europeia para a Proteção de Dados e à Agência dos Direitos Fundamentais da União Europeia.

10. Além disso, a primeira avaliação global referida no n.º 9 deve incluir uma análise:

a) Da medida em que, com base em dados estatísticos pertinentes e outras informações dos Estados-Membros, a inclusão, no ECRIS-TCN, de informações sobre a identidade dos cidadãos da União que têm também a nacionalidade de um país terceiro contribuiu para alcançar os objetivos do presente regulamento;

b) Da possibilidade de alguns Estados-Membros continuarem a utilizar o *software* nacional de aplicação do ECRIS referido no artigo 4.º;

c) Da introdução de dados dactiloscópicos no ECRIS-TCN, em particular da aplicação dos critérios mínimos referidos no artigo 5.º, n.º 1, alínea b), subalínea ii);

d) Do impacto do ECRIS e do ECRIS-TCN sobre a proteção de dados pessoais.

A análise pode, se necessário, ser acompanhada de propostas legislativas. As avaliações globais subsequentes podem incluir a análise de um ou de todos esses aspetos.

11. Os Estados-Membros, a Eurojust, a Europol e a EPPO comunicam à eu-LISA e à Comissão as informações necessárias à elaboração dos relatórios referidos nos n.ºs 3, 8 e 9, de acordo com os indicadores quantitativos previamente definidos pela Comissão, pela eu-LISA ou por ambas. Tais informações não podem prejudicar os métodos de trabalho nem incluir dados que revelem as fontes, a identidade do pessoal ou as investigações.

12. Se for pertinente, as autoridades nacionais de controlo comunicam à eu-LISA e à Comissão as informações necessárias à elaboração dos relatórios referidos no n.º 9, de acordo com os indicadores quantitativos previamente definidos pela Comissão, pela eu-LISA ou por ambas. Tais informações não podem prejudicar os métodos de trabalho nem incluir dados que revelem as fontes, a identidade do pessoal ou as investigações.

13. A eu-LISA comunica à Comissão as informações necessárias à elaboração das avaliações globais referidas no n.º 9.

Artigo 37.º

Exercício da delegação

1. O poder de adotar atos delegados é conferido à Comissão nas condições estabelecidas no presente artigo.

2. O poder de adotar atos delegados referidos no artigo 6.º, n.º 2, é conferido à Comissão por tempo indeterminado a contar de 11 de junho de 2019.

3. A delegação de poderes referida no artigo 6.º, n.º 2, pode ser revogada em qualquer momento pelo Parlamento Europeu ou pelo Conselho. A decisão de revogação põe termo à delegação dos poderes nela especificados. A decisão de revogação produz efeitos a partir do dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia* ou de uma data posterior nela especificada. A decisão de revogação não afeta os atos delegados já em vigor.

4. Antes de adotar um ato delegado, a Comissão consulta os peritos designados por cada Estado-Membro de acordo com os princípios estabelecidos no Acordo Interinstitucional, de 13 de abril de 2016, sobre legislar melhor.

5. Assim que adotar um ato delegado, a Comissão notifica-o, simultaneamente, ao Parlamento Europeu e ao Conselho.

6. Os atos delegados adotados nos termos do artigo 6.º, n.º 2, só entram em vigor se não tiverem sido formuladas objeções pelo Parlamento Europeu ou pelo Conselho no prazo de [dois meses] a contar da notificação do ato ao Parlamento Europeu e ao Conselho, ou se, antes do termo desse prazo, o Parlamento Europeu e o Conselho tiverem informado a Comissão de que não têm objeções a formular. O referido prazo é prorrogável por [dois meses] por iniciativa do Parlamento Europeu ou do Conselho.

Artigo 38.º

Procedimento de comité

1. A Comissão é assistida por um comité. Este comité é um comité na aceção do Regulamento (UE) n.º 182/2011.

2. Caso se remeta para o presente número, aplica-se o artigo 5.º do Regulamento (UE) n.º 182/2011.

Na falta de parecer do comité, a Comissão não adota o projeto de ato de execução, aplicando-se o artigo 5.º, n.º 4, terceiro parágrafo, do Regulamento (UE) n.º 182/2011.

Artigo 39.º

Grupo Consultivo

A eu-LISA cria um grupo consultivo a fim de obter conhecimentos especializados relacionados com o ECRIS-TCN e a aplicação de referência do ECRIS, em especial no contexto da elaboração do seu programa de trabalho anual e do relatório anual de atividades. Durante a fase de conceção e de desenvolvimento, aplica-se o artigo 11.º, n.º 9.

Artigo 40.º

Alterações do Regulamento (UE) 2018/1726

O Regulamento (UE) 2018/1726 é alterado do seguinte modo:

1) No artigo 1.º, o n.º 4 passa a ter a seguinte redação:

«4. A Agência é responsável pela preparação, pelo desenvolvimento e pela gestão operacional do Sistema de Entrada/Saída (SES), da DubliNet, do Sistema Europeu de Informação e Autorização de Viagem (ETIAS), do ECRIS--TCN e da aplicação de referência do ECRIS.»;

2) É aditado o seguinte artigo:

«*Artigo 8.º-A*

Funções relacionadas com o ECRIS-TCN e a aplicação de referência do ECRIS

No que respeita ao ECRIS-TCN e à aplicação de referência do ECRIS, a Agência desempenha:

a) As funções que lhe são conferidas pelo Regulamento (UE) 2019/816 do Parlamento Europeu e do Conselho (*);

b) As funções relacionadas com a formação para a utilização técnica do ECRIS-TCN e da aplicação de referência do ECRIS.»

(*) Regulamento (UE) 2019/816 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, que cria um sistema centralizado para a determinação dos Estados-Membros que possuem informações sobre condenação de nacionais de países terceiros e de apátridas (ECRIS-TCN) tendo em vista completar o Sistema Europeu de Informação sobre Registos Criminais e que altera o Regulamento (UE) 2018/1726 (HL L 135., 2019.5.22., 1. o.).»;

3) No artigo 14.º, o n.º 1 passa a ter a seguinte redação:

«1. A Agência acompanha a evolução das atividades de investigação pertinentes para a gestão operacional do SIS II, do VIS, do Eurodac, do SES, do ETIAS, da DubliNet, do ECRIS-TCN e de outros sistemas informáticos de grande escala referidos no artigo 1.º, n.º 5.»;

4) No artigo 19.º, o n.º 1 é alterado do seguinte modo:

a) A alínea ee) passa a ter a seguinte redação:

«ee) Adota os relatórios sobre o desenvolvimento do SES, nos termos do artigo 72.º, n.º 2, do Regulamento (UE) 2017/2226, os relatórios sobre o desenvolvimento do ETIAS, nos termos do artigo 92.º, n.º 2, do Regulamento (UE) 2018/1240, e os relatórios sobre o desenvolvimento do ECRIS-TCN e sobre a aplicação de referência do ECRIS, nos termos do artigo 36.º, n.º 3, do Regulamento (UE) 2019/816;»;

b) A alínea ff) passa a ter a seguinte redação:

«ff) Adota os relatórios sobre o funcionamento técnico do SIS II, nos termos, respetivamente, do artigo 50.º, n.º 4, do Regulamento (CE) n.º 1987/2006 e do artigo 66.º, n.º 4, da Decisão 2007/533/JAI, do VIS, nos termos do artigo 50.º, n.º 3, do Regulamento (CE) n.º 767/2008 e do artigo 17.º, n.º 3, da Decisão 2008/633/JAI, do SES, nos termos do artigo 72.º, n.º 4, do Regulamento (UE) 2017/2226, e do ETIAS, nos termos do artigo 92.º, n.º 4, do Regulamento (UE) 2018/1240, do ECRIS-TCN e da aplicação de referência do ECRIS, nos termos do artigo 36.º, n.º 8, do Regulamento (UE) 2019/816;»;

c) A alínea hh) passa a ter a seguinte redação:

«hh) Adota observações formais sobre os relatórios da Autoridade Europeia para a Proteção de Dados relativos às auditorias efetuadas nos termos do artigo 45.º, n.º 2, do Regulamento (CE) n.º 1987/2006, do artigo 42.º, n.º 2, do Regulamento (CE) n.º 767/2008, do artigo 31.º, n.º 2, do Regulamento (UE) n.º 603/2013, do artigo 56.º, n.º 2, do Regulamento (UE) 2017/2226, do artigo 67.º do Regulamento (UE) 2018/1240 e do artigo 29.º, n.º 2, do Regulamento (UE) 2019/816 e assegura que seja dado o adequado seguimento a essas auditorias;»;

d) É aditada a seguinte alínea:

«ll-A) Apresenta à Comissão estatísticas relacionadas com o ECRIS-TCN e a aplicação de referência do ECRIS, nos termos do artigo 32.º, n.º 3, segundo parágrafo, do Regulamento (UE) 2019/816;»;

e) A alínea mm) passa a ter a seguinte redação:

«mm) Assegura a publicação anual da lista das autoridades competentes autorizadas a consultar diretamente os dados introduzidos no SIS II, nos termos do artigo 31.º, n.º 8, do Regulamento (CE) n.º 1987/2006 e do artigo 46.º, n.º 8, da Decisão 2007/533/JAI, juntamente com a lista dos serviços dos sistemas nacionais do SIS II (gabinetes N.SIS II) e dos gabinetes SIRENE, nos termos do artigo 7.º, n.º 3, do Regulamento (CE) n.º 1987/2006 e no artigo 7.º, n.º 3, da Decisão 2007/533/JAI, respetivamente, bem como a lista das autoridades competentes nos termos do artigo 65.º, n.º 2, do Regulamento (UE) 2017/2226, a lista das autoridades competentes nos termos do artigo 87.º, n.º 2, do Regulamento (UE) 2018/1240 e a lista das autoridades centrais nos termos do artigo 34.º, n.º 2, do Regulamento (UE) 2019/816;»;

5) No artigo 22.º, n.º 4, após o terceiro parágrafo é inserido o seguinte parágrafo:

«A Eurojust, a Europol e a EPPO podem igualmente participar com o estatuto de observador nas reuniões do Conselho de Administração quando figure na ordem de trabalhos qualquer questão relativa ao ECRIS-TCN que esteja relacionada com o Regulamento (UE) 2019/816.»;

6) No artigo 24.º, n.º 3, a alínea p) passa a ter a seguinte redação:

«p) A criação das normas de confidencialidade, sem prejuízo do disposto no artigo 17.º do Estatuto dos Funcionários, em cumprimento do disposto no artigo 17.º do Regulamento (CE) n.º 1987/2006, no artigo 17.º da Decisão 2007/533/JAI, no artigo 26.º, n.º 9, do Regulamento (CE) n.º 767/2008, no artigo 4.º, n.º 4, do Regulamento (UE) n.º 603/2013, no artigo 37.º, n.º 4, do Regulamento (UE) 2017/2226, no artigo 74.º, n.º 2, do Regulamento (UE) 2018/1240 e no artigo 11.º, n.º 16, do Regulamento (UE) 2019/816»;

7) No artigo 27.º, n.º 1, é inserida a seguinte alínea:

«da) Grupo Consultivo do ECRIS-TCN;».

Artigo 41.º

Aplicação e disposições transitórias

1. Os Estados-Membros tomam as medidas necessárias para dar cumprimento ao presente regulamento o mais rapidamente possível, a fim de assegurar o bom funcionamento do ECRIS-TCN.

2. No respeitante às condenações proferidas antes da data de início da introdução dos dados nos termos do artigo 35.º, n.º 1, as autoridades centrais criam os ficheiros individuais no sistema central do seguinte modo:

a) Os dados alfanuméricos devem ser introduzidos no sistema central até ao final do período referido no artigo 35.º, n.º 2;

b) Os dados dactiloscópicos devem ser introduzidos no sistema central o mais tardar dois anos após a entrada em funcionamento, nos termos do artigo 35.º, n.º 4.

Artigo 42.º

Entrada em vigor

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 em todos os Estados-Membros, em conformidade com os Tratados.

Feito em Estrasburgo, em 17 de abril de 2019.

Pelo Parlamento Europeu	*Pelo Conselho*
O Presidente	*O Presidente*
A. TAJANI	G. CIAMBA

ANEXO

FORMULÁRIO NORMALIZADO DE PEDIDO DE INFORMAÇÕES, NOS TERMOS DO ARTIGO 17.º, N.º 1, DO REGULAMENTO (UE) 2019/816, A FIM DE OBTER INFORMAÇÕES SOBRE QUAL O ESTADO-MEMBRO DA UE, SE ALGUM HOUVER, QUE POSSUI INFORMAÇÕES SOBRE OS REGISTOS CRIMINAIS DE UM NACIONAL DE UM PAÍS TERCEIRO

Este formulário, disponível em www.eurojust.europa.eu em todas as 24 línguas oficiais das instituições da União, deve ser enviado numa dessas línguas para ECRIS-TCN@eurojust.europa.eu

Estado ou organização internacional requerente:

Nome do Estado ou organização internacional:
Autoridade que apresenta o pedido:
Representada por (*nome da pessoa*):
Título:
Morada:
Número de telefone:
Endereço eletrónico:

Processos penais para os quais a informação é pedida:

Número de referência nacional:
Autoridade competente:
Tipo de crimes sob investigação (*refira o(s) artigo(s) pertinente(s) do código penal*):
Outras informações relevantes (*por exemplo, urgência do pedido*):

Informações sobre a identidade da pessoa nacional de um país terceiro a respeito da qual se pedem informações sobre o Estado-Membro de condenação:

N.B.: apresente o máximo de informações possível.

Apelido:
Nome(s) próprio(s):
Data de nascimento:
Local de nascimento (*localidade e país*):
Nacionalidade ou nacionalidades:
Sexo:
Nome(s) anterior(es), se aplicável:
Filiação:
Número de identificação:
Tipo e número do(s) documento(s) de identificação:
Autoridade emissora do(s) documento(s):
Pseudónimos ou alcunhas:
Se disponíveis, incluir os dados dactiloscópicos.

Caso se trate de várias pessoas, devem ser indicadas separadamente

Uma lista pendente permitiria inserir domínios adicionais

Lugar	
Data	

Assinatura e carimbo (eletrónicos):

REGULAMENTO (UE) 2019/817 DO PARLAMENTO EUROPEU E DO CONSELHO

de 20 de maio de 2019

relativo à criação de um regime de interoperabilidade entre os sistemas de informação da UE no domínio das fronteiras e vistos e que altera os Regulamentos (CE) n.º 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 do Parlamento Europeu e do Conselho, e as Decisões 2004/512/CE e 2008/633/JAI do Conselho

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,

Tendo em conta o parecer do Comité Económico e Social Europeu ([1]),

Após consulta ao Comité das Regiões,

Deliberando de acordo com o processo legislativo ordinário ([2]),

Considerando o seguinte:

(1) Na comunicação, de 6 de abril de 2016, intitulada Sistemas de informação mais sólidos e inteligentes para controlar as fronteiras e garantir a segurança, 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 deu início a 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 têm as informações necessárias à sua disposição.

(2) No Roteiro para intensificar o intercâmbio e a gestão de informações, incluindo soluções de interoperabilidade no domínio da Justiça e Assuntos Internos de 6 de junho de 2016, o Conselho identificou vários desafios de caráter jurídico, técnico e operacional na interoperabilidade dos sistemas de informação da UE e apelou para a procura de soluções.

(3) Na resolução de 6 de julho de 2016 sobre as prioridades estratégicas do Programa de Trabalho da Comissão para 2017 ([3]), o Parlamento Europeu apelou para a 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) Nas conclusões de 15 de dezembro de 2016, o Conselho Europeu apelou para que se continuasse a trabalhar no sentido de alcançar a interoperabilidade dos sistemas de informação e das bases de dados da UE.

(5) No relatório final de 11 de maio de 2017, 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 a interoperabilidade pode, em princípio, gerar ganhos operacionais e ser estabelecidas em conformidade com os requisitos em matéria de proteção de dados.

([1]) JO C 283 de 10.8.2018, p. 48.
([2]) Posição do Parlamento Europeu de 16 de abril de 2019 (ainda não publicada no Jornal Oficial) e decisão do Conselho de 14 de maio de 2019.
([3]) JO C 101 de 16.3.2018, p. 116.

(6) Na comunicação de 16 de maio de 2017 intitulada Sétimo relatório sobre os progressos alcançados rumo à criação de uma União da Segurança genuína e eficaz, a Comissão definiu, em conformidade com a sua Comunicação de 6 de abril de 2016, e nas conclusões e recomendações do grupo de peritos de alto nível sobre sistemas de informação e interoperabilidade, uma nova abordagem em matéria de gestão de dados para fins de controlo das fronteiras, segurança e migração segundo a qual 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 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) Nas conclusões de 23 de junho de 2017, o Conselho Europeu, 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 com base nas propostas apresentadas pelo grupo de peritos de alto nível sobre sistemas de informação e interoperabilidade.

(9) A fim de melhorar a eficácia e a eficiência dos controlos nas fronteiras externas, contribuir para a prevenção e o combate à imigração ilegal e contribuir para um nível de segurança elevado no domínio da liberdade, da segurança e da justiça da União, incluindo a manutenção da segurança e da ordem pública e a salvaguarda da segurança nos territórios dos Estados-Membros, melhorar a aplicação da política comum em matéria de vistos, prestar assistência no âmbito do exame dos pedidos de proteção internacional, contribuir para a prevenção, deteção e investigação de infrações terroristas ou de outras infrações penais graves, ajudar na identificação de pessoas desconhecidas que não são capazes de se identificar ou de restos mortais humanos não identificados em caso de catástrofes naturais, acidentes ou ataques terroristas, com vista a preservar a confiança dos cidadãos no sistema de migração e asilo da União, nas medidas de segurança da União e nas capacidades da União para gerir as fronteiras externas, deverá 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, respeitando simultaneamente os direitos fundamentais das pessoas, em particular o direito à proteção dos dados pessoais. Para concretizar este objetivo, é necessário criar um portal europeu de pesquisa (ESP), um serviço partilhado de correspondências biométricas (serviço partilhado 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 que esses sistemas se complementem mutuamente a fim de facilitar a correta identificação de pessoas, nomeadamente pessoas desconhecidas que não são capazes de se identificar ou restos mortais humanos não identificados, 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, reforçar 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 prevenção, deteção ou investigação de infrações terroristas ou de outras infrações penais graves 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 ECRIS-TCN.

(11) Os componentes de interoperabilidade deverão abranger o SES, o VIS, o ETIAS, o Eurodac, o SIS e o ECRIS-TCN. Os referidos componentes deverão igualmente abranger os dados da Europol, mas apenas na medida em que os dados da Europol possam ser consultados em simultâneo com esses sistemas de informação da UE.

(12) Os componentes de interoperabilidade deverão processar os dados pessoais de pessoas cujos dados pessoais sejam tratados nos sistemas de informação subjacentes da UE e pela Europol.

(13) O ESP deverá ser criado para facilitar, tecnicamente, o acesso de forma rápida, contínua, eficiente, sistemática e controlada pelas autoridades dos Estados-Membros e pelas agências da União aos sistemas de informação da UE, aos dados da Europol, bem como às bases de dados da Organização Internacional de Polícia Criminal (Interpol),

na medida em que tal seja necessário ao desempenho das suas funções, em conformidade com os respetivos direitos de acesso. O ESP deverá ser criado para apoiar os objetivos do SES, do VIS, do ETIAS, do Eurodac, do SIS, do ECRIS-TCN e dos dados da Europol. Ao permitir a consulta de todos os sistemas de informação da UE pertinentes, bem como dos dados da Europol e das bases de dados da Interpol em paralelo, 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 em matéria de controlo de acessos e de proteção de dados dos sistemas subjacentes.

(14) A conceção do ESP não deverá permitir que, ao consultar as bases de dados da Interpol, os dados utilizados por um utilizador do ESP na sua consulta sejam partilhados com os titulares dos dados da Interpol. A conceção do ESP deverá igualmente garantir que as bases de dados da Interpol só sejam consultadas nos termos do direito da União e nacional aplicável.

(15) A base de dados relativa a Documentos de Viagem Roubados e Extraviados (base de dados SLTD) da Interpol permite às entidades autorizadas responsáveis pela prevenção, deteção ou investigação de infrações terroristas ou de outras infrações penais graves nos Estados-Membros, incluindo as autoridades 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 (base de dados TDAWN) da Interpol, no contexto da avaliação sobre 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 ESP deverá permitir consultas das bases de dados SLTD e TDAWN utilizando os dados de identificação de um indivíduo ou os dados dos documentos de viagem. 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 ([4]), ou as disposições nacionais de transposição do capítulo V da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho ([5]). A aplicação dessas disposições não deverá prejudicar a aplicação das regras específicas previstas na Posição Comum 2005/69/JAI do Conselho ([6]) e na Decisão 2007/533/JAI do Conselho ([7]).

(16) O ESP deverá ser desenvolvido e configurado de modo que, na consulta, apenas seja possível utilizar dados que estejam relacionados com pessoas ou documentos de viagem, ou que estejam presentes num sistema de informação da UE, nos dados da Europol ou nas bases de dados da Interpol.

(17) A fim de assegurar a utilização sistemática dos sistemas de informação pertinentes da UE, o ESP deverá ser utilizado para consultar o CIR, o SES, o VIS, o ETIAS, o Eurodac e o ECRIS-TCN. No entanto, deverá manter-se a ligação nacional aos diferentes sistemas de informação da UE a fim de proporcionar uma alternativa técnica. O ESP deverá ser igualmente utilizado pelas agências da União para consultar o SIS Central, em conformidade com os respetivos direitos de acesso e para o desempenho das suas funções. O ESP deverá constituir um meio suplementar de consulta do SIS Central, dos dados da Europol e das bases de dados da Interpol, complementando as interfaces específicas existentes.

(18) Os dados biométricos, como as impressões digitais e as imagens faciais, são únicos e, por conseguinte, muito mais fiáveis do que os dados alfanuméricos para efeito de identificação de uma pessoa. O serviço partilhado BMS deverá constituir 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 serviço partilhado BMS deverá consistir na facilitação da identificação de uma pessoa que possa estar registada em várias bases de dados, procurando correspondências com os seus dados biométricos nos diferentes sistemas e baseando-se num único componente tecnológico em vez de em diversos componentes, em cada um dos sistemas subjacentes. O serviço partilhado BMS trará vantagens em termos de segurança, bem como em termos financeiros, de manutenção e operacionais. Todos os sistemas automáticos de identificação dactiloscópica, incluindo os que são presentemente utilizados no Eurodac, VIS e SIS, utilizam modelos biométricos constituídos por dados provenientes de uma extração de características de amostras biométricas reais. O serviço partilhado BMS deverá reunir e armazenar todos estes modelos biométricos — separados, segundo um método lógico, de acordo com o sistema de informação de que provêm os dados — num único local, facilitando assim as comparações entre sistemas, mediante utilização de modelos biométricos, e permitindo economias de escala no desenvolvimento e manutenção de sistemas centrais da UE.

([4]) 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).

([5]) 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).

([6]) 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).

([7]) 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).

(19) Os modelos biométricos armazenados no serviço partilhado BMS deverão ser constituídos por dados provenientes de uma extração das características de amostras biométricas reais e ser obtidos de forma a não permitir a reversão do processo de extração. Os modelos biométricos deverão ser obtidos a partir de dados biométricos, mas não deverá ser possível obter os mesmos dados biométricos a partir dos modelos biométricos. Uma vez que os dados relativos a impressões palmares e os perfis de ADN só são armazenados no SIS e não podem ser utilizados para fins de verificações cruzadas com os dados contidos noutros sistemas de informação, em conformidade com os princípios da necessidade e da proporcionalidade, o serviço partilhado BMS não deverá armazenar os perfis de ADN nem os modelos biométricos obtidos a partir dos dados relativos a impressões palmares.

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

(21) O SES, o VIS, o ETIAS, o Eurodac e o sistema ECRIS-TCN exigem a correta identificação das pessoas cujos dados pessoais aí se encontram armazenados. O CIR deverá, por conseguinte, o facilitar a correta identificação das pessoas registadas nesses sistemas.

(22) Os dados pessoais armazenados naqueles sistemas de informação da UE podem respeitar às mesmas pessoas, mas sob diferentes identidades ou incompletas. Os Estados-Membros dispõem de meios eficazes para identificar os seus cidadãos ou residentes permanentes registados no seu território. A interoperabilidade entre os sistemas de informação da UE deverá contribuir para a correta identificação das pessoas presentes nesses sistemas. O CIR deverá armazenar os dados pessoais necessários para permitir uma identificação mais exata dos indivíduos cujos dados pessoais estão armazenados nesses sistemas, incluindo dados de identificação, dados sobre 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 não deverão ser conservados por mais tempo do que o estritamente necessário para efeitos dos sistemas subjacentes e deverão ser automaticamente eliminados quando os dados forem eliminados nos respetivos sistemas, de acordo com a sua separação lógica.

(23) A nova operação de tratamento que consiste no armazenamento desses dados no 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, os dados dos documentos de viagem e os dados biométricos serem armazenados no CIR não deverá levantar qualquer obstáculo ao tratamento de dados para efeitos do SES, VIS, ETIAS, Eurodac ou ECRIS-TCN, na medida em que o CIR será um novo componente partilhado desses sistemas subjacentes.

(24) É, por conseguinte, necessário criar um processo individual no 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 de pessoas no espaço Schengen, e apoiar o MID com o duplo objetivo de facilitar os controlos de identidade de viajantes de boa-fé e combater a fraude de identidade. O processo individual deverá armazenar toda a informação sobre identidade ligada a uma pessoa num único local e ser de acesso autorizado aos utilizadores finais.

(25) O CIR deverá, por isso, facilitar e simplificar o acesso das autoridades responsáveis pela prevenção, deteção ou investigação de infrações terroristas ou de outras infrações penais graves aos sistemas de informação da UE que não foram estabelecidos exclusivamente para efeitos de prevenção, deteção ou de investigação de crimes graves.

(26) O CIR deverá prever um recipiente partilhado para dados de identificação, dados dos documentos de viagem e dados biométricos das pessoas registadas no SES, no VIS, no ETIAS, no Eurodac e no ECRIS-TCN. O CIR deverá fazer parte da arquitetura técnica destes sistemas e funcionar como o componente partilhado entre eles para o armazenamento e consulta dos dados de identificação, dos dados dos documentos de viagem e dos dados biométricos por si tratados.

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

(28) Quando uma autoridade policial de um Estado-Membro não estiver em condições de identificar uma pessoa devido à falta de um documento de viagem ou de outro documento credível que comprove a sua identidade ou quando haja dúvidas quanto aos dados de identificação fornecidos por essa pessoa ou quanto à autenticidade do

documento de viagem ou à identidade do seu titular, ou se a pessoa for incapaz de cooperar ou se recusar a fazê-lo, essa autoridade policial deverá poder consultar o CIR a fim de identificar a pessoa em causa. Para o efeito, as autoridades policiais deverão recolher impressões digitais através de técnicas de recolha de impressões digitais por meio de digitalização direta desde que o procedimento tenha sido iniciado na presença da pessoa. Tais consultas do CIR não poderão ser permitidas para fins de identificação de menores de 12 anos, salvo se forem feitas no interesse superior da criança.

(29) Caso não seja possível utilizar os dados biométricos de uma pessoa, ou se a consulta desses dados falhar, a consulta deverá 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 CIR, as autoridades dos Estados-Membros deverão ter acesso ao sistema para consultar os dados de identificação e os dados dos documentos de viagem dessa pessoa, sem que o CIR forneça nenhuma indicação quanto ao sistema de informação da UE ao qual os dados pertencem.

(30) Os Estados-Membros deverão adotar medidas legislativas nacionais, no sentido de designar as autoridades competentes para efetuar controlos de identidade recorrendo à utilização do 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, deverá ser objeto de legislação nacional.

(31) O presente regulamento deverá também introduzir uma nova possibilidade de simplificação do acesso a dados, para além dos dados de identificação ou dos dados dos documentos de viagem existentes no SES, no VIS, no ETIAS ou no Eurodac, por parte das autoridades responsáveis pela prevenção, deteção ou investigação de infrações terroristas ou de outras infrações penais graves dos Estados-Membros e da Europol. Esses dados podem ser necessários para efeitos de prevenção, deteção ou investigação das infrações terroristas ou de outras infrações penais graves num caso específico, sempre que existam motivos razoáveis para considerar que a consulta contribuirá para a prevenção, deteção ou investigação das infrações terroristas ou outras infrações penais graves, em especial quando exista uma suspeita de que o suspeito, o autor ou a vítima de uma infração terrorista ou de outra infração penal grave é uma pessoa cujos dados estão armazenados no SES, no VIS, no ETIAS ou no Eurodac.

(32) O pleno acesso aos dados contidos no SES, no VIS, no ETIAS ou no Eurodac, necessário para fins de prevenção, deteção ou investigação de infrações terroristas ou outras infrações penais graves, para além do acesso aos dados de identificação ou aos dados dos documentos de viagem conservados pelo CIR, deverá continuar a ser regido pelos atos jurídicos aplicáveis. As autoridades designadas responsáveis pela prevenção, deteção ou investigação de infrações terroristas ou de outras infrações penais graves 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. O utilizador final autorizado pela autoridade designada deverá, por conseguinte, ser autorizado a ver em qual dos sistemas de informação da UE estão registados os dados correspondentes aos resultados da consulta. O sistema em causa seria, assim, assinalado na sequência da verificação automática da presença de uma correspondência no sistema (a chamada funcionalidade de indicadores de correspondência).

(33) Neste contexto, a resposta do CIR não deverá ser interpretada ou utilizada como fundamento ou motivo para tirar conclusões sobre uma pessoa ou tomar medidas relativamente à mesma, devendo ser utilizada apenas para efeitos de apresentação de um pedido de acesso aos sistemas de informação subjacentes da UE, em conformidade com as condições e os procedimentos estabelecidos nos atos jurídicos pertinentes que regem esse acesso. Tal pedido de acesso deverá estar sujeito ao capítulo VII do presente regulamento e, se for caso disso, ao Regulamento (UE) 2016/679, à Diretiva (UE) 2016/680 ou ao Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho ([8]).

(34) Regra geral, quando um indicador de correspondência revele que os dados estão registados no SES, no VIS, no ETIAS ou no Eurodac, as autoridades designadas ou a Europol deverão solicitar o pleno acesso a, pelo menos, um dos sistemas de informação da UE em causa. Se, excecionalmente, não for solicitado o pleno acesso, por exemplo, porque as autoridades designadas ou a Europol já obtiveram os dados por outros meios, ou porque a obtenção dos dados já não é permitida pela legislação nacional, deverá ser registada a justificação da decisão de não solicitar o acesso.

([8]) Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (JO L 295 de 21.11.2018, p. 39).

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

(36) A consulta do CIR pelas autoridades designadas e pela Europol a fim de obter uma resposta com indicador de correspondência 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 correspondência não deverá 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 correspondência. Por conseguinte, o acesso do utilizador final a um indicador de correspondência terá uma interferência muito limitada no direito à proteção de dados pessoais da pessoa em causa e permite que a autoridade designada e a Europol requeiram o acesso aos dados pessoais de forma mais eficaz.

(37) O MID deverá ser criado para apoiar o funcionamento do CIR e para apoiar os objetivos do SES, do VIS, do ETIAS, do Eurodac, do SIS e do ECRIS-TCN. Para que esses objetivos sejam atingidos, é conveniente dispor da identificação precisa das pessoas cujos dados pessoais estão armazenados nesses sistemas de informação UE.

(38) Para melhor atingir os objetivos dos sistemas de informação da UE, as autoridades que utilizam estes sistemas deverão poder realizar verificações suficientemente fiáveis das identidades das pessoas cujos dados estão armazenados em sistemas diferentes. O conjunto dos dados de identificação ou dos dados dos documentos de viagem armazenados num determinado sistema individual podem ser incorretos, incompletos ou fraudulentos, e atualmente não existe qualquer forma de detetar dados de identificação ou dados dos documentos de viagem incorretos, incompletos ou fraudulentos 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 das pessoas para estes fins.

(39) O MID deverá 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 deverá conter apenas as ligações entre as pessoas presentes em mais de um sistema de informação da UE. A ligação de dados deverá ser estritamente limitada aos dados necessários para verificar se uma pessoa está registada de forma justificada ou injustificada sob diferentes identidades em sistemas diferentes, ou para clarificar situações em que duas pessoas com dados de identificação semelhantes podem não ser a mesma pessoa. O tratamento de dados através do ESP e do serviço partilhado de BMS com o objetivo de estabelecer ligações entre os processos individuais nos diferentes sistemas deverá ser limitado ao mínimo e, por conseguinte, deverá apenas abranger a deteção de identidades múltiplas a realizar no momento em que são adicionados dados novos a um dos sistemas de informação que tenha dados armazenados no CIR ou adicionados no SIS. O MID deverá dispor de salvaguardas contra eventuais discriminações e decisões desfavoráveis para pessoas com identidades múltiplas lícitas.

(40) 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 da União Europeia. 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 e pela aplicação eficaz das políticas de asilo e de vistos da União.

(41) Sempre que uma autoridade nacional ou uma agência da União cria ou carrega novos registos, o ESP e o serviço partilhado BMS deverão comparar os dados referentes a pessoas existentes no CIR e no SIS. Esta comparação deverá ser automatizada. O CIR e o SIS deverão utilizar o BMS para detetar eventuais ligações com base em dados biométricos. O CIR e o SIS deverão utilizar o ESP para detetar eventuais ligações com base em dados alfanuméricos. O CIR e o SIS deverão ser capazes de identificar dados idênticos ou dados semelhantes sobre as pessoas armazenados em vários sistemas. Sempre que se aplique, deverá criar-se uma ligação indicando que se trata da mesma pessoa. O CIR e o SIS deverão ser configurados de forma a que os pequenos erros de transliteração ou ortográficos detetados não criem qualquer obstáculo injustificado à pessoa em causa.

(42) A autoridade nacional ou agência da União que registou os dados no respetivo sistema de informação da UE deverá confirmar ou alterar estas ligações. Essa autoridade nacional ou agência da União deverá ter acesso aos dados armazenados no CIR ou no SIS e no MID para efeitos da verificação manual das diferentes identidades.

(43) A verificação manual das diferentes identidades deverá ser assegurada pela autoridade que cria ou atualiza os dados que desencadearam uma correspondência, resultando numa ligação com dados já armazenados noutro sistema de informação da UE. A autoridade responsável pela verificação manual das diferentes identidades deverá analisá-las para determinar se se referem à mesma pessoa de forma justificada ou injustificada. Essa análise deverá ser efetuada, sempre que possível, na presença das pessoas em causa e, quando necessário, solicitando esclarecimentos ou informações adicionais. Essa análise deverá ser efetuada sem demora, em conformidade com as obrigações legais quanto à exatidão das informações ao abrigo do direito da União e do direito nacional. Especialmente nas fronteiras, a circulação das pessoas em causa deverá ser limitada durante todo o processo de verificação, que não deverá durar indefinidamente. A existência de uma ligação amarela no MID não deverá constituir, por si só, um motivo para a recusa de entrada, e toda e qualquer decisão de autorização ou recusa de entrada deverá ser tomada exclusivamente com base nas disposições aplicáveis do Regulamento (UE) 2016/399 do Parlamento Europeu e do Conselho ([9]).

(44) Para as ligações obtidas através do 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 ou sobre pessoas para efeitos de vigilância discreta, controlos de verificação ou controlos específicos, a autoridade responsável pela verificação manual das diferentes identidades deverá ser o gabinete SIRENE do Estado-Membro que criou a indicação. Essas categorias de indicações do SIS são sensíveis e não deverão ser necessariamente partilhadas com as autoridades que criam ou atualizam os dados ligados a essas categorias 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 nos termos dos Regulamentos (UE) 2018/1860 ([10]), (UE) 2018/1861 ([11]) e (UE) 2018/1862 ([12]) do Parlamento Europeu e do Conselho.

(45) A criação dessas ligações exige transparência em relação às pessoas afetadas. A fim de facilitar a aplicação das salvaguardas necessárias nos termos das regras aplicáveis da União em matéria de proteção de dados, as pessoas que tenham uma ligação branca ou vermelha após a verificação manual deverão ser informadas por escrito, sem prejuízo das limitações para proteger a segurança e a ordem pública, prevenir a criminalidade e assegurar que as investigações nacionais não sejam comprometidas. Essas pessoas deverão receber um número de identificação único que lhes permita identificar a autoridade à qual deverão dirigir-se para exercerem os seus direitos.

(46) Caso seja criada uma ligação amarela, a autoridade responsável pela verificação manual das diferentes identidades deverá ter acesso ao MID. Caso exista uma ligação vermelha, as autoridades dos Estados-Membros e as agências da União com acesso a, pelo menos, um dos sistemas de informação da UE incluídos no CIR ou ao SIS, deverão ter acesso ao MID. A ligação vermelha deverá indicar que a pessoa utiliza diferentes identidades de forma injustificada ou que a pessoa utiliza a identidade de outrem.

(47) Caso exista uma ligação verde ou branca entre os dados de dois sistemas de informação da UE, as autoridades dos Estados-Membros e as agências da União deverão ter acesso ao MID, nos casos em que a autoridade ou a agência em causa tenha acesso a ambos os sistemas de informação. Esse acesso deverá ser concedido unicamente com o propósito de permitir que essa autoridade ou agência detete potenciais casos em que os dados tenham sido incorretamente ligados ou tratados no MID, no CIR e no SIS em violação do presente regulamento e de tomar as medidas para corrigir a situação e atualizar ou apagar a ligação.

([9]) 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 (Código das Fronteiras Schengen) (JO L 77 de 23.3.2016, p. 1).

([10]) Regulamento (UE) 2018/1860 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo à utilização do Sistema de Informação de Schengen para efeitos de regresso dos nacionais de países terceiros em situação irregular (JO L 312 de 7.12.2018, p. 1).

([11]) Regulamento (UE) 2018/1861 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen (SIS) no domínio dos controlos de fronteira, e que altera a Convenção de Aplicação do Acordo de Schengen e altera e revoga o Regulamento (CE) n.º 1987/2006 (JO L 312 de 7.12.2018, p. 14).

([12]) Regulamento (UE) 2018/1862 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen (SIS) no domínio da cooperação policial e da cooperação judiciária em matéria penal, e que altera e revoga a Decisão 2007/533/JAI do Conselho e revoga o Regulamento (CE) n.º 1986/2006 do Parlamento Europeu e do Conselho e a Decisão 2010/261/UE da Comissão (JO L 312 de 7.12.2018, p. 56).

(48) A Agência europeia para a gestão operacional de sistemas informáticos de grande escala no espaço da liberdade, segurança e justiça (eu-LISA) deverá criar mecanismos automatizados de controlo de qualidade de dados e indicadores comuns da qualidade dos dados. A eu-LISA deverá ser responsável por desenvolver uma capacidade central de monitorização da qualidade dos dados, bem como por elaborar periodicamente relatórios de análise de dados para melhorar o controlo da aplicação dos sistemas de informação da UE por parte dos Estados-Membros. Os indicadores comuns de qualidade deverão 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.

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

(50) O Formato de Mensagem Universal (UMF) deverá constituir uma norma para o intercâmbio estruturado de informações transfronteiriço entre os sistemas de informação, autoridades e/ou organizações no domínio da Justiça e Assuntos Internos. O UMF deverá 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.

(51) A aplicação da norma UMF poderá ser tida em consideração no VIS, no SIS e em quaisquer outros modelos de intercâmbio de informações transfronteiriço e sistemas de informação, existentes ou novos, no domínio da justiça e dos assuntos internos, desenvolvidos pelos Estados-Membros.

(52) 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, nos termos dos atos jurídicos aplicáveis. A eu-LISA deverá criar, aplicar e alojar o CRRS nos seus sítios técnicos. A eu-LISA deverá conter dados estatísticos anonimizados dos sistemas de informação da UE, do CIR, do MID e do serviço partilhado BMS. Os dados contidos no CRRS não deverão permitir identificar pessoas. A eu-LISA deverá tornar os dados anónimos de forma automatizada e deverá registar esses mesmos dados anonimizados no CRRS. O processo de tornar os dados anónimos deverá ser automatizado e o pessoal da eu-LISA não deverá ter acesso direto aos dados pessoais armazenados nos sistemas de informação da UE ou nos componentes de interoperabilidade.

(53) O Regulamento (UE) 2016/679 aplica-se ao tratamento de dados pessoais para efeitos de interoperabilidade 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.

(54) Caso o tratamento de dados pessoais pelos Estados-Membros para efeitos de interoperabilidade nos termos do presente regulamento seja efetuado pelas autoridades competentes para efeitos de prevenção, deteção ou investigação de infrações terroristas ou de outras infrações penais graves, aplica-se a Diretiva (UE) 2016/680.

(55) O Regulamento (UE) 2016/679, o Regulamento (UE) 2018/1725 ou, se for caso disso, a Diretiva (UE) 2016/680 deverão aplicar-se igualmente às transferências de dados pessoais para países terceiros ou organizações internacionais realizadas nos termos do presente regulamento. Sem prejuízo dos motivos da transferência nos termos do capítulo V do Regulamento (UE) 2016/679 ou, se for caso disso, da Diretiva (UE) 2016/680, qualquer decisão de um órgão jurisdicional ou de uma autoridade administrativa de um país terceiro que exija a um responsável pelo tratamento dos dados ou a um subcontratante a transferência ou a divulgação de dados pessoais só deverá ser reconhecida ou executada, seja de que forma for, com base num acordo internacional em vigor entre o país terceiro requerente e a União ou um Estado-Membro.

(56) As disposições específicas sobre proteção de dados dos Regulamentos (UE) 2017/2226 ([13]), (CE) n.º 767/2008 ([14]), (UE) 2018/1240 ([15]) do Parlamento Europeu e do Conselho e do Regulamento (UE) 2018/1861 aplicam-se ao tratamento de dados pessoais nos sistemas regidos por esses regulamentos.

(57) O Regulamento (UE) 2018/1725 aplica-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 do Parlamento Europeu e do Conselho ([16]), que se aplica ao tratamento de dados pessoais pela Europol.

(58) As autoridades de controlo referidas no Regulamento (UE) 2016/679 ou na Diretiva (UE) 2016/680 deverão controlar a legalidade do tratamento dos dados pessoais pelos Estados-Membros. A Autoridade Europeia para a Proteção de Dados deverá 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. Para que a Autoridade Europeia para a Proteção de Dados cumpra as tarefas que lhe são confiadas por força do presente regulamento, são necessários meios suficientes, nomeadamente humanos e financeiros.

(59) 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 do Parlamento Europeu e do Conselho ([17]) e emitiu parecer em 16 de abril de 2018 ([18]).

(60) O Grupo do Artigo 29.º para a Proteção de Dados formulou um parecer em 11 de abril de 2018.

(61) Os Estados-Membros e a eu-LISA deverão 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 deverá igualmente assegurar a utilização contínua das mais recentes evoluções tecnológicas necessárias para garantir a integridade dos dados no contexto do desenvolvimento, conceção e gestão dos componentes de interoperabilidade. As obrigações da eu-LISA neste domínio deverão incluir a adoção das medidas necessárias para impedir o acesso de pessoas não autorizadas, como pessoal de prestadores de serviços externos, aos dados pessoais tratados através dos componentes de interoperabilidade. Na adjudicação de contratos de prestação de serviços, os Estados-Membros e a eu-LISA deverão ter em consideração todas as medidas necessárias para garantir o cumprimento da legislação ou da regulamentação relativa à proteção dos dados pessoais e da privacidade das pessoas ou para salvaguardar interesses essenciais em matéria de segurança, em conformidade com o Regulamento (UE, Euratom) 2018/1046 do Parlamento Europeu e do Conselho ([19]) e as convenções internacionais aplicáveis. A eu-LISA deverá aplicar os princípios da privacidade desde a conceção e por defeito durante o desenvolvimento dos componentes de interoperabilidade.

(62) 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. Esses impactos resultarão de uma aplicação combinada das regras existentes do Regulamento (UE) 2016/399 e das regras em matéria de interoperabilidade previstas no presente regulamento.

(63) Como consequência desta aplicação combinada das regras, o ESP deverá constituir o principal ponto de acesso para a consulta sistemática obrigatória de bases de dados relativamente a pessoas nos pontos de passagem de fronteiras previstos pelo Regulamento (UE) 2016/399. Além disso, para determinar se a pessoa reúne as condições de entrada estabelecidas no Regulamento (UE) 2016/399, os guardas de fronteira deverão ter em

([13]) 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, que determina as condições de acesso ao SES para efeitos de aplicação da lei, e que altera a Convenção de Aplicação do Acordo de Schengen e os Regulamentos (CE) n.º 767/2008 e (UE) n.º 1077/2011 (JO L 327 de 9.12.2017, p. 20).

([14]) 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).

([15]) Regulamento (UE) 2018/1240 do Parlamento Europeu e do Conselho, de 12 de setembro de 2018, que cria um Sistema Europeu de Informação e Autorização de Viagem (ETIAS) e altera os Regulamentos (UE) n.º 1077/2011, (UE) n.º 515/2014, (UE) 2016/399, (UE) 2016/1624 e (UE)2017/2226 (JO L 236 de 19.9.2018, p. 1).

([16]) Regulamento (UE) 2016/794 do Parlamento Europeu e do Conselho, de 11 de maio de 2016, que cria a Agência da União Europeia para a Cooperação Policial (Europol) e que substitui e revoga as Decisões 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI e 2009/968/JAI do Conselho (JO L 135 de 24.5.2016, p. 53).

([17]) 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).

([18]) JO C 233 de 4.7.2018, p. 12.

([19]) Regulamento (UE, Euratom) 2018/1046 do Parlamento Europeu e do Conselho, de 18 de julho de 2018, relativo às disposições financeiras aplicáveis ao orçamento geral da União, que altera os Regulamentos (UE) n.º 1296/2013, (UE) n.º 1301/2013, (UE) n.º 1303/2013, UE n.º 1304/2013, (UE) n.º 1309/2013, (UE) n.º 1316/2013, (UE) n.º 223/2014 e (UE) n.º 283/2014, e a Decisão n.º 541/2014/UE, e revoga o Regulamento (UE, Euratom) n.º 966/2012 (JO L 193 de 30.7.2018, p. 1).

consideração os dados de identificação ou os dados dos documentos de viagem que fizeram com que uma ligação no MID fosse classificada como ligação vermelha. Todavia, a presença de uma ligação vermelha não deverá constituir, por si só, um motivo de recusa de entrada e os atuais motivos de recusa da entrada constantes no Regulamento (UE) 2016/399 não deverão, por conseguinte, ser alterados.

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

(65) Se o resultado de uma consulta ao MID, através do ESP, for uma ligação amarela ou detetar uma ligação vermelha, o guarda de fronteira deverá consultar o CIR ou o SIS, ou ambos, para avaliar as informações sobre a pessoa controlada, para verificar manualmente os dados de identificação e para adaptar a cor da ligação, caso se aplique.

(66) Para efeitos de estatísticas e para a elaboração de relatórios, é necessário autorizar o acesso ao pessoal autorizado das autoridades, instituições e agências da União competentes a que se refere o presente regulamento para consulta de determinados dados relacionados com determinados componentes de interoperabilidade, sem permitir a identificação das pessoas.

(67) Para as autoridades dos Estados-Membros e as agências da União se adaptarem aos novos requisitos de utilização do ESP, é necessário prever um período transitório. De igual modo, a fim de permitir o funcionamento coerente e ótimo do MID, deverão ser estabelecidas medidas transitórias para a sua entrada em funcionamento.

(68) Atendendo a que o objetivo do presente regulamento, a saber, a criação de um regime de interoperabilidade entre os sistemas de informação da UE, não pode ser suficientemente alcançado pelos Estados-Membros, mas pode, devido à dimensão e aos efeitos da ação, ser mais bem alcançado ao nível da União, a União pode tomar medidas, em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do Tratado da União Europeia (TUE). Em conformidade com o princípio da proporcionalidade consagrado no mesmo artigo, o presente regulamento não excede o necessário para alcançar esse objetivo.

(69) O montante remanescente no orçamento reservado às fronteiras inteligentes no Regulamento (UE) n.º 515/2014 do Parlamento Europeu e do Conselho ([20]) deverá ser reafetado para fins do presente regulamento, nos termos do artigo 5.º, n.º 5, alínea b), do Regulamento (UE) n.º 515/2014, para cobrir os custos de desenvolvimento dos componentes de interoperabilidade.

(70) A fim de completar determinados aspetos técnicos pormenorizados do presente regulamento, o poder de adotar atos nos termos do artigo 290.º do Tratado sobre o Funcionamento da União Europeia (TFUE) deverá ser delegado na Comissão no que diz respeito a:

— prorrogar o período transitório para a utilização do ESP;

— prorrogar o período transitório para a utilização do detetor de identidades múltiplas da unidade central do ETIAS;

— procedimentos para determinar os casos em que os dados de identificação podem ser considerados idênticos ou similares;

— normas relativas ao funcionamento do CRRS, incluindo as garantias específicas para o tratamento dos dados pessoais e as normas de segurança aplicáveis ao repositório;

— regras pormenorizadas de funcionamento do portal Web.

É particularmente importante que a Comissão proceda às consultas adequadas durante os trabalhos preparatórios, inclusive ao nível de peritos, e que essas consultas sejam conduzidas de acordo com os princípios estabelecidos no Acordo Interinstitucional, de 13 de abril de 2016, sobre legislar melhor ([21]). Em particular, a fim de assegurar a igualdade de participação na preparação dos atos delegados, o Parlamento Europeu e o Conselho recebem todos os documentos ao mesmo tempo que os peritos dos Estados-Membros, e os respetivos peritos têm sistematicamente acesso às reuniões dos grupos de peritos da Comissão que tratem da preparação dos atos delegados.

(71) A fim de assegurar condições uniformes para a execução do presente regulamento, deverão ser atribuídas competências de execução à Comissão para fixar as datas a partir das quais o ESP, o serviço partilhado BMS, o CIR, o MID e o CRRS entram em funcionamento.

([20]) 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).

([21]) JO L 123 de 12.5.2016, p. 1.

(72) Deverão ser ainda atribuídas competências de execução à Comissão para a adoção de regras específicas sobre: os pormenores técnicos dos perfis dos utilizadores do ESP; as especificações da solução técnica para facilitar a consulta dos sistemas de informação da UE, dos dados da Europol e das bases de dados da Interpol pelo ESP e o formato das respostas do ESP; as normas técnicas para a criação de ligações no MID entre dados de diferentes sistemas de informação da UE; o conteúdo e apresentação do formulário para informação do titular dos dados em caso de criação de uma ligação vermelha; os requisitos de desempenho e monitorização do desempenho do serviço partilhado BMS; os mecanismos, procedimentos e indicadores automatizados de controlo da qualidade dos dados; o desenvolvimento da norma UMF; o procedimento de cooperação em caso de incidentes de segurança; e as especificações da solução técnica para os Estados– Membros gerirem os pedidos de acesso dos utilizadores. Essas competências deverão ser exercidas nos termos do Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho ([22]).

(73) Uma vez que os componentes de interoperabilidade envolvem o tratamento de quantidades significativas de dados pessoais sensíveis, é importante que as pessoas cujos dados são tratados através desses componentes possam, efetivamente, exercer os seus direitos enquanto titulares dos dados, tal como previsto no Regulamento (UE) 2016/679, na Diretiva (UE) 2016/680 e no Regulamento (UE) 2018/1725. Os titulares dos dados deverão dispor de um portal Web que lhes facilite o exercício dos seus direitos de acesso e de retificação, apagamento e limitação do tratamento dos seus dados pessoais. A criação e a gestão desse portal Web caberão à eu-LISA.

(74) Um dos princípios fundamentais da proteção de dados é a minimização dos dados: ao abrigo do artigo 5.º, n.º 1, alínea c), do Regulamento (UE) 2016/679, o tratamento de dados pessoais deve ser adequado, pertinente e limitado ao que é necessário relativamente às finalidades para as quais são tratados. Por este motivo, os componentes de interoperabilidade não deverão armazenar novos dados pessoais, com exceção das ligações que serão armazenadas no MID e que constituem o mínimo necessário para efeitos do presente regulamento.

(75) O presente regulamento deverá conter disposições claras sobre a responsabilização e o direito a indemnização pelo tratamento ilegal de dados pessoais e por qualquer ato que seja incompatível com o mesmo. As referidas disposições deverão ser aplicáveis, sem prejuízo do direito a indemnização e da responsabilização da pessoa que efetuou o tratamento dos dados ou do subcontratante, nos termos do Regulamento (UE) 2016/679, da Diretiva (UE) 2016/680 e do Regulamento (UE) 2018/1725. A eu-LISA deverá ser responsável pelos danos causados na sua qualidade de subcontratante de dados se não tiver cumprido as obrigações específicas que lhe incumbem por força do presente regulamento ou se não tiver seguido as instruções lícitas do Estado-Membro responsável pelo tratamento dos dados.

(76) O presente regulamento aplica-se sem prejuízo da aplicação da Diretiva 2004/38/CE do Parlamento Europeu e do Conselho ([23]).

(77) Nos termos dos artigos 1.º e 2.º do Protocolo n.º 22, relativo à posição da Dinamarca, anexo ao TUE e ao TFUE, a Dinamarca não participa na adoção do presente regulamento, e não fica a ele vinculada nem sujeita à sua aplicação. Uma vez que o presente regulamento desenvolve o acervo de Schengen, a Dinamarca decide, nos termos do artigo 4.º do Protocolo acima referido e no prazo de seis meses a contar da data de decisão do Conselho relativa ao presente regulamento, se procede à sua transposição para o seu direito interno.

(78) O presente regulamento constitui um desenvolvimento das disposições do acervo de Schengen em que o Reino Unido não participa, nos termos da Decisão 2000/365/CE do Conselho ([24]). Por conseguinte, o Reino Unido não participa na sua adoção e não fica a ele vinculado nem sujeito à sua aplicação.

(79) O presente regulamento constitui um desenvolvimento das disposições do acervo de Schengen em que a Irlanda não participa, nos termos da Decisão 2002/192/CE do Conselho ([25]). Por conseguinte, a Irlanda não participa na sua adoção e não fica a ele vinculada nem sujeita à sua aplicação.

([22]) 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).

([23]) Diretiva 2004/38/CE do Parlamento Europeu e do Conselho, de 29 de abril de 2004, relativa ao direito de livre circulação e residência dos cidadãos da União e dos membros das suas famílias no território dos Estados-Membros, que altera o Regulamento (CEE) n.º 1612/68 e que revoga as Diretivas 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE e 93/96/CEE (JO L 158 de 30.4.2004, p. 77).

([24]) 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).

([25]) 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).

(80) 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, à aplicação e ao desenvolvimento do acervo de Schengen ([26]), que se inserem no domínio a que se referem os pontos A, B, C e G do artigo 1.º da Decisão 1999/437/CE do Conselho ([27]).

(81) 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 ([28]), que se inserem no domínio a que se referem os pontos A, B, C e G do artigo 1.º da Decisão 1999/437/CE, em conjugação com o artigo 3.º da Decisão 2008/146/CE do Conselho ([29]).

(82) Em relação ao Listenstaine, 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 Listenstaine 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 Schengen ([30]) que se inserem no domínio a que se referem os pontos A, B, C e G do artigo 1.º da Decisão 1999/437/CE, em conjugação com o artigo 3.º da Decisão 2011/350/UE do Conselho ([31]).

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

(84) Para que o presente regulamento possa ser integrado no regime jurídico vigente, os Regulamentos (CE) n.º 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861, as Decisões 2004/512/CE ([32]) e 2008/633/JAI ([33]) do Conselho deverão ser alterados,

ADOTARAM O PRESENTE REGULAMENTO:

CAPÍTULO I

Disposições gerais

Artigo 1.º

Objeto

1. O presente regulamento, juntamente com o Regulamento (UE) 2019/818 do Parlamento Europeu e do Conselho ([34]), estabelece um regime destinado a 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).

([26]) JO L 176 de 10.7.1999, p. 36.
([27]) Decisão 1999/437/CE do Conselho, de 17 de maio de 1999, relativa a determinadas regras de aplicação do Acordo celebrado pelo Conselho da União Europeia com a República da Islândia e o Reino da Noruega relativo à associação dos dois Estados à execução, à aplicação e ao desenvolvimento do acervo de Schengen (JO L 176 de 10.7.1999, p. 31).
([28]) JO L 53 de 27.2.2008, p. 52.
([29]) Decisão 2008/146/CE do Conselho, de 28 de janeiro de 2008, respeitante à celebração, em nome da Comunidade Europeia, do 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 Schengen (JO L 53 de 27.2.2008, p. 1).
([30]) JO L 160 de 18.6.2011, p. 21.
([31]) Decisão 2011/350/UE do Conselho, de 7 de março de 2011, respeitante à celebração, em nome da União Europeia, do Protocolo entre a União Europeia, a Comunidade Europeia, a Confederação Suíça e o Principado do Listenstaine relativo à adesão do Principado do Listenstaine 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 Schengen, no que respeita à supressão dos controlos nas fronteiras internas e à circulação das pessoas (JO L 160 de 18.6.2011, p. 19).
([32]) Decisão 2004/512/CE do Conselho, de 8 de junho de 2004, que estabelece o Sistema de Informação sobre Vistos (VIS) (JO L 213 de 15.6.2004, p. 5).
([33]) Decisão 2008/633/JAI do Conselho, de 23 de junho de 2008, relativa ao acesso para consulta ao Sistema de Informação sobre Vistos (VIS) por parte das autoridades designadas dos Estados-Membros e por parte da Europol para efeitos de prevenção, deteção e investigação de infrações terroristas e outras infrações penais graves (JO L 218 de 13.8.2008, p. 129).
([34]) Regulamento (UE) 2019/818 do Parlamento Europeu e do Conselho, de 20 de maio de 2019, relativo à criação de um regime de interoperabilidade entre os sistemas de informação da UE no domínio da cooperação policial e judiciária, asilo e migração e que altera os Regulamentos (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816 (ver página 85 do presente Jornal Oficial).

2. O regime inclui os seguintes componentes de interoperabilidade:

a) Um portal europeu de pesquisa (ESP);

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

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

d) Um detetor de identidades múltiplas (MID).

3. O presente regulamento inclui também disposições sobre os requisitos de qualidade dos dados, um formato de mensagem universal (UMF), um repositório central para a elaboração de relatórios e estatísticas (CRRS), e 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, ao desenvolvimento e ao funcionamento dos componentes de interoperabilidade.

4. O presente regulamento adapta igualmente os procedimentos e condições que regem o acesso das autoridades designadas e da Agência da União Europeia para a Cooperação Policial (Europol) ao SES, ao VIS, ao ETIAS e ao Eurodac para fins de prevenção, deteção ou investigação de infrações terroristas ou de outras infrações penais graves.

5. O presente regulamento estabelece igualmente um regime de verificação da identidade e da identificação de pessoas.

Artigo 2.º

Objetivos

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

a) Melhorar a eficácia e a eficiência dos controlos de fronteira nas fronteiras externas;

b) Contribuir para a prevenção e o combate à imigração ilegal;

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, salvaguardando a segurança nos territórios dos Estados-Membros;

d) Melhorar a aplicação da política comum de vistos;

e) Auxiliar na análise dos pedidos de proteção internacional;

f) Contribuir para a prevenção, deteção e investigação de infrações terroristas e outras infrações penais graves;

g) Facilitar a identificação de pessoas desconhecidas que não são capazes de se identificar ou de restos mortais humanos não identificados em caso de catástrofes naturais, acidentes ou ataques terroristas.

2. Os objetivos referidos no n.º 1 devem ser alcançados mediante:

a) A garantia de correta identificação das pessoas;

b) O contributo para combater a fraude de identidade;

c) A melhoria da qualidade dos dados e uma harmonização dos requisitos de qualidade dos dados armazenados nos sistemas de informação da UE, respeitando simultaneamente os requisitos previstos nos atos jurídicos que regem o tratamento de dados dos sistemas individuais, bem como as normas e os princípios em matéria de proteção de dados;

d) A facilitação da aplicação, por parte dos Estados-Membros, dos aspetos técnicos e operacionais dos sistemas de informação da UE e o apoio a essa aplicação;

e) O reforço, a simplificação e a maior uniformidade das condições de segurança e de proteção dos dados que regem os respetivos sistemas de informação da UE, sem prejuízo da proteção especial e das salvaguardas concedidas a determinadas categorias de dados;

f) A racionalização das condições de acesso das autoridades designadas ao SES, VIS, ETIAS e Eurodac, assegurando simultaneamente as condições necessárias e proporcionadas para esse acesso;

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

Artigo 3.º

Âmbito de aplicação

1. O presente regulamento aplica-se ao SES, ao VIS, ao ETIAS e ao 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 do presente artigo e cujos dados sejam recolhidos para os fins definidos nos artigos 1.º e 2.º do Regulamento (CE) n.º 767/2008, no artigo 1.º do Regulamento (UE) 2017/2226, nos artigos 1.º e 4.º do Regulamento (UE) 2018/1240, no artigo 1.º do Regulamento (UE) n.º 2018/1860 e no artigo 1.º do Regulamento (UE) 2018/1861.

Artigo 4.º

Definições

Para efeitos do presente regulamento, entende-se por:

1) «Fronteiras externas», as fronteiras externas, na aceção do artigo 2.º, ponto 2, do Regulamento (UE) 2016/399;

2) «Controlos de fronteira», os controlos de fronteira, na aceção do artigo 2.º, ponto 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 a que se refere o artigo 51.º, n.º 1, do Regulamento (UE) 2016/679 e a autoridade de controlo a que se refere o artigo 41.º, n.º 1, da Diretiva (UE) 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) «Dados alfanuméricos», os dados representados por letras, dígitos, carateres especiais, espaços e sinais de pontuação;

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

9) «Dados dactiloscópicos», imagens das impressões digitais e das impressões digitais latentes que, devido ao seu caráter único e aos pontos de referência que contêm, permitem comparações rigorosas e fiáveis sobre a identidade de uma pessoa;

10) «Imagem facial», a imagem digitalizada do rosto de uma pessoa;

11) «Dados biométricos», os dados dactiloscópicos e a imagem facial ou ambos;

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

13) «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;

14) «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;

15) «Sistemas de informação da EU», o SES, o VIS, o ETIAS, o Eurodac, o SIS e o ECRIS-TCN;

16) «Dados da Europol», os dados pessoais tratados pela Europol para os fins previstos no artigo 18.º, n.º 2, alíneas a), b) e c), do Regulamento (UE) 2016/794;

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

18 «Correspondência», existência de uma correspondência em resultado de uma comparação automatizada de dados pessoais registados, ou a ser registados, num sistema de informação ou numa base de dados;

19) «Autoridade policial», uma «autoridade competente», na aceção do artigo 3.º, ponto 7, da Diretiva (UE) 2016/680;

20) «Autoridades designadas», as autoridades designadas dos Estados-Membros na aceção do artigo 3.º, n.º 1, ponto 26, do Regulamento (UE) 2017/2226, do artigo 2.º, n.º 1, alínea e), da Decisão 2008/633/JAI e do artigo 3.º, n.º 1, ponto 21, do Regulamento (UE) 2018/1240;

21) «Infração terrorista», uma infração prevista na legislação nacional que corresponda ou seja equivalente a uma das infrações referidas na Diretiva (UE) 2017/541 do Parlamento Europeu e do Conselho ([35]);

22) «Infração penal grave», uma infração que corresponda ou seja equivalente a uma das infrações referidas no artigo 2.º, n.º 2, da Decisão-Quadro 2002/584/JAI do Conselho ([36]), 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;

23) «Sistema de Entrada/Saída» ou «SES», o Sistema de Entrada/Saída criado pelo Regulamento (UE) 2017/2226;

24) «Sistema de Informação sobre Vistos» ou «VIS», o Sistema de Informação sobre Vistos criado pelo Regulamento (CE) n.º 767/2008;

25) «Sistema Europeu de Informação e Autorização de Viagem» ou «ETIAS», o Sistema Europeu de Informação e Autorização de Viagem criado pelo Regulamento (UE) 2018/1240;

26) «Eurodac», Eurodac, criado pelo Regulamento (UE) n.º 603/2013 do Parlamento Europeu e do Conselho ([37]);

27) «Sistema de Informação Schengen» ou «SIS», o Sistema de Informação Schengen criado pelos Regulamentos (UE) 2018/1860, (UE) 2018/1861 e (UE) 2018/1862;

28) «ECRIS-TCN», o sistema centralizado de identificação de Estados-Membros que possui informações sobre condenações de nacionais de países terceiros e de apátridas, criado pelo Regulamento (UE) 2019/816 do Parlamento Europeu e do Conselho ([38]).

Artigo 5.º

Não discriminação e direitos fundamentais

O tratamento de dados pessoais para efeitos do presente regulamento não pode originar discriminação de pessoas em razão do género, da raça, da cor, da origem étnica ou social, das características genéticas, da língua, da religião ou crença, das opiniões políticas ou de outra natureza, da pertença a uma minoria nacional, do património, do nascimento, da deficiência, da idade ou da orientação sexual. O respeito pela dignidade e integridade humanas e pelos direitos fundamentais, incluindo o direito ao respeito pela vida privada e à proteção dos dados pessoais, deve ser integralmente assegurado. Deve ser dispensada especial atenção às crianças, aos idosos, às pessoas com deficiência e às pessoas com necessidade de proteção internacional. O interesse superior da criança deve ser uma consideração primordial.

CAPÍTULO II

Portal europeu de pesquisa

Artigo 6.º

Portal europeu de pesquisa

1. É criado um portal europeu de pesquisa (ESP) para facilitar o acesso rápido, contínuo, eficiente, sistemático e controlado das autoridades dos Estados-Membros e das agências da União aos sistemas de informação da UE, aos dados da Europol e às bases de dados da Interpol para o desempenho das suas funções e em conformidade com os respetivos direitos de acesso ao SES, ao VIS, ao ETIAS, ao Eurodac, ao SIS e ao ECRIS-TCN e com os objetivos e finalidades dos mesmos.

([35]) Diretiva (UE) 2017/541 do Parlamento Europeu e do Conselho, de 15 de março de 2017, relativa à luta contra o terrorismo e que substitui a Decisão-Quadro 2002/475/JAI do Conselho e altera a Decisão 2005/671/JAI do Conselho (JO L 88 de 31.3.2017, p. 6).

([36]) Decisão-Quadro 2002/584/JAI do Conselho, de 13 de junho de 2002, relativa ao mandado de detenção europeu e aos processos de entrega entre os Estados-Membros (JO L 190 de 18.7.2002, p. 1).

([37]) Regulamento (UE) n.º 603/2013 do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativo à criação do sistema «Eurodac» de comparação de impressões digitais para efeitos da aplicação efetiva do Regulamento (UE) n.º 604/2013, que estabelece os critérios e mecanismos de determinação do Estado-Membro responsável pela análise de um pedido de proteção internacional apresentado num dos Estados-Membros por um nacional de um país terceiro ou um apátrida, e de pedidos de comparação com os dados Eurodac apresentados pelas autoridades responsáveis dos Estados-Membros e pela Europol para fins de aplicação da lei e que altera o Regulamento (UE) n.º 1077/2011 que cria uma Agência europeia para a gestão operacional de sistemas informáticos de grande escala no espaço de liberdade, segurança e justiça (JO L 180 de 29.6.2013, p. 1).

([38]) Regulamento (UE) 2019/816 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, que cria um sistema centralizado para a determinação dos Estados-Membros que possuem informações sobre condenações de nacionais de países terceiros e de apátridas tendo em vista completar e apoiar o Sistema Europeu de Informação sobre Registos Criminais (sistema ECRIS-TCN) e que altera o Regulamento (UE) 2018/1726 (ver página 1 do presente Jornal Oficial).

2. O ESP é composto por:

a) Uma infraestrutura central, incluindo 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 as agências da União que têm o direito de utilizar o ESP;

c) Uma infraestrutura de comunicação segura entre o ESP e o SES, o VIS, o ETIAS, o Eurodac, o SIS Central, o ECRIS-TCN, os dados da Europol e as bases de dados da Interpol, bem como entre o ESP e as infraestruturas centrais do CIR e do MID.

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 às agências da União que dispõem de acesso a, pelo menos, um dos sistemas de informação da UE, de acordo com os atos jurídicos que regem esses sistemas de informação da UE, ao CIR, ao MID, de acordo com o presente regulamento, aos dados da Europol de acordo com o Regulamento (UE) 2016/794 ou às bases de dados da Interpol de acordo com o direito da União ou direito nacional aplicável ao referido acesso.

As referidas autoridades dos Estados-Membros e agências da União podem utilizar o ESP e os dados por ele fornecidos unicamente para os objetivos e finalidades previstos nos atos jurídicos que regem esses sistemas de informação da UE, no Regulamento (UE) 2016/794 e no presente regulamento.

2. As autoridades dos Estados-Membros e as agências da União 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, como referido nos atos jurídicos que regem esses sistemas de informação da UE e no direito nacional. Essas autoridades e agências 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 nos Regulamentos (UE) 2018/1860 e (UE) 2018/1861.

4. Quando previsto pelo direito da União, as agências da União a que se refere o n.º 1 devem utilizar o ESP para pesquisar dados relativos a pessoas ou aos seus documentos de viagem no SIS Central.

5. As autoridades dos Estados-Membros e as agências da União referidas no n.º 1 podem utilizar o ESP para pesquisar dados relativos a pessoas ou aos seus documentos de viagem nos dados da Europol, 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, em cooperação com os Estados-Membros, um perfil baseado na categoria de utilizador do ESP e nas finalidades das consultas, em conformidade com os pormenores técnicos e os direitos de acesso a que se refere o n.º 2. Cada perfil deve incluir, nos termos do direito da União e do direito nacional, a seguinte informação

a) Os campos de dados a utilizar 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;

c) Os dados específicos contidos nos sistemas de informação da UE, os dados da Europol e as bases de dados da Interpol que podem ser consultados;

d) As categorias de dados que podem ser fornecidos em cada resposta.

2. A Comissão deve adotar atos de execução, a fim de especificar os pormenores técnicos dos perfis referidos no n.º 1, em conformidade com os respetivos direitos de acesso dos utilizadores ESP, conforme previsto nos atos jurídicos que regem os sistemas de informação da UE e de acordo com o direito nacional. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 74.º, n.º 2.

3. Os perfis referidos no n.º 1 devem ser revistos periodicamente pela eu-LISA, em cooperação com os Estados-Membros, pelo menos uma vez por ano e, se necessário, atualizados.

Artigo 9.º

Consultas

1. Os utilizadores do ESP iniciam uma consulta introduzindo dados alfanuméricos ou biométricos no ESP. Ao iniciar-se uma consulta, o ESP consulta o SES, o ETIAS, o VIS, o SIS, o Eurodac, o ECRIS-TCN e o CIR, os dados da Europol e as bases de dados da Interpol, utilizando simultaneamente os dados introduzidos pelo utilizador do ESP e de acordo com o perfil do utilizador.

2. As categorias de dados utilizados para iniciar uma consulta através do ESP correspondem às categorias 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 atos jurídicos que lhes são aplicáveis.

3. A eu-LISA deve desenvolver, em cooperação com os Estados-Membros, um documento de controlo das interfaces para o ESP baseado no UMF referido no artigo 38.º.

4. Em resposta a uma consulta de um utilizador do ESP, o SES, o ETIAS, o VIS, o SIS, o Eurodac, o ECRIS-TCN, o CIR e o MID, os dados da Europol e as bases de dados da Interpol, devem responder à consulta, fornecendo os dados em sua posse.

Sem prejuízo do disposto no artigo 20.º, a resposta do ESP deve indicar qual o sistema de informação ou base de dados da UE a que os dados pertencem.

O ESP não fornece informações relativas aos dados dos sistemas de informação da UE, aos dados da Europol nem às bases de dados da Interpol aos quais o utilizador não tem acesso nos termos do direito da União e do direito nacional aplicáveis.

5. As consultas das bases de dados da Interpol lançadas através do ESP devem ser efetuadas de molde a não revelar qualquer informação ao proprietário do alerta da Interpol.

6. O ESP deve fornecer respostas ao utilizador assim que os dados de um dos sistemas de informação da UE, os dados da Europol ou as bases de dados da Interpol estiverem disponíveis. Essas respostas devem conter apenas os dados aos quais o utilizador tem acesso ao abrigo do direito da União e do direito nacional.

7. A Comissão deve adotar um ato de execução para especificar o procedimento técnico para as consultas do ESP nos sistemas de informação da UE, nos dados da Europol e nas bases de dados da Interpol e o formato das respostas do ESP. O referido ato de execução é adotado pelo procedimento de exame a que se refere o artigo 74.º, n.º 2.

Artigo 10.º

Manutenção de registos

1. Sem prejuízo do disposto no artigo 46.º do Regulamento (UE) 2017/2226, no artigo 34.º do Regulamento (CE) n.º 767/2008, no artigo 69.º do Regulamento (UE) 2018/1240 e nos artigos 12.º e 18.º do Regulamento (UE) 2018/1861, a eu-LISA deve conservar registos de todas as operações de tratamento de dados realizadas no ESP. Esses registos devem incluir o seguinte:

a) O Estado-Membro ou a agência da União que lança a consulta e o perfil de ESP utilizado;

b) A data e a hora da consulta;

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

2. Cada Estado-Membro deve manter registos das consultas feitas pelas suas autoridades e pelo pessoal devidamente autorizado dessas autoridades a utilizar o ESP. Cada agência da União deve manter registos das consultas feitas pelo seu pessoal devidamente autorizado a utilizar o ESP.

3. Os registos referidos nos n.os 1 e 2 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 e a integridade dos dados. Esses registos devem estar protegidos por medidas adequadas contra o acesso não autorizado e apagados um ano após a sua criação. Se, no entanto, forem necessários para procedimentos de controlo que já tenham sido iniciados, devem, nesse caso, ser apagados logo que deixarem de ser necessários para o efeito.

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 ou o CIR, devido a uma falha do ESP, os utilizadores do ESP devem ser notificados pela eu-LISA de forma automatizada.

2. No caso de impossibilidade técnica de utilizar o ESP para consultar um ou vários sistemas de informação da UE ou o CIR, devido a uma falha da infraestrutura nacional de um Estado-Membro, esse Estado-Membro deve notificar a eu-LISA e a Comissão de forma automatizada.

3. Nos casos referidos nos n.os 1 ou 2, do presente artigo, e até que a falha técnica seja resolvida, a obrigação referida no artigo 7.º, n.os 2 e 4, não se aplica e os Estados-Membros devem aceder aos sistemas de informação da UE ou ao CIR diretamente, caso o direito da União ou o direito nacional o preveja.

4. Em caso de impossibilidade técnica de utilizar o ESP para consultar um ou vários sistemas de informação da UE ou o CIR, devido a uma falha da infraestrutura de uma agência da União, a agência em causa notifica a eu-LISA e a Comissão de forma automatizada.

CAPÍTULO III

Serviço partilhado de correspondências biométricas

Artigo 12.º

Serviço partilhado de correspondências biométricas

1. É criado um serviço partilhado de correspondências biométricas (serviço partilhado BMS) onde são armazenados modelos biométricos obtidos com base nos dados biométricos referidos no artigo 13.º armazenados no CIR e no SIS, e que permite consultar vários sistemas de informação da UE usando dados biométricos, para efeitos de apoio do CIR e do MID e dos objetivos do SES, do VIS, do Eurodac, do SIS e do ECRIS-TCN.

2. O serviço partilhado BMS é composto por:

a) Uma infraestrutura central que substitui os sistemas centrais, respetivamente, do SES, do VIS, do SIS, do Eurodac e do ECRIS-TCN, na medida em que armazena modelos biométricos e permite buscas de dados biométricos;

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

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

Artigo 13.º

Armazenamento de modelos biométricos no serviço partilhado de correspondências biométricas

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

a) Os dados referidos no artigo 16.º, n.º 1, alínea d), no artigo 17.º, n.º 1, alíneas b) e c), e no artigo 18.º, n.º 2, alíneas a), b) e c), do Regulamento (UE) 2017/2226;

b) Os dados referidos no artigo 9.º, ponto 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 (UE) 2018/1861, à exceção dos dados relativos a impressões palmares;

d) Os dados referidos no artigo 4.º, n.º 1, alíneas u) e v), do Regulamento (UE) 2018/1860, à exceção dos dados relativos a impressões palmares.

Os modelos biométricos são armazenados no serviço partilhado BMS, separados de forma lógica de acordo com o sistema de informação de onde provêm os dados.

2. Para cada conjunto de dados a que se refere o n.º 1, o serviço partilhado BMS inclui em cada modelo biométrico uma referência aos sistemas de informação da UE onde estão armazenados os dados biométricos correspondentes e uma referência aos registos efetivos nesses sistemas de informação da UE.

3. Os modelos biométricos são introduzidos no serviço partilhado BMS somente após um controlo automatizado da qualidade dos dados biométricos adicionados a um dos sistemas de informação da UE. Esse controlo é efetuado pelo serviço partilhado 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.

5. A Comissão deve estabelecer, por meio de um ato de execução, requisitos de desempenho e disposições práticas para monitorizar o desempenho do serviço partilhado BMS, a fim de assegurar que a eficácia das pesquisas biométricas respeite os procedimentos urgentes, como os controlos nas fronteiras e as identificações. O referido ato de execução é adotado pelo procedimento de exame a que se refere o artigo 74.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 serviço partilhado BMS. As consultas com dados biométricos devem ser efetuadas em conformidade com os fins previstos no presente regulamento e nos Regulamentos (CE) n.º 767/2008, (UE) 2017/2226, (UE) 2018/1860, (UE) 2018/1861, (UE) 2018/1862 e no (UE) 2019/816.

Artigo 15.º

Conservação de dados no serviço partilhado de correspondências biométricas

Os dados referidos no artigo 13.º, n.ºs 1 e 2, devem ser conservados no serviço partilhado BMS unicamente enquanto os dados biométricos correspondentes estiverem armazenados no CIR ou no SIS. Os dados devem ser apagados do serviço partilhado BMS de forma automatizada.

Artigo 16.º

Manutenção de registos

1. Sem prejuízo do disposto no artigo 46.º do Regulamento (UE) 2017/2226, no artigo 34.º do Regulamento (CE) n.º 767/2008 e nos artigos 12.º e 18.º do Regulamento (UE) 2018/1861, a eu-LISA deve conservar registos de todas as operações de tratamento de dados realizadas no serviço partilhado BMS. Esses registos devem incluir o seguinte:

a) O Estado-Membro ou a agência da União que inicia a consulta;

b) O histórico da criação e do armazenamento de modelos biométricos;

c) Os sistemas de informação da UE consultados utilizando os modelos biométricos armazenados no serviço partilhado BMS;

d) A data e a hora da consulta;

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

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

2. Cada Estado-Membro deve manter registos das consultas feitas pelas suas autoridades e pelo pessoal devidamente autorizado dessas autoridades a utilizar o serviço partilhado BMS. Cada agência da União deve manter registos das consultas feitas pelo seu pessoal devidamente autorizado a utilizar o serviço partilhado BMS.

3. Os registos referidos no n.º 1 e no n.º 2 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 e a integridade dos dados. Esses registos devem estar protegidos por medidas adequadas contra acesso não autorizado e ser apagados um ano após a sua criação. No entanto, caso sejam necessários para procedimentos de controlo que já se tenham sido iniciados, devem ser apagados logo que deixarem de ser necessários para esse efeito.

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 ECRIS-TCN e contém 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 ECRIS-TCN nos termos do artigo 20.º, de apoiar o funcionamento do MID nos termos do artigo 21.º e de facilitar e simplificar o acesso das autoridades designadas e da Europol ao SES, ao VIS, ao ETIAS e ao Eurodac, sempre que tal for necessário para efeitos de prevenção, deteção ou investigação de infrações terroristas ou outras infrações penais graves nos termos do artigo 22.º.

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 ECRIS-TCN na medida em que armazena os dados referidos no artigo 18.º;

b) Um canal de comunicação seguro entre o CIR, os Estados-Membros e as agências da União que têm o direito de utilizar o CIR nos termos do direito da União e do direito nacional;

c) Uma infraestrutura de comunicação segura entre o CIR e o SES, o VIS, o ETIAS, o Eurodac e o ECRIS-TCN, bem como com as infraestruturas centrais do ESP, do serviço partilhado BMS e do MID.

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

4. Caso seja tecnicamente impossível consultar o CIR, devido a uma falha do CIR, para efeitos de identificação de uma pessoa nos termos do artigo 20.º, de deteção de identidades múltiplas nos termos do artigo 21.º ou de prevenção, deteção ou investigação de infrações terroristas ou outras infrações penais graves nos termos do artigo 22.º, os utilizadores do CIR devem ser notificados pela eu-LISA de forma automatizada.

5. A eu-LISA deve, em cooperação com os Estados-Membros, desenvolver para o CIR um documento de controlo das interfaces baseado no UMF referido no artigo 38.º.

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), no artigo 17.º, n.º 1, alíneas a), b) e c), e no artigo 18.º, n.ºs 1 e 2, do Regulamento (UE) 2017/2226;

b) Os dados referidos no artigo 9.º, ponto 4, alíneas a), a c) e artigo 9.º, pontos 5 e 6 do Regulamento (CE) n.º 767/2008;

c) Os dados referidos no artigo 17.º, n.º 2, alíneas a), a e) do Regulamento (UE) 2018/1240;

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

3. As autoridades que acedem ao CIR devem fazê-lo em conformidade com os seus direitos de acesso, tal como referidos nos atos jurídicos que regem os sistemas de informação da UE e no direito nacional e em conformidade com os seus direitos de acesso nos termos do presente regulamento para os efeitos referidos nos artigos 20.º, 21.º e 22.º.

4. Para cada série de dados a que se refere o n.º 1, o CIR deve incluir uma referência ao registo efetivo nos sistemas de informação da UE a que os dados pertencem.

5. 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 ou 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. Caso seja criada uma ligação branca ou vermelha no MID nos termos dos artigos 32.º ou 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. As consultas do CIR devem ser realizadas por uma autoridade policial, nos termos dos n.ºs 2 e 5, apenas nas seguintes circunstâncias:

a) Caso uma autoridade policial não consiga identificar uma pessoa, devido à falta de um documento de viagem ou de outro documento credível que comprove a identidade dessa pessoa;

b) Em caso de dúvidas sobre os dados de identificação fornecidos por uma pessoa;

c) Em caso de dúvidas sobre a autenticidade do documento de viagem ou de outro documento credível fornecido por uma pessoa;

d) Em caso de dúvidas sobre a identidade do titular de um documento de viagem ou de outro documento credível; ou

e) Caso a pessoa não possa ou se recuse a cooperar.

Essas consultas não são autorizadas quando se trate de menores de 12 anos, salvo se forem feitas no superior interesse da criança.

2. Sempre que se verifique uma das circunstâncias previstas no n.º 1 e uma autoridade policial tenha sido habilitada para o efeito por medidas legislativas nacionais, tal como referido no n.º 5, pode, exclusivamente para efeitos de identificação de uma pessoa, consultar o CIR usando os dados biométricos dessa pessoa que foram obtidos em tempo real durante um controlo de identidade, desde que o procedimento tenha sido iniciado na presença dessa pessoa.

3. Sempre que a consulta indicar que os dados relativos a essa pessoa estão armazenados no CIR, a autoridade policial 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.

4. Sempre que uma autoridade policial tenha sido habilitada para o efeito por medidas legislativas nacionais, a que se refere o n.º 6, pode, em caso de catástrofe natural, de acidente ou de um atentado terrorista, e exclusivamente para efeitos de identificação de pessoas desconhecidas que não sejam capazes de se identificar ou de restos mortais humanos não identificados, consultar o CIR, usando os dados biométricos dessas pessoas.

5. Os Estados-Membros que pretendam usar a possibilidade prevista no n.º 2 devem adotar medidas legislativas nacionais. Ao fazê-lo, os Estados-Membros devem ter em conta a necessidade de evitar qualquer discriminação contra nacionais de países terceiros. Essas medidas legislativas devem especificar exatamente os objetivos da identificação referidos no artigo 2.º, n.º 1, alíneas b) e c), designar as autoridades policiais competentes e estabelecer os procedimentos, as condições e os critérios desses controlos de identidade.

6. Os Estados-Membros que pretendam aplicar o n.º 4 devem adotar medidas legislativas nacionais que estabeleçam os procedimentos, as condições e os critérios para o efeito.

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, nos termos do artigo 28.º, n.º 4, a autoridade responsável pela verificação manual das diferentes identidades, nos termos do artigo 29.º, deve ter acesso, unicamente para efeitos dessa verificação, aos dados referidos no artigo 18.º, n.ºs 1 e 2, armazenados no CIR associados a uma ligação amarela.

2. Sempre que uma consulta do CIR se traduzir numa ligação vermelha, nos termos do 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 referidos no artigo 18.º, n.ºs 1 e 2, armazenados no CIR associados a uma ligação vermelha.

Artigo 22.º

Consulta do repositório comum de dados de identificação para efeitos de prevenção, deteção ou investigação de infrações terroristas ou outras infrações penais graves

1. Num caso específico, sempre que existam motivos razoáveis para crer que a consulta dos sistemas de informação da UE contribuirá para a prevenção, deteção ou investigação de infrações terroristas ou outras infrações penais graves, nomeadamente caso haja indícios de que o suspeito, autor ou vítima de uma infração terrorista ou de outras infrações penais graves é uma pessoa cujos dados estão armazenados no SES, no VIS ou no ETIAS, as autoridades designadas e a Europol podem consultar o CIR para obter informações sobre se existem dados sobre uma determinada pessoa no SES, no VIS ou no ETIAS.

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

A resposta com a indicação da existência de dados relativos a essa pessoa em qualquer um dos sistemas de informação da UE referidos no n.º 1 só pode ser utilizada para efeitos de apresentação de um pedido de acesso pleno, no respeito das condições e dos procedimentos definidos nos atos jurídicos que regem esse acesso.

Em caso de correspondência ou de correspondências múltiplas, a autoridade designada ou a Europol devem solicitar um acesso pleno a, pelo menos, um dos sistemas de informação para os quais foi gerada uma correspondência.

No caso excecional, de não ser solicitado esse acesso pleno, as autoridades designadas devem registar a justificação fornecida para não efetuar o pedido, a qual deve ser rastreável até ao processo nacional. A Europol deve registá-la no processo correspondente.

3. O pleno acesso aos dados contidos no SES, no VIS ou no ETIAS para efeitos de prevenção, deteção ou investigação de infrações terroristas ou outras infrações penais graves continua sujeito às condições e procedimentos estabelecidos nos atos jurídicos que regem esse acesso.

Artigo 23.º

Conservação de dados no repositório comum de dados de identificação

1. Os dados referidos no artigo 18.º, n.ºs 1, 2 e 4 devem ser eliminados do CIR de forma automatizada em conformidade com as disposições em matéria de conservação de dados do Regulamento (UE) 2017/2226, do Regulamento (CE) n.º 767/2008 e do Regulamento (UE) 2018/1240, respetivamente.

2. O processo individual deve permanecer armazenado no CIR apenas enquanto os dados correspondentes permanecerem armazenados em, pelo menos, um dos sistemas de informação da UE 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 (UE) 2017/2226, no artigo 34.º do Regulamento (CE) n.º 767/2008 e no artigo 69.º do Regulamento (UE) 2018/1240, a eu-LISA deve conservar registos de todas as operações de tratamento de dados realizadas no CIR nos termos dos n.os 2, 3 e 4 do presente artigo.

2. A eu-LISA deve conservar, nos termos do artigo 20.º, registos de todas as operações de tratamento de dados realizadas no CIR. Esses registos devem incluir o seguinte:

a) O Estado-Membro ou a agência da União que inicia a consulta;

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

c) A data e a hora da consulta;

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

e) Os resultados da consulta.

3. A eu-LISA deve conservar, nos termos do artigo 21.º, registos de todas as operações de tratamento de dados realizadas no CIR Esses registos devem incluir o seguinte:

a) O Estado-Membro ou a agência da União que inicia a consulta;

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

c) A data e a hora da consulta;

d) Caso seja criada uma ligação, os dados utilizados para iniciar a consulta e os resultados da consulta com indicação do sistema de informação da UE do qual os dados foram recebidos.

4. A eu-LISA deve conservar registos, nos termos do artigo 22.º, de todas as operações de tratamento de dados realizadas no CIR. Esses registos devem incluir o seguinte:

a) A data e a hora da consulta;

b) Os dados utilizados para iniciar a consulta;

c) Os resultados da consulta;

d) O Estado-Membro ou a agência da União que consulta o CIR;

Os registos desse acesso devem ser verificados periodicamente pela autoridade de controlo competente nos termos do artigo 41.º da Diretiva (UE) 2016/680 ou pela Autoridade Europeia para a Proteção de Dados nos termos do artigo 43.º do Regulamento (UE) 2016/794, a intervalos não superiores a seis meses, a fim de verificar se os procedimentos e condições estabelecidos no artigo 22.º, n.º 1 e n.º 2 do presente regulamento são cumpridos.

5. Cada Estado-Membro deve manter registos das consultas efetuadas pelas suas autoridades e pelo pessoal devidamente autorizado dessas autoridades a utilizar o CIR, nos termos dos artigos 20.º, 21.º e 22.º. Cada agência da União deve manter registos das consultas feitas pelo seu pessoal devidamente autorizado a utilizar o CIR, nos termos dos artigos 21.º e 22.º.

Além disso, para qualquer acesso ao CIR nos termos do artigo 22.º, cada Estado-Membro deve conservar os seguintes registos:

a) A referência do processo nacional;

b) A finalidade do acesso;

c) Nos termos das regras nacionais, a identificação de utilizador único do funcionário que efetuou a consulta e do funcionário que ordenou a consulta.

6. Em conformidade com o Regulamento (UE) 2016/794, para qualquer acesso ao CIR nos termos do artigo 22.º do presente regulamento, a Europol deve conservar registos da identificação de utilizador único do funcionário que efetuou a consulta e do funcionário que a ordenou.

7 Os registos referidos nos n.os 2 a 6 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 e a integridade dos dados. Esses registos devem estar protegidos por medidas adequadas contra acesso não autorizado e ser apagados um ano após a sua criação. No entanto, se forem necessários para procedimentos de controlo que já tenham sido iniciados, devem ser apagados logo que deixarem de ser necessários para o efeito.

8. A eu-LISA deve armazenar os registos relacionados com o histórico dos dados nos processos individuais. A eu-LISA deve apagar esses registos de forma automatizada, 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 processo de confirmação de identidade, tal como referido no artigo 34.º, contendo ligações entre os dados nos sistemas de informação da UE que fazem parte do CIR e do SIS e que permite detetar 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 ECRIS-TCN.

2. O MID é composto por:

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

b) Uma infraestrutura de comunicação segura para ligar o MID ao SIS e as infraestruturas centrais do ESP 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 das diferentes identidades a que se refere o artigo 29.º, deve ser concedido acesso aos dados referidos no artigo 34.º armazenados no MID às seguintes entidades:

a) Autoridades competentes designadas nos termos do artigo 9.º, n.º 2, do Regulamento (UE) 2017/2226, aquando da criação ou atualização de um processo individual no SES em conformidade com o artigo 14.º desse Regulamento;

b) Autoridades responsáveis pelos vistos a que se refere o artigo 6.º, do Regulamento (CE) n.º 767/2008 ao criar ou atualizar um processo de requerimento de visto no VIS, em conformidade com esse Regulamento;

c) A unidade central do ETIAS e as unidades nacionais do ETIAS durante a realização do procedimento previsto nos artigos 22.º e 26.º do Regulamento (UE) 2018/1240;

d) Gabinete SIRENE do Estado-Membro que criar ou atualizar uma indicação SIS em conformidade com os Regulamentos (UE) 2018/1860 e (UE) 2018/1861.

2. As autoridades dos Estados-Membros e as agências da União que tenham acesso a, pelo menos, um sistema de informação da UE incluído no CIR 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.

3. As autoridades dos Estados-Membros e as agências da União devem ter acesso às ligações brancas a que se refere o artigo 33.º, caso tenham acesso aos dois sistemas de informação da UE que contêm dados entre os quais a ligação branca foi criada.

4. As autoridades dos Estados-Membros e as agências da União devem ter acesso às ligações verdes a que se refere o artigo 31.º, caso tenham acesso aos dois sistemas de informação da UE que contêm dados entre os quais a ligação verde foi criada e uma consulta a esses sistemas de informação tenha revelado uma correspondência com os dois conjuntos de dados ligados.

Artigo 27.º

Deteção de identidades múltiplas

1. Deve ser iniciada uma deteção de identidades múltiplas no CIR e no SIS se:

a) For criado ou atualizado um processo individual no SES, em conformidade com o artigo 14.º do Regulamento (UE) 2017/2226;

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

c) For criado ou atualizado um processo de pedido no ETIAS, em conformidade com o artigo 19.º do Regulamento (UE) 2018/1240;

d) For criada ou atualizada uma indicação sobre uma pessoa no SIS em conformidade com o artigo 3.º do Regulamento (UE) 2018/1860 e o capítulo V do Regulamento (UE) 2018/1861.

2. Se os dados contidos num sistema de informação da UE a que se refere o n.º 1 contiverem dados biométricos, o CIR e o SIS Central devem utilizar o serviço partilhado BMS a fim de realizar a deteção de identidades múltiplas. O serviço partilhado BMS deve comparar os modelos biométricos obtidos a partir de quaisquer novos dados biométricos com os modelos biométricos já constantes do serviço partilhado BMS para verificar se os dados pertencentes à mesma pessoa se encontram 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 ESP para pesquisar os dados armazenados no SIS Central e no CIR utilizando, respetivamente, os seguintes dados:

a) Apelido; nomes próprios; data de nascimento; local de nascimento; nacionalidade ou nacionalidades; e género; conforme referido no artigo 16.º, n.º 1, alínea a), no artigo 17.º, n.º 1, e no artigo 18.º, n.º 1, do Regulamento (UE) 2017/2226;

b) Apelido; nomes próprios; data de nascimento; sexo; local e país de nascimento; nacionalidades; conforme referido no artigo 9.º, ponto 4, alínea a) e a-A), do Regulamento (CE) n.º 767/2008;

c) Apelido, nomes próprios, apelido de nascimento, pseudónimos, data de nascimento, local de nascimento, género e nacionalidade ou nacionalidades atuais; a que se refere o artigo 17.º, n.º 2, do Regulamento (UE) 2018/1240;

d) Apelidos, nomes próprios, nomes de nascimento, nomes e pseudónimos utilizados anteriormente, local de nascimento, data de nascimento, género e nacionalidade ou nacionalidades eventuais, a que se refere o artigo 20.º, n.º 2, do Regulamento (UE) 2018/1861;

e) Apelidos, nomes próprios, nomes de nascimento, nomes e pseudónimos utilizados anteriormente, local de nascimento, data de nascimento, género e nacionalidade ou nacionalidades eventuais, a que se refere o artigo 4.º do Regulamento (UE) 2018/1860;

4. Para além do processo a que se referem os n.ºs 2 e 3, o CIR e o SIS Central devem utilizar o ESP para pesquisar os dados armazenados no SIS Central e no CIR, respetivamente, utilizando dados do documento de viagem.

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

Artigo 28.º

Resultados da deteção de identidades múltiplas

1. Nos casos em que as consultas referidas no artigo 27.º, n.ºs 2, 3 e 4, não indicarem qualquer correspondência, os procedimentos a que se refere o artigo 27.º, n.º 1, devem de acordo com os atos jurídicos que os regem.

2. Se a pesquisa referida no artigo 27.º, n.ºs 2, 3 e 4, indicar uma ou várias correspondências, o CIR e, se for caso disso, o SIS devem criar uma ligação entre os dados utilizados para lançar a pesquisa e os dados que desencadearam a correspondência.

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

3. Se a pesquisa referida no artigo 27.º, n.ºs 2, 3 e 4, indicar uma ou várias correspondências e os dados de identificação dos ficheiros ligados forem os mesmos ou semelhantes, deve ser criada uma ligação branca em conformidade com o artigo 33.º.

4. Se a pesquisa referida no artigo 27.º, n.ºs 2, 3 e 4, detetar uma ou várias correspondências 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 aplica-se o procedimento previsto no artigo 29.º.

5. A Comissão deve adotar atos delegados nos termos do artigo 73.º, que estabelecem os procedimentos para determinar os casos em que dados de identificação e podem ser considerados os mesmos ou similares.

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

7. A Comissão deve, em cooperação com a eu-LISA, estabelecer as regras técnicas necessárias para criar ligações entre dados de diferentes sistemas de informação da UE através de atos de execução. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 74.º, n.º 2.

Artigo 29.º

Verificação manual das diferentes identidades e autoridades responsáveis

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

a) A autoridade competente designada nos termos do artigo 9.º, n.º 2, do Regulamento (UE) 2017/2226, no que respeita a correspondências que ocorreram aquando da criação ou atualização de um processo individual no SES em conformidade com esse regulamento;

b) Autoridades responsáveis pelos vistos a que se refere o artigo 6.º, n.º 1, do Regulamento (CE) n.º 767/2008, para correspondências que ocorreram aquando da criação ou atualização de um processo de requerimento de visto no VIS, em conformidade com esse regulamento

c) A unidade central do ETIAS e as unidades nacionais do ETIAS, para correspondências que ocorreram aquando da criação ou atualização de um processo de pedido em conformidade com o Regulamento (UE) 2018/1240;

d) O gabinete SIRENE do Estado-Membro, para correspondências que ocorreram aquando da criação ou atualização de uma indicação no SIS em conformidade com os Regulamentos (UE) 2018/1860 e (UE) 2018/1861.

O MID deve indicar a autoridade responsável pela verificação manual das diferentes identidades no processo de confirmação de identidade.

2. A autoridade responsável pela verificação manual das diferentes identidades 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 numa indicação relativa a:

a) Pessoas procuradas para efeitos de detenção, entrega ou extradição, tal como referido no artigo 26.º do Regulamento (UE) 2018/1862;

b) Pessoas desaparecidas ou vulneráveis, tal como referido no artigo 32.º do Regulamento (UE) 2018/1862;

c) Pessoas procuradas no âmbito de um processo judicial, tal como referido no artigo 34.º do Regulamento (UE) 2018/1862;

d) Pessoas para efeitos de vigilância discreta, controlo de verificação ou de controlo específico referido no artigo 36.º do Regulamento (UE) 2018/1862.

3. Sem prejuízo do disposto no n.º 4 do presente artigo, a autoridade responsável pela verificação manual das diferentes identidades deve ter acesso aos dados ligados contidos no processo de confirmação de identidade pertinente e aos dados de identificação ligados no CIR e, se for caso disso, no SIS. A referida autoridade deve avaliar as diversas identidades sem demora. Uma vez concluída essa avaliação, deve 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 manual das diferentes identidades no processo de confirmação de identidade for a autoridade competente designada nos termos do artigo 9.º, n.º 2, do Regulamento (UE) 2017/2226 que cria ou atualiza um processo individual no SES, em conformidade com o artigo 14.º desse regulamento, e quando é criada uma ligação amarela, essa autoridade deve realizar verificações adicionais. Exclusivamente para esse fim, essa autoridade deve ter acesso aos dados pertinentes contidos no processo de confirmação de identidade. Essa autoridade deve avaliar as diferentes identidades, atualizar a ligação nos termos dos artigos 31.º, 32.º e 33.º do presente regulamento e acrescentá-la ao processo de confirmação de identidade sem demora.

Essa verificação manual das diferentes identidades deve ser iniciada na presença da pessoa em causa, a quem deve ser oferecida a oportunidade de explicar as circunstâncias à autoridade responsável, que deve ter em conta essas explicações.

Caso a verificação manual das diferentes identidades tenha lugar na fronteira, deve ocorrer no prazo de 12 horas a contar da criação de uma ligação amarela nos termos do artigo 28.º, n.º 4, sempre que possível.

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

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

Artigo 30.º

Ligação amarela

1. Quando a verificação manual das diferentes identidades não tiver sido feita, deve ser classificada a amarelo uma ligação entre os dados de dois ou mais sistemas de informação da UE em qualquer dos seguintes casos:

a) Os dados ligados partilham os mesmos dados biométricos, mas têm dados de identificação similares ou diferentes;

b) Os dados ligados possuem dados de identificação diferentes, mas partilham os mesmos dados do documento de viagem e pelo menos um dos sistemas de informação da UE não dispõe de dados biométricos da pessoa em causa;

c) Os dados ligados partilham os mesmos dados de identificação, mas têm dados biométricos diferentes;

d) Os dados ligados têm dados de identificação similares ou diferentes e partilham os mesmos dados do documento de viagem, mas têm dados biométricos diferentes.

2. Quando uma ligação é classificada a amarelo, em conformidade com o disposto no n.º 1, aplica-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 da UE deve ser classificada como verde se:

a) Os dados ligados têm dados biométricos diferentes, mas partilham os mesmos dados de identificação e a autoridade responsável pela verificação manual das diferentes identidades concluiu que os dados ligados se referem a duas pessoas diferentes;

b) Os dados ligados têm dados biométricos diferentes, têm dados de identificação similares ou diferentes, têm os mesmos dados do documento de viagem, e a autoridade responsável pela verificação manual das diferentes identidades concluiu que os dados ligados se referem a duas pessoas diferentes;

c) Os dados ligados têm dados de identificação diferentes, mas partilham os mesmos dados do documento de viagem, pelo menos um dos sistemas de informação da UE não dispõe de dados biométricos sobre a pessoa em causa e a autoridade responsável pela verificação manual das diferentes identidades concluiu que os dados ligados se referem a duas pessoas diferentes.

2. Quando o CIR ou o SIS são consultados e se existe uma ligação verde entre dois ou mais sistemas de informação da UE, o MID indica que os dados de identificação dos dados ligados não correspondem à mesma pessoa.

3. A autoridade de um Estado-Membro deve verificar os dados pertinentes armazenados no CIR e no SIS e, se necessário, retificar ou apagar sem demora a ligação do MID, caso tenha indícios de que uma ligação verde foi registada de forma incorreta no MID, ou que uma ligação verde está desatualizada ou de que foram tratados dados no MID ou nos sistemas de informação da UE em violação do presente regulamento. Essa autoridade do Estado-Membro deve informar sem demora o Estado-Membro responsável pela verificação manual das diferentes identidades.

Artigo 32.º

Ligação vermelha

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

a) Os dados ligados partilham os mesmos dados biométricos, mas apresentam dados de identificação similares ou diferentes e a autoridade responsável pela verificação manual das diferentes identidades concluiu que os dados ligados se referem, de forma injustificada, à mesma pessoa;

b) Os dados ligados possuem os mesmos dados de identificação ou dados de identificação semelhantes ou diferentes e os mesmos dados do documento de viagem, mas dados biométricos diferentes e a autoridade responsável pela verificação manual das diferentes identidades concluiu que os dados ligados se referem a duas pessoas diferentes em que, pelo menos, um deles utiliza, de forma injustificada, o mesmo documento de viagem;

c) Os dados ligados partilham os mesmos dados de identificação, mas têm dados biométricos diferentes e os dados do documento de viagem são diferentes ou inexistentes, e a autoridade responsável pela verificação manual das diferentes identidades concluiu que os dados ligados se referem, de forma injustificada, a duas pessoas diferentes;

d) Os dados ligados têm dados de identificação diferentes, mas têm os mesmos dados de documento de viagem, pelo menos um dos sistemas de informação da UE não dispõe de dados biométricos sobre a pessoa e a autoridade responsável pela verificação manual das diferentes identidades concluiu que os dados ligados se referem, de forma injustificada, à mesma pessoa.

2. Quando o CIR ou o SIS são consultados e existe uma ligação vermelha entre dados de dois ou mais sistemas de informação da UE, o MID indica 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, e as eventuais consequências jurídicas para a pessoa baseiam-se apenas nos dados pertinentes relativos a essa pessoa. Nenhuma consequência jurídica para a pessoa em causa deve advir exclusivamente da existência de uma ligação vermelha.

3. Nos casos em que é criada uma ligação vermelha entre os dados do SES, do VIS, do ETIAS, do Eurodac ou do ECRIS-TCN, o processo individual guardado no CIR deve ser atualizado em conformidade com o artigo 19.º, n.º 2.

4. Sem prejuízo das disposições relativas ao tratamento de indicações no SIS referidas no Regulamento (UE) 2018/1860, no Regulamento (UE) 2018/1861 e no Regulamento (UE) 2018/1862, 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 ligação vermelha é criada, a autoridade responsável pela verificação manual das diferentes identidades deve informar a pessoa em causa da existência de dados de identificação múltiplos ilegais e fornecer-lhe o número de identificação único, tal como referido no artigo 34.º, alínea c), do presente regulamento, uma referência à autoridade responsável pela verificação manual das diferentes identidades, tal como referido no artigo 34.º, alínea d), do presente regulamento, e o endereço do portal Web criado em conformidade com o artigo 49.º, do presente regulamento.

5. A informação a que se refere o n.º 4, deve ser dada por escrito pela autoridade responsável pela verificação manual das diferentes identidades por meio de um formulário normalizado. A Comissão determina o conteúdo e a apresentação desse formulário por meio de atos de execução. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 74.º, n.º 2.

6. Nos casos em que uma ligação vermelha é criada, o MID notifica as autoridades responsáveis pelos dados ligados de forma automatizada.

7. Sempre que uma autoridade de um Estado-Membro ou uma agência da União com acesso ao CIR ou ao SIS tenha indícios de que uma ligação vermelha foi registada de forma incorreta no MID ou de que os dados tratados no MID, no CIR ou no SIS foram tratados em violação do presente regulamento, essa autoridade ou agência deve verificar os dados relevantes armazenados no CIR e no SIS e deve:

a) Caso a ligação diga respeito a uma das indicações do SIS a que se refere o artigo 29.º, n.º 2, informar imediatamente o gabinete SIRENE do Estado-Membro que criou a indicação no SIS;

b) Nos restantes casos, retificar ou apagar imediatamente a ligação do MID.

Caso o gabinete SIRENE seja contactado nos termos da alínea a), do primeiro parágrafo, o gabinete deve verificar os elementos de prova fornecidos pela autoridade do Estado-Membro ou da agência da União e, se for caso disso, retificar ou apagar imediatamente a ligação do MID.

A autoridade do Estado-Membro que obtém os elementos de prova deve informar sem demora a autoridade do Estado-Membro responsável pela verificação manual das diferentes identidades, de uma eventual retificação ou apagamento de uma ligação vermelha.

Artigo 33.º

Ligação branca

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

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

b) Os dados ligados partilham os mesmos dados de identificação ou dados de identificação semelhantes, os mesmos dados do documento de viagem e pelo menos um dos sistemas de informação da UE não dispõe de dados biométricos da pessoa em causa;

c) Os dados ligados partilham os mesmos dados biométricos e os mesmos dados do documento de viagem e dados de identificação similares;

d) Os dados ligados partilham os mesmos dados biométricos, mas têm dados de identificação similares ou diferentes e a autoridade responsável pela verificação das diferentes identidades concluiu que os dados ligados se referem justificadamente à mesma pessoa.

2. Quando o CIR ou o SIS são consultados e existe uma ligação branca entre dois ou mais dos sistemas de informação da UE, o MID indica que os dados de identificação de dados ligados correspondem à mesma pessoa. Os sistemas de informação da UE consultados respondem indicando, se for caso disso, todos os dados ligados sobre a pessoa, desencadeando assim uma correspondência 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 ECRIS-TCN, o processo individual guardado no CIR deve ser atualizado em conformidade com o artigo 19.º, n.º 2.

4. Sem prejuízo das disposições relativas ao tratamento de indicações no SIS constantes dos Regulamento (UE) 2018/1860, no Regulamento (UE) 2018/1861 e no Regulamento (UE) 2018/1862, 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 é criada uma ligação branca na sequência de uma verificação manual das diferentes identidades, a autoridade responsável pela verificação manual das diferentes identidades deve informar a pessoa em causa da existência de dados de identificação similares ou diferentes e fornecer-lhe um número de identificação único, tal como referido no artigo 34.º, alínea c), do presente regulamento, uma referência à autoridade responsável pela verificação manual das diferentes identidades, tal como referido no artigo 34.º, alínea d), do presente regulamento, e o endereço do portal Web criado em conformidade com o artigo 49.º do presente regulamento.

5. A autoridade de um Estado-Membro deve verificar os dados pertinentes armazenados no CIR e no SIS e, se necessário, retificar ou apagar sem demora a ligação do MID, caso tenha indícios de que uma ligação branca foi registada de forma incorreta no MID, ou que uma ligação branca está desatualizada ou de que foram tratados dados no MID ou nos sistemas de informação da UE em violação do presente regulamento. Essa autoridade do Estado-Membro deve informar sem demora o Estado-Membro responsável pela verificação manual das diferentes identidades.

6. A informação a que se refere o n.º 4 deve ser prestada por escrito, através de formulário normalizado, pela autoridade responsável pela verificação manual das diferentes identidades. A Comissão determina o conteúdo e apresentação desse formulário através de atos de execução. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 74.º, n.º 2.

Artigo 34.º

Processo de confirmação de identidade

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

a) As ligações, tal como referido nos artigos 30.º a 33.º;

b) Uma referência aos sistemas de informação da UE, nos quais os dados estão ligados;

c) Um número de identificação único, permitindo a extração dos dados a partir dos sistemas de informação da UE correspondentes;

d) A autoridade responsável pela verificação manual das diferentes identidades;

e) A data de criação ou de atualização da ligação.

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 MID apenas enquanto os dados permanecerem armazenados em dois ou mais sistemas de informação da UE. Os processos de confirmação de identidade e respetivos dados, devem ser apagados do MID de forma automatizada.

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 o seguinte:

a) O Estado-Membro que inicia a consulta;

b) O objetivo do acesso do utilizador;

c) A data e a hora da consulta;

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

e) A referência aos dados ligados;

f) O histórico do processo de confirmação de identidade.

2. Cada Estado-Membro deve manter registos das consultas feitas pelas suas autoridades e pelo pessoal devidamente autorizado dessas autoridades a utilizar o MID. Cada agência da União deve manter registos das consultas feitas pelo seu pessoal devidamente autorizado a utilizar o MID.

3. Os registos referidos nos n.os 1 e 2 só podem ser utilizados para controlo da proteção de dados, incluindo a verificação da admissibilidade de uma consulta e da legalidade do tratamento dos dados, bem como para garantir a sua segurança e integridade. Esses registos devem estar protegidos por medidas adequadas contra o acesso não autorizado e apagados um ano após a sua criação. Se, no entanto, forem necessários para procedimentos de controlo que já tenham tido início, esses registos devem ser apagados logo que deixarem de ser necessários para o efeito.

CAPÍTULO VI

Medidas de apoio à interoperabilidade

Artigo 37.º

Qualidade dos dados

1. Sem prejuízo das responsabilidades dos Estados-Membros em matéria de qualidade dos dados introduzidos nos sistemas, a eu-LISA deve criar mecanismos e procedimentos automatizados de controlo de qualidade de dados sobre os dados armazenados no SES, no VIS, no ETIAS, no SIS, no serviço partilhado BMS e no CIR.

2. A eu-LISA deve implementar mecanismos para avaliar a exatidão do BMS, indicadores comuns de qualidade dos dados e as normas mínimas de qualidade para armazenar os dados no SES, VIS, ETIAS, SIS, serviço partilhado BMS e CIR.

Só os dados que cumprem as normas mínimas de qualidade podem ser introduzidos no SES, no VIS, no ETIAS, no SIS, no serviço partilhado BMS, no CIR e no 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. A pedido, a eu-LISA deve também apresentar esse relatório ao Parlamento Europeu e ao Conselho. Os relatórios apresentados nos termos do presente número não podem conter quaisquer dados pessoais.

4. As informações pormenorizadas relativas aos mecanismos e procedimentos automatizados de controlo da qualidade, indicadores comuns de qualidade dos dados e normas mínimas de qualidade para armazenar os dados no SES, VIS, ETIAS, SIS, no serviço partilhado BMS e CIR, em especial no que se refere aos dados biométricos, devem ser estabelecidos em atos de execução. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 74.º, n.º 2.

5. Um ano após a criação dos mecanismos e procedimentos automatizados de controlo da qualidade dos dados, indicadores comuns da qualidade dos dados e normas mínimas de qualidade de 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, em especial, os problemas de qualidade dos dados devido a dados erróneos armazenados nos sistemas de informação da UE. Os Estados-Membros comunicam periodicamente à Comissão quaisquer progressos na aplicação deste 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, ao Comité Europeu para a Proteção de Dados e à Agência dos Direitos Fundamentais da União Europeia, criada pelo Regulamento (CE) n.º 168/2007 do Conselho ([39]).

Artigo 38.º

Formato de mensagem universal

1. O presente artigo estabelece a norma relativa ao Formato de Mensagem Universal (UMF). A UMF define as normas relativas a determinado conteúdo de intercâmbio de informações transfronteiriço, entre sistemas de informação, autoridades ou organizações no domínio da Justiça e Assuntos Internos.

2. A norma UMF deve ser utilizada no desenvolvimento do SES, do ETIAS, do ESP, do CIR, do MID e, se for caso disso, no desenvolvimento pela eu-LISA ou por qualquer outra agência da União de novos modelos de intercâmbio de informações e de sistemas de informação no domínio da Justiça e Assuntos Internos.

3. A Comissão deve adotar um ato de execução para estabelecer e desenvolver a norma UMF referida no n.º 1 do presente artigo. Esse ato de execução é adotado pelo procedimento de exame a que se refere o artigo 74.º, n.º 2.

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, em conformidade com os respetivos atos jurídicos que regem esses sistemas, e para fornecer 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 e as estatísticas referidos no artigo 63.º do Regulamento (UE) 2017/2226, no artigo 17.º do Regulamento (CE) n.º 767/2008, no artigo 84.º do Regulamento (UE) 2018/1240, no artigo 60.º do Regulamento (UE) 2018/1861 e no artigo 16.º do Regulamento (UE) 2018/1860, logicamente separados pelo sistema de informações da UE. O acesso ao CRRS deve ser concedido mediante um acesso controlado, seguro, com 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 (UE) 2017/2226, o artigo 17.º do Regulamento (CE) n.º 767/2008, o artigo 84.º do Regulamento (UE) 2018/1240 e o artigo 60.º do Regulamento (UE) 2018/1861.

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

Os dados contidos no CRRS não podem permitir a identificação de pessoas.

4. O CRRS é constituído pelos seguintes elementos:

a) Os instrumentos necessários para anonimizar os dados;

b) Uma infraestrutura central, constituída por um repositório de dados anónimos;

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

5. A Comissão deve adotar atos delegados nos termos do artigo 73.º a fim de estabelecer regras pormenorizadas sobre o funcionamento do CRRS, incluindo garantias específicas para o tratamento dos dados pessoais nos termos dos n.ºs 2 e 3 do presente artigo e regras de segurança aplicáveis ao repositório.

([39]) 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).

CAPÍTULO VII

Proteção de dados

Artigo 40.º

Responsável pelo tratamento de dados

1. No que respeita ao tratamento dos dados no serviço partilhado BMS, as autoridades dos Estados-Membros que são responsáveis pelo tratamento de dados do SES, VIS e SIS, respetivamente, devem ser responsáveis pelo tratamento dos dados, em conformidade com o artigo 4.º, ponto 7, do Regulamento (UE) 2016/679 ou o artigo 3.º, ponto 8, da Diretiva (UE) 2016/680, no que diz respeito aos modelos biométricos obtidos a partir dos dados referidos no artigo 13.º do presente regulamento introduzidos nos sistemas respetivos, sendo responsáveis pelo tratamento dos modelos biométricos no serviço partilhado BMS.

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

3. No que respeita ao tratamento dos dados no MID:

a) A Agência Europeia da Guarda de Fronteiras e Costeira é responsável pelo tratamento dos dados na aceção do artigo 3.º, ponto 8, do Regulamento (UE) 2018/1725, 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 responsáveis pelo tratamento, em conformidade com o artigo 4.º, ponto 7, do Regulamento (UE) 2016/679 ou o artigo 3.º, ponto 8, da Diretiva (UE) 2016/680, sendo responsáveis pelo tratamento dos dados pessoais no MID.

4. Para efeitos de controlo da proteção de dados, incluindo a verificação da admissibilidade de uma consulta e da legalidade do tratamento dos dados, os responsáveis pelo tratamento dos dados devem ter acesso aos registos referidos nos artigos 10.º, 16.º, 24.º e 36.º para fins de autocontrolo, como referido no artigo 44.º.

Artigo 41.º

Subcontratante de dados

No que respeita ao tratamento de dados pessoais no serviço partilhado BMS, no CIR e no MID, a eu-LISA deve ser um subcontratante de dados na aceção do artigo 3.º, ponto 12, alínea a) do Regulamento (UE) 2018/1725.

Artigo 42.º

Segurança do tratamento

1. A eu-LISA, a unidade central do ETIAS, a Europol e as autoridades dos Estados-Membros devem garantir a segurança do tratamento dos dados pessoais que decorre de acordo com o presente regulamento. A eu-LISA, a unidade central do ETIAS, a Europol e as autoridades dos Estados-Membros devem cooperar em tarefas relacionadas com a segurança.

2. Sem prejuízo do artigo 33.º do Regulamento (UE) 2018/1725, 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) Recusar o acesso de pessoas não autorizadas às instalações e ao equipamento de tratamento de dados;

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

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

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

f) Impedir que os sistemas de tratamento automatizado de dados sejam utilizados por pessoas não autorizadas usando equipamento de comunicação de dados;

g) 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;

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

i) 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;

j) Impedir a leitura, a cópia, a alteração ou a eliminação não autorizada 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;

k) Assegurar que, em caso de interrupção, é possível restaurar o funcionamento normal dos sistemas instalados;

l) Assegurar a fiabilidade, garantindo que as eventuais falhas no funcionamento dos componentes de interoperabilidade são devidamente notificadas;

m) 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 e avaliar essas medidas de segurança à luz dos novos desenvolvimentos tecnológicos.

4. Os Estados-Membros, a Europol e a unidade central do ETIAS 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

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 sem demora a Comissão, a eu-LISA, as autoridades de controlo competentes e a Autoridade Europeia para a Proteção de Dados de quaisquer incidentes de segurança.

Sem prejuízo dos artigos 34.º e 35.º do Regulamento (UE) 2018/1725 e do artigo 34.º do Regulamento (UE) 2016/794, a unidade central do ETIAS e a Europol devem notificar sem demora a Comissão, a eu-LISA e a Autoridade Europeia para a Proteção de Dados de quaisquer incidentes de segurança.

Em caso de incidente de segurança em relação aos componentes de interoperabilidade da infraestrutura central, a eu-LISA deve notificar sem demora 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 sem demora aos Estados-Membros, à unidade central do ETIAS e à Europol e comunicadas em conformidade com o plano de gestão de incidentes fornecido pela eu-LISA.

5. Os Estados-Membros em causa, a unidade central do ETIAS, a Europol 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 são adotados pelo procedimento de exame a que se refere o artigo 74.º, n.º 2.

Artigo 44.º

Autocontrolo

Os Estados-Membros e as agências competentes da União devem assegurar que cada autoridade com direito de acesso aos componentes de interoperabilidade toma as medidas necessárias para controlar o cumprimento do presente 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 através da verificação frequente dos registos referidos nos artigos 10.º, 16.º, 24.º e 36.º, e cooperar, se necessário, com as autoridades de controlo e com a Autoridade Europeia para a Proteção de Dados.

Artigo 45.º

Sanções

Os Estados-Membros asseguram que qualquer utilização abusiva de dados, tratamento de dados ou intercâmbio de dados que viole o disposto no presente regulamento seja punível nos termos do direito nacional. As sanções previstas devem ser efetivas, proporcionadas e dissuasivas.

Artigo 46.º

Responsabilidade

1. Sem prejuízo do direito à indemnização e da responsabilidade do responsável pelo tratamento dos dados ou do subcontratante nos termos do Regulamento (UE) 2016/679, da Diretiva (UE) 2016/680 e do Regulamento (UE) 2018/1725:

a) Qualquer pessoa ou Estado-Membro que tenha sofrido danos materiais ou imateriais em virtude de uma operação ilícita de tratamento de dados pessoais ou de qualquer outro ato incompatível com o presente regulamento levados a cabo por um Estado-Membro tem direito a ser indemnizado por esse Estado-Membro;

b) Qualquer pessoa ou Estado-Membro que tenha sofrido danos materiais ou imateriais em virtude de um ato da Europol, da Agência Europeia da Guarda de Fronteiras e Costeira ou da eu-LISA incompatível com o presente regulamento tem direito a ser indemnizado pela agência em causa.

O Estado-Membro em causa, a Europol, a Agência Europeia da Guarda de Fronteiras e Costeira ou a eu-LISA ficam total ou parcialmente exonerados da sua responsabilidade por força do primeiro parágrafo, se provarem que o evento que deu origem aos danos não lhes é imputável.

2. Se o incumprimento por um Estado-Membro das obrigações que lhe incumbem por força do presente regulamento causar danos aos componentes de interoperabilidade, esse Estado-Membro é responsável pelos danos, a menos e na medida em que a eu-LISA ou outro Estado-Membro vinculado pelo presente regulamento não tenha tomado medidas razoáveis para prevenir os danos ou minimizar o seu impacto.

3. Os pedidos de indemnização a um Estado-Membro pelos danos referidos nos n.os 1 e 2 são regulados pelo direito interno do Estado-Membro requerido. Os pedidos de indemnização apresentados ao responsável pelo tratamento dos dados ou à eu-LISA pelos danos referidos nos n.os 1 e 2 ficam sujeitos às condições previstas nos Tratados.

Artigo 47.º

Direito à informação

1. A autoridade responsável pela recolha dos dados das pessoas cujos dados são conservados no serviço partilhado BMS, no CIR ou no MID deve facultar às pessoas cujos dados são recolhidos as informações previstas nos termos dos artigos 13.º e 14.º do Regulamento (UE) 2016/679, dos artigos 12.º e 13.º da Diretiva (UE) 2016/680 e dos artigos 15.º e 16.º do Regulamento (UE) 2018/1725. A autoridade deve fornecer as informações no momento da recolha desses dados.

2. Todas as informações devem ser disponibilizadas em linguagem clara e simples, numa versão linguística que a pessoa em causa compreenda ou que se espere, de forma razoável, que compreenda. Tal deve incluir o fornecimento de informações de uma maneira adequada à idade dos titulares de dados que sejam menores.

3. As pessoas cujos dados estejam registados no SES, no VIS ou no ETIAS devem ser informadas sobre o tratamento de dados pessoais 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 (UE) 2017/2226;

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 19.º do Regulamento (UE) 2018/1240.

Artigo 48.º

Direito de acesso, de retificação e de apagamento de dados pessoais armazenados no MID e limitação do tratamento desses dados

1. A fim de exercer os seus direitos ao abrigo dos artigos 15.º a 18.º do Regulamento (UE) 2016/679, dos artigos 17.º a 20.º do Regulamento (UE) 2018/1725 e dos artigos 14.º, 15.º e 16.º da Diretiva (UE) 2016/680, qualquer pessoa tem o direito de se dirigir à autoridade competente de qualquer Estado-Membro, que deve examinar e responder ao pedido.

2. O Estado-Membro que examine o pedido deve responder sem demora injustificada e, em qualquer caso, no prazo de 45 dias a contar da receção do pedido. Esse prazo pode ser prorrogado por 15 dias, se necessário, tendo em conta a complexidade e o número de pedidos. O Estado-Membro que examinou o pedido deve informar o titular dos dados da prorrogação e dos motivos da demora no prazo de 45 dias a contar da data de receção do pedido. Os Estados-Membros podem decidir que estas respostas sejam dadas pelos serviços centrais.

3. Se for apresentado um pedido de retificação ou apagamento de dados pessoais a um Estado-Membro diferente do Estado-Membro responsável pela verificação manual das diferentes identidades, o Estado-Membro ao qual foi apresentado o pedido deve contactar as autoridades do Estado-Membro responsável pela verificação manual das diferentes identidades no prazo de sete dias. O Estado-Membro responsável pela verificação manual das diferentes identidades deve verificar a exatidão dos dados e a legalidade do tratamento dos dados sem demora injustificada e, em qualquer caso, no prazo de 30 dias a contar desse contacto. Esse prazo pode ser prorrogado por 15 dias, se necessário, tendo em conta a complexidade e o número de pedidos. O Estado– Membro responsável pela verificação manual das diferentes identidades informa o Estado-Membro, ao qual foi apresentado o pedido, da prorrogação do prazo bem como a sua fundamentação. O Estado-Membro que contactou a autoridade do Estado-Membro responsável pela verificação manual das diferentes identidades informa a pessoa em causa sobre o procedimento subsequente.

4. Se for apresentado um pedido de retificação ou apagamento de dados pessoais a um Estado-Membro e a unidade central do ETIAS foi responsável pela verificação manual das diferentes identidades, o Estado-Membro ao qual foi apresentado o pedido deve contactar a unidade central do ETIAS no prazo de sete dias, solicitando que emita o seu parecer. A unidade central do ETIAS emite parecer, sem demora injustificada, qualquer caso, no prazo de 30 dias a contar desse contacto. Esse prazo pode ser prorrogado por 15 dias, se necessário, tendo em conta a complexidade e o número de pedidos. O Estado-Membro que contactou a unidade central do ETIAS informa a pessoa em causa sobre o procedimento subsequente.

5. Sempre que, na sequência de um exame, se concluir que os dados armazenados no MID são inexatos ou foram registados ilegalmente, o Estado-Membro responsável pela verificação manual das diferentes identidades ou, caso não tenha havido um Estado-Membro responsável pela verificação manual das diferentes identidades ou a unidade central do ETIAS tenha sido responsável pela verificação manual das diferentes identidades, o Estado-Membro ao qual foi apresentado o pedido deve proceder sem demora injustificada à sua retificação ou ao seu apagamento. A pessoa em causa deve ser informada por escrito de que os seus dados foram retificados ou apagados.

6. Caso os dados armazenados no MID sejam alterados por um Estado-Membro durante o respetivo período de conservação, esse Estado-Membro 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 correspondência, esse Estado-Membro deve apagar os dados do processo de confirmação de identidade. Sempre que o tratamento automatizado comunicar uma ou várias correspondências, esse Estado-Membro deve criar ou atualizar a ligação em questão em conformidade com as disposições aplicáveis do presente regulamento.

7. Sempre que o Estado-Membro responsável pela verificação manual das diferentes identidades ou, se for caso disso, o Estado-Membro ao qual foi apresentado o pedido não considerar que os dados armazenados no MID são 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.

8. A decisão a que se refere o n.º 7 deve informar também o interessado sobre a possibilidade de impugnar a decisão tomada relativamente ao pedido de acesso, retificação, apagamento ou limitação do tratamento de dados pessoais 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 de controlo.

9. Qualquer pedido de acesso, retificação, apagamento ou limitação do tratamento de dados pessoais 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 presente artigo, após o que serão imediatamente apagadas.

10. O Estado-Membro responsável pela verificação manual das diferentes identidades ou, se for caso disso, o Estado-Membro ao qual foi apresentado o pedido, deve conservar um registo escrito relativo à apresentação de um pedido de acesso, retificação, apagamento ou limitação do tratamento de dados pessoais e à forma como foi tratado, e disponibilizar sem demora esse registo às autoridades de controlo.

11. O presente artigo aplica-se sem prejuízo das limitações e restrições aos direitos previstos no presente artigo nos termos do Regulamento (UE) 2016/679 e da Diretiva (UE) 2016/680.

Artigo 49.º

Portal Web

1. É criado um portal Web com o objetivo de facilitar o exercício dos direitos de acesso, retificação, apagamento ou de limitação do tratamento de dados pessoais.

2. O portal Web deve conter informações sobre os direitos e procedimentos referidos nos artigos 47.º e 48.º e uma interface do utilizador que permita às pessoas cujos dados são tratados através do MID e que foram informadas da presença de uma ligação vermelha, em conformidade com o artigo 32.º, n.º 4, receber os dados de contacto da autoridade competente do Estado-Membro responsável pela verificação manual das diferentes identidades.

3. A fim de obter os dados de contacto da autoridade competente do Estado-Membro responsável pela verificação manual das diferentes identidades, a pessoa cujos dados são tratados através do MID deve inserir a referência à autoridade responsável pela verificação manual das diferentes identidades referida no artigo 34.º, alínea d). O portal Web deve utilizar esta referência para obter os dados de contacto da autoridade competente do Estado-Membro responsável pela verificação manual das diferentes identidades. O portal Web deve também incluir um modelo de mensagem de correio eletrónico para facilitar a comunicação entre o utilizador do portal e a autoridade competente do Estado-Membro responsável pela verificação manual das diferentes identidades. Essa mensagem deve incluir um campo relativo ao número de identificação único referido no artigo 34.º, alínea c), a fim de permitir à autoridade competente do Estado-Membro responsável pela verificação manual das diferentes identidades a identificação dos dados em causa.

4. Os Estados-Membros devem fornecer à eu-LISA os dados de contacto de todas as autoridades competentes para examinar e responder a qualquer pedido, tal como referido nos artigos 47.º e 48.º, e verificar regularmente se esses dados de contacto estão atualizados.

5. A eu-LISA deve desenvolver o portal Web, ficando responsável pela sua gestão técnica.

6. A Comissão deve adotar um ato delegado, nos termos do artigo 73.º, a fim de estabelecer regras pormenorizadas sobre o funcionamento do portal Web, incluindo a interface do utilizador, as línguas em que o portal deve estar disponível e o modelo de mensagem de correio eletrónico.

Artigo 50.º

Comunicação de dados pessoais a países terceiros, organizações internacionais e entidades privadas

Sem prejuízo do disposto no artigo 65.º do Regulamento (UE) 2018/1240, nos artigos 25.º e 26.ºdo Regulamento (UE) 2016/794, no artigo 41.º do Regulamento (UE) 2017/2226, no artigo 31.º do Regulamento (CE) n.º 767/2008 e da consulta das bases de dados da Interpol através do ESP, nos termos do artigo 9.º, n.º 5, do presente regulamento, que cumpram as disposições do capítulo V do Regulamento (UE) 2018/1725 e do capítulo V do Regulamento (UE) 2016/679, os dados pessoais armazenados, tratados ou consultados pelos componentes de interoperabilidade não podem ser transferidos nem disponibilizados a países terceiros, organizações internacionais ou entidades privadas.

Artigo 51.º

Fiscalização pelas autoridades de controlo

1. Cada Estado-Membro assegura que as autoridades de controlo controlam de forma independente a legalidade do tratamento dos dados pessoais a que se refere o presente regulamento pelo Estado-Membro em causa, incluindo a sua transmissão aos componentes de interoperabilidade e a partir dos mesmos.

2. Cada Estado-Membro assegura que as disposições legislativas, regulamentares e administrativas nacionais adotadas nos termos da Diretiva (UE) 2016/680 sejam igualmente aplicáveis, se for caso disso, ao acesso aos componentes de interoperabilidade pelas autoridades policiais e pelas autoridades designadas, inclusive no que respeita aos direitos das pessoas a cujos dados se tem assim acesso.

3. As autoridades de controlo devem garantir a realização de uma auditoria às operações de tratamento de dados pessoais pelas autoridades nacionais competentes para efeitos do presente regulamento em conformidade com as normas internacionais de auditoria aplicáveis, pelo menos de quatro em quatro anos.

As autoridades de controlo publicam anualmente o número de pedidos de retificação, apagamento ou limitação do tratamento de dados pessoais, as medidas subsequentemente tomadas e o número de retificações, apagamentos e limitações de tratamento que tiveram lugar na sequência dos pedidos apresentados pelas pessoas em causa.

4. Os Estados-Membros devem assegurar que as autoridades de controlo dispõem dos meios e da capacidade técnica necessários para cumprir as tarefas que lhes são confiadas no âmbito do presente regulamento.

5. Os Estados-Membros comunicam todas as informações solicitadas por qualquer uma das autoridades de controlo referidas no artigo 51.º, n.º 1, do Regulamento (UE) 2016/679 e, em especial, fornecem-lhe informações relativas às atividades desenvolvidas no âmbito das suas atribuições estabelecidas pelo presente regulamento. Os Estados-Membros concedem às autoridades de controlo referidas no artigo 51.º, n.º 1, do Regulamento (UE) 2016/679 o acesso aos seus registos referidos nos artigos 10.º, 16.º, 24.º e 36.º, do presente regulamento, às suas justificações referidas no artigo 22.º, n.º 2, do presente regulamento, e permitem-lhes o acesso, a qualquer momento, a todas as suas instalações utilizadas para fins de interoperabilidade.

Artigo 52.º

Auditorias pela Autoridade Europeia para a Proteção de Dados

A Autoridade Europeia para a Proteção de Dados deve garantir a realização de uma auditoria às operações de tratamento de dados pessoais efetuadas pela eu-LISA, pela unidade central do ETIAS e pela Europol para efeitos do presente regulamento, 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, aos Estados-Membros e à agência da União em causa. Deve ser dada à eu-LISA, à unidade central do ETIAS e à Europol a oportunidade de efetuar comentários antes da adoção dos relatórios.

A eu-LISA, a unidade central do ETIAS e a Europol fornecem à Autoridade Europeia para a Proteção de Dados as informações por esta solicitadas, concedem à Autoridade Europeia para a Proteção de Dados o acesso a todos os documentos e aos seus registos referidos nos artigos 10.º, 16.º, 24.º e 36.º, e permitem à Autoridade Europeia para a Proteção de Dados o acesso permanente a todas as suas instalações.

Artigo 53.º

Cooperação entre as autoridades de controlo e a Autoridade Europeia para a Proteção de Dados

1. As autoridades de controlo e a Autoridade Europeia para a Proteção de Dados, agindo cada uma no âmbito das respetivas competências, cooperam ativamente no âmbito das respetivas responsabilidades e asseguram a supervisão coordenada da utilização dos componentes de interoperabilidade e a aplicação das restantes disposições do presente regulamento, em particular se a Autoridade Europeia para a Proteção de Dados ou uma autoridade 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.

2. Nos casos referidos no n.º 1 do presente artigo, o controlo coordenado deve ser assegurado nos termos do artigo 62.º do Regulamento (UE) 2018/1725.

3. O Comité Europeu para a Proteção de Dados deve enviar um relatório das suas atividades nos termos do presente artigo ao Parlamento Europeu, ao Conselho, à Comissão, à Europol, à Agência Europeia da Guarda de Fronteiras e Costeira e à eu-LISA até 12 de junho de 2021 e, posteriormente, de dois em dois anos. O referido relatório deve incluir um capítulo sobre cada Estado-Membro, elaborado pela respetiva autoridade de controlo.

CAPÍTULO VIII

Responsabilidades

Artigo 54.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 desempenho a que se refere o artigo 55.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, do Eurodac, e do ECRIS-TCN, e o ESP, o serviço partilhado BMS, o CIR, o MID e o CRRS.

Sem prejuízo do disposto no artigo 66.º, a eu-LISA não tem acesso a nenhum dos dados pessoais tratados através do ESP, do serviço partilhado BMS, do CIR ou do MID.

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, VIS, ETIAS ou SIS 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 no artigo 8.º, n.º 2, artigo 9.º, n.º 7, artigo 28.º, n.ºs 5 e 7, artigo 37.º, n.º 4, artigo 38.º, n.º 3, artigo 39.º, n.º 5, artigo 43.º, n.º 5 e artigo 78.º, n.º 10.

O desenvolvimento deve consistir na elaboração e implementação das especificações técnicas, nos testes e na gestão e coordenação globais 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. Este 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 75.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 pelo direito da União pelos atos jurídicos que regem o desenvolvimento, o estabelecimento, o funcionamento e a utilização de todos os sistemas de informação da UE e que irão participar nos componentes de interoperabilidade.

5. O Conselho de Gestão do Programa deve reunir-se periodicamente 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 da eu-LISA 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 pelo direito da União pelos atos jurídicos que regem o desenvolvimento, o estabelecimento, o funcionamento e a utilização de todos os sistemas de informação da UE e que irão participar nos componentes de interoperabilidade.

Todas as despesas de viagem e de estadia incorridas pelos membros do Conselho de Gestão do Programa devem ser pagas pela eu-LISA, aplicando-se o artigo 10.º do regulamento interno da eu-LISA com as necessárias adaptações. A eu-LISA deve assegurar o secretariado ao Conselho de Gestão do Programa.

O Grupo Consultivo de Interoperabilidade, referido no artigo 75.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 55.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 dos componentes de interoperabilidade, incluindo a manutenção e os desenvolvimentos tecnológicos. Em cooperação com os Estados-Membros, deve assegurar que seja usada 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 e soluções técnicas necessárias para manter o funcionamento dos componentes de interoperabilidade, prestando serviços ininterruptos aos Estados-Membros e às agências da União 24 horas por dia e 7 dias por semana, em conformidade com o presente regulamento. A gestão técnica dos componentes de interoperabilidade deve incluir 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.

Todos os componentes de interoperabilidade devem ser desenvolvidos e geridos de forma a assegurar um acesso rápido, contínuo, eficiente e controlado, assim como a disponibilidade total e ininterrupta dos componentes e dos dados armazenados no MID, no serviço partilhado BMS e no CIR, e um tempo de resposta adaptado às necessidades operacionais das autoridades dos Estados-Membros e das agências da União.

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.

Sem prejuízo do artigo 66.º, a eu-LISA não tem acesso a nenhum dos dados pessoais tratados através do ESP, do serviço partilhado BMS, do CIR e do MID.

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 BMS e no CIR 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 56.º

Responsabilidades dos Estados-Membros

1. Cada Estado-Membro é responsável pelo seguinte:

a) Ligação à infraestrutura de comunicação do ESP e do CIR;

b) Integração dos sistemas e infraestruturas nacionais existentes com o ESP, o CIR e o MID;

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 das autoridades nacionais competentes ao ESP, ao CIR e ao MID 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.ºs 5 e 6, a fim de aceder ao CIR para efeitos de identificação;

f) Verificação manual das diferentes identidades a que se refere o artigo 29.º;

g) Cumprimento dos requisitos de qualidade dos dados estabelecidos nos termos do direito da União;

h) Cumprimento das regras de cada sistema de informação da UE relativas à segurança e à integridade dos dados pessoais;

i) 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 ao CIR.

Artigo 57.º

Responsabilidades da unidade central do ETIAS

A unidade central do ETIAS é responsável pela:

a) Verificação manual das diferentes identidades, nos termos do artigo 29.º;

b) Realização de uma deteção de identidades múltiplas entre os dados armazenados no SES, VIS, Eurodac e SIS referidos no artigo 69.º.

CAPÍTULO IX

Alteração de outros atos jurídicos da União

Artigo 58.º

Alteração do Regulamento (CE) n.º 767/2008

O Regulamento (CE) n.º 767/2008 é alterado do seguinte modo:

1) Ao artigo 1.º é aditado o seguinte número:

«Através do armazenamento dos dados de identificação, dos dados dos documentos de viagem e dos dados biométricos no repositório comum de dados de identificação (CIR) estabelecido pelo artigo 17.º, n.º 1, do Regulamento (UE) 2019/817 do Parlamento Europeu e do Conselho (*), o VIS contribui para facilitar e apoiar a identificação correta das pessoas registadas no VIS nas condições e para o estabelecido no artigo 20.º desse regulamento.

(*) Regulamento (UE) 2019/817 do Parlamento Europeu e do Conselho, de 20 de maio de 2019, relativo à criação de um regime de interoperabilidade entre os sistemas de informação da UE no domínio das fronteiras e vistos e que altera os Regulamentos (CE) n.º 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 do Parlamento Europeu e do Conselho, e as Decisões 2004/512/CE e 2008/633/JAI do Conselho (JO L 135 de 22.5.2019, p. 27).».

2) Ao 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 identificação", os dados mencionados no artigo 9.º, n.º 4, alíneas a) e a-A);

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

3) No artigo 5.º é inserido o seguinte número:

«1-A) O CIR contém os dados referidos no artigo 9.º, n.º 4, alíneas a) a c), no artigo 9.º, n.º s5 e 6, sendo os restantes dados VIS armazenados no sistema central do VIS.».

4) No artigo 6.º, o n.º 2, passa a ter a seguinte redação:

«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 das agências da União competentes para os efeitos previstos nos artigos 20.º e 21.º do Regulamento (UE) 2019/817. O acesso é limitado na medida em que estes dados sejam necessários para a execução das suas tarefas conformes com essas finalidades e proporcionais aos objetivos pretendidos.».

5) No artigo 9.º, ponto 4, as alíneas a) a c), passam a ter a seguinte redação:

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

a-A) Apelido de nascimento [apelido(s) anterior(es)]; local e país de nascimento; nacionalidade atual e 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;

c-A) Autoridade que emitiu o documento de viagem e a respetiva data de emissão;».

Artigo 59.º

Alteração do Regulamento (UE) 2016/399

No artigo 8.º, é inserido o seguinte número:

«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 no artigo 25.º, n.º 1 e no artigo 6.º, n.º 1 do Regulamento (UE) 2019/817 do Parlamento Europeu e do Conselho (*) se traduzir respetivamente numa ligação amarela ou numa ligação vermelha, o guarda de fronteira deve proceder à consulta do repositório comum de dados de identificação estabelecido pelo artigo 17.º, n.º 1, desse ou do SIS ou ambos para avaliar as diferenças nos dados de identificação ou nos dados do documento de viagem ligados. O guarda de fronteira deve efetuar qualquer verificação adicional necessária para tomar uma decisão sobre o estatuto e a cor da ligação.

Nos termos do artigo 69.º, n.º 1, do Regulamento (UE) n.º 2019/817, o presente número é aplicável a partir do início das operações do detetor de identidades múltiplas nos termos do artigo 72.º, n.º 4 desse regulamento.

(*) Regulamento (UE) 2019/817 do Parlamento Europeu e do Conselho, de 20 de maio de 2019, relativo à criação de um regime de interoperabilidade entre os sistemas de informação da UE no domínio das fronteiras e vistos e que altera os Regulamentos (CE) n.º 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 do Parlamento Europeu e do Conselho, e as Decisões 2004/512/CE e 2008/633/JAI do Conselho (JO L 135 de 22.5.2019, p. 27).».

Artigo 60.º

Alteração do Regulamento (UE) 2017/2226

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

1) Ao artigo 1.º, é aditado o seguinte número:

«3. Através do armazenamento dos dados de identificação, dos dados dos documentos de viagem e dos dados biométricos no repositório comum de dados de identificação (CIR) estabelecido pelo artigo 17.º, n.º 1, do Regulamento (UE) 2019/817 do Parlamento Europeu e do Conselho (*), o SES contribui para facilitar e apoiar a identificação correta das pessoas registadas no SES, nas condições e com o objetivo do artigo 20.º desse regulamento.

(*) Regulamento (UE) 2019/817 do Parlamento Europeu e do Conselho, de 20 de maio de 2019, relativo à criação de um regime de interoperabilidade entre os sistemas de informação da UE no domínio das fronteiras e vistos e que altera os Regulamentos (CE) n.º 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 do Parlamento Europeu e do Conselho, e as Decisões 2004/512/CE e 2008/633/JAI do Conselho (JO L 135 de 22.5.2019, p. 27).».

2) No artigo 3.º, o n.º 1 é alterado do seguinte modo:

a) O ponto 22 passa a ter a seguinte redação:

«22) "Dados VIS", todos os dados armazenados no sistema central do VIS e no CIR em conformidade com os artigos 15.º a 20.º;»;

b) É inserido o seguinte ponto:

«22-A) "Dados de identificação", os dados a que se refere o artigo 16.º, n.º 1, alínea a), bem como os dados relevantes referidos nos artigos 17.º, n.º 1, e 18.º, n.º 1;»;

c) São aditados os seguintes pontos:

«32) "ESP", o portal europeu de pesquisa criado pelo artigo 6.º, n.º 1, do Regulamento (UE) 2019/817;

33) "CIR", o repositório comum de dados de identificação na aceção do artigo 17.º, n.º 1, do Regulamento (UE) 2019/817.».

3) No artigo 6.º, ao n.º 1, é aditada a seguinte alínea:

«j) Garantir a identificação correta das pessoas;».

4) O artigo 7.º, é alterado do seguinte modo:

a) O n.º 1 é alterado do seguinte modo:

i) É inserida a seguinte alínea:

«a-A) A infraestrutura central do CIR a que se refere o artigo 17.º, n.º 2, alínea a), do Regulamento (UE) 2019/817»;

ii) A alínea f) passa a ter a seguinte redação:

«f) Uma infraestrutura de comunicação segura entre o sistema central do SES e as infraestruturas centrais do ESP e o CIR.»;

b) É inserido o seguinte número:

«1-A. O CIR contém os dados referidos no artigo 16.º, n.º 1, alíneas a) a d), no artigo 17.º, n.º 1, alíneas a), b) e c) e no artigo 18.º, n.ºs 1 e 2. Os restantes dados do SES são armazenados no Sistema Central do SES.».

5) Ao artigo 9.º é aditado o seguinte número:

«4. O acesso aos 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 das agências da União que são competentes para os efeitos previstos nos artigos 20.º e artigo 21.º do Regulamento (UE) 2019/817. Tal acesso deve ser limitado na medida do necessário à execução das funções das autoridades nacionais e agências da União em conformidade com as finalidades e deve ser proporcionado aos objetivos pretendidos.».

6) O artigo 21.º é alterado do seguinte modo:

a) O n.º 1 passa a ter a seguinte redação:

«1. Em caso de impossibilidade técnica de introduzir dados no Sistema Central do SES ou do CIR ou em caso de avaria do Sistema Central do SES ou do CIR, os dados referidos nos artigos 16.º a 20.º são armazenados temporariamente na IUN. Se tal não for possível, os dados são armazenados localmente de forma temporária em formato eletrónico. Em ambos os casos, os dados são introduzidos no Sistema Central do SES ou no CIR logo que a impossibilidade técnica ou a avaria tenha sido reparada. Os Estados-Membros tomam as medidas adequadas e mobilizam as infraestruturas, os equipamentos e os recursos necessários para garantir que tal armazenamento local temporário possa ser efetuado em qualquer momento e em relação a qualquer dos seus pontos de passagem de fronteira.»;

b) No n.º 2, o primeiro parágrafo passa a ter a seguinte redação:

«2. Sem prejuízo da obrigação de efetuar os controlos de fronteira segundo o Regulamento (UE) 2016/399, a autoridade de fronteiras, na situação excecional em que seja tecnicamente impossível introduzir dados tanto no sistema central do SES e do CIR, ou na IUN, e se for tecnicamente impossível armazenar temporariamente os dados localmente em formato eletrónico, deve armazenar manualmente os dados a que se referem os artigos 16.º a 20.º do presente regulamento, com exceção dos dados biométricos, e deve apor um carimbo de entrada ou de saída no documento de viagem do nacional de um país terceiro. Esses dados são introduzidos no Sistema Central do SES e no CIR logo que tecnicamente possível.».

7) O artigo 23.º é alterado do seguinte modo:

a) É inserido o seguinte número:

«2-A. Para efeitos das verificações previstas no n.º 1 do presente artigo, a autoridade responsável pelas fronteiras lança uma consulta através ESP, a fim de comparar os dados relativos ao nacional de país terceiro com os dados relevantes do SES e do VIS.»;

b) No n.º 4, o primeiro parágrafo passa a ter a seguinte redação:

«4. Sempre que a pesquisa com os dados alfanuméricos referidos no n.º 2 do presente artigo indicar que o SES não contém dados relativos ao nacional de país terceiro, sempre que a verificação do nacional de país terceiro nos termos do n.º 2 do presente artigo não tiver dado resultados, ou sempre que existirem dúvidas quanto à identidade do nacional de país terceiro, as autoridades responsáveis pelas fronteiras têm acesso aos dados para efeitos de identificação, nos termos do artigo 27.º, a fim de criar ou atualizar um processo individual em conformidade com o artigo 14.º.».

8) No artigo 32.º, é inserido o seguinte número:

«1-A. Nos casos em que as autoridades designadas lançaram uma consulta do CIR em conformidade com o artigo 22.º do Regulamento (UE) 2019/817, podem ter acesso ao SES para consulta quando as condições estabelecidas no presente artigo forem satisfeitas e quando a resposta recebida, tal como referido no artigo 22.º, n.º 2, do Regulamento (UE) 2019/817 revelar que os dados estão armazenados no SES.».

9) No artigo 33.º é inserido o seguinte número:

«1-A. Nos casos em que a Europol lançar uma consulta ao CIR em conformidade com o artigo 22.º do Regulamento (UE) 2019/817, pode ter acesso ao SES para consulta quando as condições estabelecidas no presente artigo forem satisfeitas e quando a resposta recebida, tal como referido no artigo 22.º, n.º 2, do Regulamento (UE) 2019/817 revelar que os dados estão armazenados no SES.».

10) O artigo 34.º, é alterado do seguinte modo:

a) Nos n.ºs 1 e 2, a expressão «no sistema central do SES» é substituída pela expressão «no CIR e no sistema central do SES».

b) No n.º 5, a expressão «do sistema central do SES» é substituída pela expressão «do sistema central do SES e do CIR».

11) No artigo 35.º, o n.º 7 passa a ter a seguinte redação:

«7. 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.».

12) No artigo 36.º, a expressão «do sistema central do SES» é substituída pela expressão «do sistema central do SES e do CIR».

13) O artigo 37.º, é alterado do seguinte modo:

a) O n.º 1, passa a ter a seguinte redação:

«1. A eu-LISA é responsável pelo desenvolvimento do Sistema Central do SES e do CIR, das IUN, da infraestrutura de comunicação e do canal de comunicação seguro entre o sistema central do SES e o sistema central do VIS. A eu-LISA é igualmente responsável pelo desenvolvimento do serviço Web referido no artigo 13.º e pelo repositório de dados referido no artigo 63.º, n.º 2, em conformidade com as regras pormenorizadas referidas nos artigos 13.º, n.º 7, e com as especificações e as condições adotadas nos termos do artigo 36.º, primeiro parágrafo, alíneas h) e pelo desenvolvimento do repositório de dados a que se refere o artigo 63.º, n.º 2.»;

b) No n.º 3, o primeiro parágrafo passa a ter a seguinte redação:

«3. A eu-LISA é responsável pela gestão operacional do Sistema Central do SES e do CIR, das IUN e do canal de comunicação seguro entre o sistema central do SES e o sistema central do VIS. Em cooperação com os Estados-Membros, garante que é utilizada permanentemente a melhor tecnologia disponível, sob reserva de uma análise de custo-benefício, no Sistema Central do SES e no CIR, nas IUN, na infraestrutura de comunicação, no canal de comunicação seguro entre o sistema central do SES e o sistema central do VIS, no serviço Web referido no artigo 13.º e no repositório de dados referido no artigo 63.º, n.º 2. A eu-LISA é também responsável pela gestão operacional da infraestrutura de comunicação entre o Sistema Central do SES e as IUN, pelo serviço Web referido no artigo 13.º e pelo repositório de dados referido no artigo 63.º, n.º 2.».

14) Ao artigo 46.º, n.º 1, é aditada a seguinte alínea:

«f) Uma referência à utilização do ESP para consultar o SES, tal como referido no artigo 7.º, n.º 2, do Regulamento (UE) 2019/817.».

15) O artigo 63.º é alterado do seguinte modo:

a) O n.º 2 passa a ter a seguinte redação:

«2. Para os efeitos do n.º 1 do presente artigo, a eu-LISA armazena os dados referidos nesse número no repositório central para a elaboração de relatórios e estatísticas referido no artigo 39.º do Regulamento (UE) 2019/817.».

b) Ao n.º 4, é aditado o seguinte parágrafo:

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

Artigo 61.º

Alteração do Regulamento (UE) 2018/1240

O Regulamento (UE) 2018/1240 é alterado do seguinte modo:

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

«3. Através do armazenamento dos dados de identificação e dos dados dos documentos de viagem no repositório comum de dados de identificação (CIR) estabelecido pelo artigo 17.º, n.º 1, do Regulamento (UE) 2019/817 do Parlamento Europeu e do Conselho (*), o ETIAS contribui para facilitar e apoiar a identificação correta das pessoas registadas no ETIAS, nas condições e com o objetivo do artigo 20.º desse regulamento.

(*) Regulamento (UE) 2019/817 do Parlamento Europeu e do Conselho de, 20 de maio de 2019, relativo à criação de um regime de interoperabilidade entre os sistemas de informação da UE no domínio das fronteiras e vistos e que altera os Regulamentos (CE) n.º 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 do Parlamento Europeu e do Conselho, e as Decisões 2004/512/CE e 2008/633/JAI do Conselho (JO L 135 de 22.5.2019, p. 27).».

2) Ao artigo 3.º, n.º 1, são aditadas as seguintes alíneas:

«(23) "CIR", o repositório comum de dados de identificação criado pelo artigo 17.º, n.º 1, do Regulamento (UE) 2019/817;

(24) "ESP", o portal europeu de pesquisa criado pelo artigo 6.º, n.º 1, do Regulamento (UE) 2019/817;

(25) "Sistema Central ETIAS", o Sistema Central, referido no artigo 6.º, n.º 2, alínea a), juntamente com o CIR na medida em que o CIR contém os dados referidos no artigo 6.º, n.º 2-A;

(26) "Dados de identificação", os dados a que se refere o artigo 17.º, n.º 2, alíneas a), b) e c);

(27) "Dados do documento de viagem", os dados a que se refere o artigo 17.º, n.º 2, alíneas d) e e), e o código de três letras do país emissor do documento de viagem referido no artigo 19.º, n.º 3, alínea c);».

3) Ao artigo 4.º é aditada a seguinte alínea:

«g) Contribuir para a identificação correta das pessoas;».

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

a) O n.º 2 é alterado do seguinte modo:

i) A alínea a) passa a ter a seguinte redação:

«a) Um sistema central, incluindo a lista de vigilância ETIAS a que se refere o artigo 34.º;»;

ii) É inserida a seguinte alínea:

«a-A) O CIR;»;

iii) A alínea d) passa a ter a seguinte redação:

«d) Numa infraestrutura de comunicação segura entre o sistema central e as infraestruturas centrais do ESP e o CIR;»;

b) É inserido o seguinte número:

«2-A. O CIR contém os dados de identificação e os dados dos documentos de viagem. Os restantes dados devem ser armazenados no Sistema Central.».

5) O artigo 13.º é alterado do seguinte modo:

a) É inserido o seguinte número:

«4-A. O acesso aos dados de identificação e aos documentos de viagem do ETIAS armazenados no CIR deve ser também exclusivamente reservado ao pessoal devidamente autorizado das autoridades nacionais de cada Estado-Membro e ao pessoal devidamente autorizado das agências da União que são competentes para os efeitos previstos no artigo 20.º e artigo 21.º do Regulamento (UE) 2019/817. Esse acesso deve ser limitado na medida dos dados necessários à execução das suas funções em conformidade com as finalidades e deve ser proporcionado aos objetivos pretendidos.»;

b) O n.º 5 passa a ter a seguinte redação:

«5. Cada Estado-Membro designa as autoridades nacionais competentes a que se referem os n.ºs 1, 2, 4 e 4-A do presente artigo e comunica à eu-LISA uma lista dessas autoridades, sem demora, em conformidade com o artigo 87.º, n.º 2. A lista deve indicar a finalidade para a qual o pessoal devidamente autorizado de cada autoridade tem acesso aos dados do Sistema de Informação ETIAS, em conformidade com os n.ºs 1, 2, 4 e 4-A do presente artigo.».

6) No artigo 17.º, o n.º 2, é alterado do seguinte modo:

a) A alínea a) passa a ter a seguinte redação:

«a) Apelido, nome(s) próprio(s), apelidos de nascimento, data de nascimento, local de nascimento, sexo, nacionalidade atual;»;

b) É inserida a seguinte alínea:

«a-A) País de nascimento, nome(s) próprio(s) dos progenitores;».

7) No artigo 19.º, n.º 4, a expressão «artigo 17.º, n.º 2, alínea a)» é substituída pela expressão «artigo 17.º, n.º 2, alíneas a) e a-A)».

8) O artigo 20.º é alterado do seguinte modo:

a) No n.º 2, o primeiro parágrafo passa a ter a seguinte redação:

«2. O sistema central ETIAS lança uma consulta através do ESP, a fim de comparar os dados pertinentes a que se refere o artigo 17.º, n.º 2, alíneas a), a-A), b), c), d), f), g), j), k) e m), e o artigo 17.º, n.º 8, com os dados constantes de um registo, processo ou indicação registados num processo de pedido armazenado no sistema central ETIAS, SIS; SES, VIS, Eurodac, dados da Europol e bases de dados da Interpol SLTD e TDAWN.»;

b) No n.º 4, a expressão «artigo 17.º, n.º 2, alíneas a), b), c), d), f), g), j), k) e m)» é substituída pela expressão «artigo 17.º, n.º 2, alíneas a), a-A), b), c), d), f), g), j), k) e m)»;

c) No n.º 5, a expressão «artigo 17.º, n.º 2, alíneas a), c), f), h) e i)» é substituída pela expressão «artigo 17.º, n.º 2, alíneas a), a-A), c), f), h) e i)».

9) No artigo 23.º, o n.º 1 passa a ter a seguinte redação:

«1. O sistema central ETIAS lança uma consulta através do ESP, a fim de comparar os dados pertinentes a que se refere o artigo 17.º, n.º 2, alíneas a), a-A), b) e d), com os dados constantes do SIS, a fim de determinar se o requerente é objeto de uma das seguintes indicações:

a) Indicação relativa a uma pessoa desaparecida;

b) Indicação relativa a uma pessoa procurada no âmbito de um processo judicial;

c) Indicação relativa a uma pessoa procurada para efeitos de vigilância discreta, ou de controlos específicos.».

10) No artigo 52.º, é inserido o seguinte número:

«1-A. Nos casos em que tiverem lançado uma consulta do CIR em conformidade com o artigo 22.º do Regulamento (UE) 2019/817, as autoridades designadas podem aceder aos processos de pedido armazenados no sistema central ETIAS em conformidade com o presente artigo, para consulta, quando a resposta recebida, tal como referido no n.º 2 do artigo 22.º do Regulamento (UE) 2019/817 indicar que os dados estão armazenados nos processos de pedido armazenados no sistema central ETIAS.».

11) No artigo 53.º, é inserido o seguinte número:

«1-A. Nos casos em que tiverem lançado uma consulta do CIR em conformidade com o artigo 22.º do Regulamento (UE) 2019/817, a Europol pode aceder aos processos de pedido armazenados no sistema central ETIAS em conformidade com o presente artigo, para consulta, quando a resposta recebida, tal como referido no n.º 2 do artigo 22.º do Regulamento (UE) 2019/817 indicar que os dados estão armazenados nos processos de pedido armazenados no sistema central ETIAS.»;

12) No artigo 65.º, n.º 3, quinto parágrafo, a expressão «artigo 17.º, n.º 2, alíneas a), b), d), e) e f)» é substituída pela expressão «artigo 17.º, n.º 2, alíneas a), a-A), b), d), e) e f)».

13) No artigo 69.º, n.º 1, é inserida a seguinte alínea:

«c-A) Sempre que adequado, uma referência à utilização do ESP para consultar o sistema central ETIAS, tal como referido no artigo 7.º, n.º 2, do Regulamento (UE) 2019/817.».

14) No artigo 73.º, n.º 2, a expressão «o repositório central de dados» é substituída pela expressão «o repositório central para a elaboração de relatórios e estatísticas referidos no artigo 39.º do Regulamento (UE) 2019/817, na medida em que contém dados obtidos a partir do sistema central ETIAS em conformidade com o artigo 84.º do presente regulamento.».

15) No artigo 74.º, n.º 1, o primeiro parágrafo passa a ter a seguinte redação:

«1. Após a entrada em funcionamento do ETIAS, a eu-LISA é responsável pela gestão técnica do sistema central ETIAS e das IUN. A eu-LISA também é responsável pelos ensaios técnicos necessários para o estabelecimento e a atualização das regras de verificação do ETIAS. Em cooperação com os Estados-Membros, garante que é sempre utilizada a melhor tecnologia disponível, sob reserva de uma análise de custo-benefício. A eu-LISA é também responsável pela gestão técnica das infraestruturas de comunicação entre o sistema central ETIAS e as IUN, bem como do sítio Web público, da aplicação para dispositivos móveis, do serviço de correio eletrónico, do serviço de conta segura, da ferramenta de verificação para os requerentes, da ferramenta de consentimento para requerentes, da ferramenta de avaliação para a lista de vigilância ETIAS, do portal para as transportadoras, do serviço Web e das aplicações informáticas de tratamento dos pedidos.».

16) No artigo 84.º, n.º 2, o primeiro parágrafo passa a ter a seguinte redação:

«2. Para os efeitos do n.º 1 do presente artigo, a eu-LISA armazena os dados referidos nesse número no repositório central para a elaboração de relatórios e estatísticas referido no artigo 39.º do Regulamento (UE) 2019/817. Em conformidade com o artigo 39.º, n.º 1, desseregulamento, os dados estatísticos intersistemas e os relatórios analíticos devem permitir às autoridades enumeradas no n.º 1 do presente artigo obter relatórios personalizáveis e dados estatísticos para melhorar a aplicação das regras de verificação a que se refere o artigo 33.º, melhorar a avaliação dos riscos de segurança ou de imigração ilegal ou um elevado risco de epidemia, melhorar a eficácia dos controlos nas fronteiras e ajudar a unidade central e as unidades nacionais ETIAS a tratar os pedidos de autorização de viagem.».

17) Ao artigo 84.º, n.º 4, é aditado o seguinte parágrafo:

«As estatísticas diárias devem ser conservadas no repositório central para a elaboração de relatórios e estatísticas a que se refere o artigo 39.º do Regulamento (UE) 2019/817.».

Artigo 62.º

Alteração do Regulamento (UE) 2018/1726

O Regulamento (UE) 2018/1726 é alterado do seguinte modo:

1) O artigo 12.º passa a ter a seguinte redação:

«*Artigo 12.º*

Qualidade dos dados

1. Sem prejuízo das responsabilidades dos Estados-Membros em relação aos dados introduzidos nos sistemas sob a responsabilidade operacional da Agência, esta, em estreita cooperação com os seus grupos consultivos, estabelece, para todos os sistemas sob a responsabilidade operacional da Agência, mecanismos e procedimentos automatizados de controlo da qualidade dos dados e indicadores comuns da qualidade dos dados, bem como as normas mínimas de qualidade para o armazenamento de dados, em conformidade com as disposições pertinentes dos atos jurídicos que regem esses dados e sistemas e com o artigo 37.º dos Regulamento (UE) 2019/817 (*) e (UE) 2019/818 (**) do Parlamento Europeu e do Conselho.

2. A Agência cria um repositório central contendo apenas dados anonimizados para a elaboração de relatórios e estatísticas em conformidade com o artigo 39.º dos Regulamentos (UE) 2019/817 e (UE) 2019/818, sujeitos a disposições específicas nos atos jurídicos que regem o desenvolvimento, a criação, o funcionamento e a utilização de sistemas informáticos de grande escala geridos pela Agência.

(*) Regulamento (UE) 2019/817 do Parlamento Europeu e do Conselho, de 20 de maio de 2019, relativo à criação de um regime de interoperabilidade entre os sistemas de informação da UE no domínio das fronteiras e vistos e que altera os Regulamentos (CE) n.º 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 do Parlamento Europeu e do Conselho, e as Decisões 2004/512/CE e 2008/633/JAI do Conselho (JO L 135 de 22.5.2019, p. 27).

(**) Regulamento (UE) 2019/818 do Parlamento Europeu e do Conselho, de 20 de maio de 2019, relativo à criação de um quadro para a interoperabilidade entre os sistemas de informação da UE no domínio da cooperação policial e judiciária, asilo e migração, e que altera os Regulamentos (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816 (JO L 135 de 22.5.2019, p. 85).».

2) No artigo 19.º, o n.º 1 é alterado do seguinte modo:

a) É inserida a seguinte alínea:

«e-ea) Adota os relatórios sobre o ponto da situação do desenvolvimento dos componentes de interoperabilidade, nos termos do artigo 78.º, n.º 2, do Regulamento (UE) 2019/817 e do artigo 74.º, n.º 2 do Regulamento (UE) 2019/818.».

b) A alínea f-f) passa a ter a seguinte redação:

«(f-f) Adota os relatórios sobre o funcionamento técnico do SIS, nos termos do artigo 60.º, n.º 7, do Regulamento (UE) 2018/1861 do Parlamento Europeu e do Conselho (*) e do artigo 74.º, n.º 8, do Regulamento (UE) 2018/1862 do Parlamento Europeu e do Conselho (**), do VIS, nos termos do artigo 50.º, n.º 3, do Regulamento (CE) n.º 767/2008 e do artigo 17.º, n.º 3, da Decisão 2008/633/JAI, do SES, nos termos do artigo 72.º, n.º 4, do Regulamento (UE) 2017/2226, do ETIAS, nos termos do artigo 92.º, n.º 4, do Regulamento (UE) 2018/1240 relativo ao ECRIS-TCN e à aplicação de referência ECRIS, nos termos do artigo 36.º, n.º 8 do Regulamento (UE) 2019/816 do Parlamento Europeu e do Conselho (***) dos componentes de interoperabilidade, nos termos do artigo 78.º, n.º 3, do Regulamento (UE) 2019/817 e do artigo 74.º, n.º 3 do Regulamento (UE) 2019/818;

(*) Regulamento (UE) 2018/1861 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen (SIS) no domínio dos controlos de fronteira e que altera a Convenção de Aplicação do Acordo de Schengen e altera e revoga o Regulamento (CE) n.º 1987/2006 (JO L 312 de 7.12.2018, p. 14).

(**) Regulamento (UE) 2018/1862 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen (SIS) no domínio da cooperação policial e da cooperação judiciária em matéria penal, que altera e revoga a Decisão 2007/533/JAI do Conselho e revoga o Regulamento (CE) e revoga o Regulamento (CE) n.º 1986/2006 do Parlamento Europeu e do Conselho e a Decisão 2010/261/UE da Comissão (JO L 312 de 7.12.2018, p. 56).

(***) Regulamento (UE) 2019/816 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, que cria um sistema centralizado para a determinação dos Estados-Membros que possuem informações sobre condenações de nacionais de países terceiros e de apátridas tendo em vista completar e apoiar o Sistema Europeu de Informação sobre Registos Criminais (ECRIS-TCN) e que altera o Regulamento (UE) 2018/1726 (JO L 135 de 22.5.2019, p. 1).»;

c) A alínea h-h) passa a ter a seguinte redação:

«h-h) Adota observações formais sobre os relatórios da Autoridade Europeia para a Proteção de Dados em matéria de auditoria, nos termos do artigo 56.º, n.º 2, do Regulamento (UE) 2018/1861, do artigo 42.º, n.º 2, do Regulamento (CE) n.º 767/2008, do artigo 31.º, n.º 2, do Regulamento (UE) n.º 603/2013, do artigo 56.º, n.º 2, do Regulamento (UE) 2017/226, do artigo 67.º do Regulamento (UE) 2018/1240, do artigo 29.º, n.º 2, do Regulamento (UE) 2019/816 e do artigo 52.º dos Regulamentos (UE) 2019/817 e (UE) 2019/818, e assegura que seja dado o adequado seguimento a essas auditorias;».

d) A alínea m-m) passa a ter a seguinte redação:

«m-m) Assegura a publicação anual da lista das autoridades competentes autorizadas a consultar diretamente os dados no SIS, nos termos do artigo 41.º, n.º 8, do Regulamento (UE) 2018/1861 e do artigo 56.º, n.º 7, do Regulamento (UE) 2018/1862, juntamente com a lista dos gabinetes dos sistemas nacionais do SIS (N. SIS) e dos gabinetes SIRENE, em conformidade com o artigo 7.º, n.º 3, do Regulamento (UE) 2018/1861 e o artigo 7.º, n.º 3, do Regulamento (UE) 2018/1862, respetivamente, bem como a lista de autoridades competentes, nos termos do artigo 65.º, n.º 2, do Regulamento (UE) 2017/2226, a lista de autoridades competentes nos termos do artigo 87.º, n.º 2, do Regulamento (UE) 2018/1240, a lista de autoridades centrais nos termos do artigo 34.º, n.º 2, do Regulamento (UE) 2019/816 e a lista de autoridades nos termos do artigo 71.º, n.º 1, do Regulamento (UE) 2019/817 e o artigo 67.º, n.º 1, do Regulamento (UE) 2019/818.»;

3) No artigo 22. .º, o n. .º 4 passa a ter a seguinte redação:

«4. A Europol e a Eurojust podem participar nas reuniões do Conselho de Administração com o estatuto de observador, quando da ordem de trabalhos conste qualquer questão relativa ao SIS II relacionada com a aplicação da Decisão 2007/533/JAI.

A Agência Europeia da Guarda de Fronteiras e Costeira pode participar nas reuniões do Conselho de Administração com o estatuto de observador, quando da ordem de trabalhos conste qualquer questão relativa ao SIS relacionada com a aplicação do Regulamento (UE) 2016/1624.

A Europol também pode participar nas reuniões do Conselho de Administração com o estatuto de observador, quando da ordem de trabalhos conste qualquer questão relativa ao VIS relacionada com a aplicação da Decisão 2008/633/JAI, ou qualquer questão relativa ao Eurodac relacionada com a aplicação do Regulamento (UE) n.º 603/2013.

A Europol também pode participar nas reuniões do Conselho de Administração com o estatuto de observador, quando da ordem de trabalhos conste qualquer questão relativa ao SES relacionada com a aplicação do Regulamento (UE) 2017/2226 ou uma questão relativa ao ETIAS relacionada com o Regulamento (UE) 2018/1240.

A Agência Europeia da Guarda de Fronteiras e Costeira também pode participar nas reuniões do Conselho de Administração com o estatuto de observador, quando da ordem de trabalhos conste qualquer questão relativa ao ETIAS relacionada com aplicação do Regulamento (UE) 2018/1240.

A Eurojust, a Europol e a Procuradoria Europeia também podem participar nas reuniões do Conselho de Administração com o estatuto de observador, quando da ordem de trabalhos conste qualquer questão relativa ao Regulamento (UE) 2019/816.

A Europol, a Eurojust e a Agência Europeia da Guarda de Fronteiras e Costeira também podem participar nas reuniões do Conselho de Administração com o estatuto de observador, quando da ordem de trabalhos conste qualquer questão relativa ao Regulamento (UE) 2019/817 e (UE) 2019/818.

O Conselho de Administração pode convidar qualquer outra pessoa, cuja opinião possa ser útil, a participar nas suas reuniões com o estatuto de observador.».

4) No artigo 24.º, n.º 3, a alínea p) passa a ter a seguinte redação:

«(p) Sem prejuízo do disposto no artigo 17.º do Estatuto dos Funcionários, o estabelecimento das normas de confidencialidade, em cumprimento do disposto no artigo 17.º do Regulamento (CE) n.º 1987/2006, no artigo 17.º da Decisão 2007/533/JAI, no artigo 26.º, n.º 9, do Regulamento (CE) n.º 767/2008 e no artigo 4.º, n.º 4, do Regulamento (UE) n.º 603/2013; no artigo 37.º, n.º 4, do Regulamento (UE) 2017/2226, no artigo 74.º, n.º 2, do Regulamento (UE) 2018/1240, no artigo 11.º, n.º 16, do Regulamento (UE) 2019/816 e no artigo 55.º, n.º 2, dos Regulamentos (UE) 2019/817 e (UE) 2019/818;».

5) O artigo 27.º, é alterado do seguinte modo:

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

«d-a) Grupo Consultivo da Interoperabilidade;».

b) O n.º 3 passa a ter a seguinte redação:

«3. A Europol e a Eurojust e a Agência Europeia da Guarda de Fronteiras e Costeira podem, cada uma, nomear um representante para o Grupo Consultivo do SIS II.

A Europol pode nomear também um representante para os Grupos Consultivos do VIS e do Eurodac e do SES-ETIAS.

A Agência Europeia da Guarda de Fronteiras e Costeira pode nomear também um representante para o Grupo Consultivo do SES-ETIAS.

A Eurojust, e a Europol e a Procuradoria Europeia podem nomear também um representante para o Grupo Consultivo do Sistema ECRIS-NPT.

A Europol, a Eurojust e a Agência Europeia da Guarda de Fronteiras e Costeira podem, cada uma, nomear um representante para o Grupo Consultivo da Interoperabilidade.».

Artigo 63.º

Alteração do Regulamento (UE) 2018/1861

O Regulamento (UE) 2018/1861 é alterado do seguinte modo:

1) Ao artigo 3.º, são aditados os seguintes pontos:

«(22) "ESP", o portal europeu de pesquisa estabelecido pelo artigo 6.º, n.º 1, do Regulamento (UE) 2019/817 do Parlamento Europeu e do Conselho (*).

(23) "BMS", o serviço partilhado de correspondências biométricas estabelecido pelo artigo 12.º, n.º 1, do Regulamento (UE) 2019/817.

(24) "CIR", o repositório comum de dados de identificação estabelecido pelo artigo 17.º, n.º 1, do Regulamento (UE) 2019/817;

(25) "MID", o detetor de identidades múltiplas estabelecido pelo 25.º, n.º 1, do Regulamento (UE) 2019/817.

(*) Regulamento (UE) 2019/817 do Parlamento Europeu e do Conselho, de 20 de maio de 2019, relativo à criação de um regime de interoperabilidade entre os sistemas de informação da UE no domínio das fronteiras e vistos e que altera os Regulamentos (CE) n.º 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 do Parlamento Europeu e do Conselho, e as Decisões 2004/512/CE e 2008/633/JAI do Conselho (JO L 135 de 22.5.2019, p. 27).».

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

a) No n.º 1, as alíneas b) e c) passam a ter a seguinte redação:

«b) Um sistema nacional (N.SIS) em cada Estado-Membro, constituído pelos sistemas de dados nacionais que comunicam com o SIS Central, e que inclui, pelo menos, um N.SIS de salvaguarda nacional ou partilhado;

c) Uma infraestrutura de comunicação entre o CS-SIS, o CS-SIS de salvaguarda e a NI-SIS ("infraestrutura de comunicação") que proporciona uma rede virtual cifrada dedicada aos dados do SIS e ao intercâmbio de dados entre os Gabinetes SIRENE a que se refere o artigo 7.º, n.º 2; e

d) Uma infraestrutura de comunicação segura entre o CS-SIS e as infraestruturas centrais do ESP, do BMS e do MID.».

b) São aditados os seguintes números:

«8. Sem prejuízo do disposto nos n.ºs 1 a 5, os dados do SIS podem também ser consultados através do ESP.

9. Sem prejuízo do disposto nos n.ºs 1 a 5, os dados do SIS podem também ser transmitidos pela infraestrutura de comunicação segura definida no n.º 1, alínea d). Essas transmissões devem cingir-se aos dados necessários para os efeitos referidos no Regulamento (UE) 2019/817.».

3) No artigo 7.º, é inserido o seguinte número:

«2-A. O gabinete SIRENE assume também a verificação manual das diferentes identidades em conformidade com o artigo 29.º do Regulamento (UE) 2019/817. Na medida do necessário para executar esta tarefa, os gabinetes SIRENE devem ter acesso aos dados armazenados no CIR e no MID para os efeitos previstos nos artigos 21.º e 26.º do Regulamento (UE) 2019/817.».

4) No artigo 12.º, o n.º 1 passa a ter a seguinte redação:

«1. Os Estados-Membros devem garantir que todos os acessos e todos os intercâmbios de dados pessoais no âmbito do CS-SIS fiquem documentados no N.SIS, a fim de verificar a legalidade da consulta e a legalidade do tratamento de dados, proceder ao autocontrolo e assegurar o bom funcionamento do N.SIS, bem como a integridade e a segurança dos dados. Este requisito não é aplicável aos processos automáticos a que se refere o artigo 4.º, n.º 6, alíneas, a), b) e c);

Os Estados-Membros devem garantir que todos os acessos a dados pessoais pelo ESP fiquem também documentados, a fim de verificar a legalidade da consulta e a legalidade do tratamento de dados, proceder ao autocontrolo e assegurar a integridade e a segurança dos dados.».

5) Ao artigo 34.º, n.º 1, é aditada a seguinte alínea:

«g) Verificação das diferentes identidades e luta contra a fraude de identidade, em conformidade com o capítulo V do Regulamento (UE) 2019/817.».

6) No artigo 60. .º, o n. .º 6 passa a ter a seguinte redação:

«6. Para os efeitos do artigo 15.º, n.º 4 e dos n.ºs 3, 4 e 5 do presente artigo, a eu-LISA deve armazenar os dados a que se refere o artigo 15.º, n.º 4 e o n.º 3 do presente artigo, que não permitam a identificação de pessoas no repositório central para a elaboração de relatórios e estatísticas referido no artigo 39.º do Regulamento (UE) 2019/817.

A Agência permite que a Comissão e os organismos referidos no n.º 5 do presente artigo obtenham relatórios e estatísticas específicas. Mediante pedido, a eu-LISA confere acesso ao repositório central para obtenção de relatórios e estatísticas nos termos do artigo 39.º do Regulamento (UE) 2019/817 aos Estados-Membros, à Comissão, à Europol e à Agência Europeia da Guarda de Fronteiras e Costeira.».

Artigo 64.º

Alteração da Decisão 2004/512/CE

No artigo 1.º da Decisão 2004/512/CE do Conselho o n.º 2, passa a ter a seguinte redação:

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

a) Numa infraestrutura central de repositório comum de dados de identificação, a que se refere o artigo 17.º, n.º 2, alínea a), do Regulamento (UE) 2019/817 do Parlamento Europeu e do Conselho (*);

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, n.º 1, do Regulamento (UE) 2019/817 e o repositório comum de dados de identificação estabelecido pelo artigo 17.º, n.º 1, do Regulamento (UE) 2019/817.

(*) Regulamento (UE) 2019/817 do Parlamento Europeu e do Conselho, de 20 de maio de 2019, que estabelece um quadro para a interoperabilidade entre os sistemas de informação da UE no domínio das fronteiras e vistos e que altera os Regulamentos (CE) n.º 767/2008, (UE) 2016/399(UE) 2017/2226(UE) 2018/1240, (UE) 2018/1726, (UE) 2018/1861 e as Decisões 2004/512/CE e 2008/633/JAI do Conselho (JO L 135 de 22.5.2019, p. 27).»

Artigo 65.º

Alteração da Decisão 2008/633/JAI

A Decisão 2008/633/JAI é alterada do seguinte modo:

1) No artigo 5.º, é inserido o seguinte número:

«1-A. Nos casos em que as autoridades designadas tiverem lançado uma consulta do repositório comum de dados de identificação CIR em conformidade com o artigo 22.º do Regulamento (UE) 2019/817 do Parlamento Europeu e do Conselho (*), e quando as condições de acesso estabelecidas no presente artigo forem satisfeitas, podem aceder ao VIS para consulta quando a resposta recebida, tal como referido no n.º 2 do artigo 22.º desse regulamento revelar que os dados estão armazenados no VIS.

(*) Regulamento (UE) 2019/817 do Parlamento Europeu e do Conselho, de 20 de maio de 2019, relativo à criação de um regime de interoperabilidade entre os sistemas de informação da UE no domínio das fronteiras e vistos e que altera os Regulamentos (CE) n.º 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 do Parlamento Europeu e do Conselho, e as Decisões 2004/512/CE e 2008/633/JAI do Conselho (JO L 135 de 22.5.2019, p. 27).»

2) No artigo 7.º é inserido o seguinte número:

«1-A. Nos casos em que a Europol tiver lançado uma consulta do CIR em conformidade com o artigo 22.º do Regulamento (UE) 2019/817, e quando as condições de acesso estabelecidas no presente artigo forem satisfeitas, a Europol pode aceder ao VIS para consulta quando a resposta recebida, tal como referido no artigo 22.º, n.º 3, desse regulamento revelar que os dados estão armazenados no VIS.».

CAPÍTULO X

Disposições finais

Artigo 66.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 ESP, unicamente para efeitos da elaboração de relatórios e estatísticas:

a) Número de consultas por utilizador do perfil ESP;

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

Os dados não podem permitir a identificação de pessoas.

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 CIR, unicamente para efeitos da elaboração de relatórios e estatísticas:

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

b) Nacionalidade, género 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.

Os dados não podem permitir a identificação de pessoas.

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 MID unicamente para efeitos da elaboração de relatórios e estatísticas:

a) Número de consultas efetuadas com e sem dados biométricos;

b) Número de cada tipo de ligação e sistemas de informação da União com os dados da ligação;

c) Período de tempo durante o qual uma ligação amarela e vermelha permaneceu no sistema.

Os dados não podem permitir a identificação de pessoas.

4. O pessoal devidamente autorizado da Agência Europeia da Guarda de Fronteiras e Costeira, deve ter acesso ao sistema para consultar os dados referidos nos n.os 1, 2 e 3 do presente artigo, para efeitos de realização de análises de risco e avaliações da vulnerabilidade, tal como referido nos artigos 11.º e 13.º do Regulamento (UE) 2016/1624 do Parlamento Europeu e do Conselho ([40]).

5. O pessoal devidamente autorizado da Europol tem acesso ao sistema para consultar os dados a que se referem os n.os 2 e 3, do presente artigo, para efeitos de realização de análises estratégicas, temáticas e operacionais referidas no artigo 18.º, n.º 2, alíneas b) e c), do Regulamento (UE) 2016/794.

6. Para efeitos dos n.os 1, 2 e 3, a eu-LISA deve conservar os dados referidos nesses números no CRRS. Os dados incluídos do CRRS não podem permitir a identificação de pessoas, mas devem permitir às autoridades enumeradas nos n.os 1, 2 e 3 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.

7. A pedido, a Comissão disponibiliza informações relevantes à Agência da União Europeia dos Direitos Fundamentais, a fim de avaliar o impacto do presente regulamento nos direitos fundamentais.

Artigo 67.º

Período transitório aplicável à utilização do portal europeu de pesquisa

1. Durante um prazo 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.

2. Se uma avaliação da aplicação do ESP mostrar que é necessário prorrogar o prazo a que se refere o n.º 1 do presente artigo, em especial devido ao impacto da introdução do ESP na organização e na duração dos controlos de fronteira, a Comissão fica habilitada a adotar um ato delegado, nos termos do artigo 73.º, a fim de alterar o presente regulamento, prorrogando esse prazo uma única vez, por um período não superior a um ano.

Artigo 68.º

Período transitório aplicável às disposições relativas ao acesso ao repositório comum de dados de identificação para efeitos de prevenção, deteção ou investigação de infrações terroristas ou outras infrações penais graves

O artigo 22.º, o artigo 60.º, pontos 8 e 9, o artigo 61.º, pontos, 10 e 11 e o artigo 65.º, aplicam-se a partir da data de início das operações do CIR a que se refere o artigo 72.º, n.º 3.

([40]) 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).

Artigo 69.º

Período transitório aplicável à 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 72.º, n.º 4, alínea b) e antes do início do funcionamento do MID, a unidade central do ETIAS é responsável por efetuar uma deteção de identidades múltiplas usando os dados armazenados no SES, no VIS, no Eurodac e no SIS. As deteções de identidades múltiplas devem ser efetuadas utilizando apenas os dados biométricos.

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

Se a consulta detetar uma ou várias correspondências s 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 correspondências s, deve ser criada uma ligação para cada elemento de dados que desencadeou a correspondência.

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

4. Quando for criada uma ligação a uma indicação no SIS que não seja um alerta nos termos do artigo 3.o do Regulamento (UE) 2018/1860, dos artigos 24.o e 25.o do Regulamento (UE) 2018/1861 ou do artigo 38.o do Regulamento (UE) 2018/1862, o MID deve facultar ao gabinete SIRENE do Estado-Membro que criou a indicação acesso aos dados de identificação presentes nos diferentes sistemas de informação.

5. A unidade central ETIAS ou, nos casos previstos no n.º 4 do presente artigo, 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 unidade central do ETIAS notifica apenas a Comissão, em conformidade com o artigo 71.º, n.º 3, logo que todas as ligações amarelas tenham sido verificadas manualmente e o seu estado tenha sido atualizado em ligações verdes, brancas ou vermelhas.

7. Os Estados-Membros devem apoiar a unidade central ETIAS, se for caso disso, na realização da deteção de identidades múltiplas referida no presente artigo.

8. A Comissão fica habilitada a adotar um ato delegado, nos termos do artigo 73.º, para alterar o presente regulamento e prorrogar o prazo referido no n.º 1 do presente artigo por um período de seis meses, renovável duas vezes por seis meses de cada vez. Essa prorrogação só é concedida se uma avaliação do prazo previsto para a conclusão da deteção de identidades múltiplas a que se refere o presente artigo evidenciar que a deteção de identidades múltiplas não pode ser concluída antes do termo do período previsto no n.º 1 ou da eventual prorrogação por razões alheias à vontade da unidade central do ETIAS e que não podem ser aplicadas quaisquer medidas corretivas. Essa avaliação é realizada o mais tardar três meses antes do termo desse prazo ou do prazo da prorrogação em curso.

Artigo 70.º

Custos

1. Os custos decorrentes da criação e funcionamento do ESP, do serviço partilhado BMS, do CIR e do MID ficam a cargo do 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. Sem prejuízo de outro financiamento para este efeito a partir de outras fontes do orçamento geral da União Europeia, será mobilizado um montante de 32 077 000 EUR a partir da dotação de 791 000 000 EUR prevista no artigo 5.º, n.º 5, alínea b), do Regulamento (UE) n.º 515/2014, para cobrir os custos de aplicação do presente regulamento, tal como previsto nos n.ºs 1 e 2 do presente artigo.

4. A partir do montante referido no n.º 3, 22 861 000 EUR são atribuídos à eu-LISA, 9 072 000 EUR são atribuídos à Europol e 144 000 EUR à Agência da União Europeia para a Formação Policial (CEPOL), para apoiar estas agências no desempenho das respetivas funções, em conformidade com o presente regulamento. Esse financiamento é executado em regime de gestão indireta.

5. Os custos incorridos pelas autoridades designadas são suportados por cada Estado-Membro e pela Europol respetivamente. Os custos da ligação das autoridades designadas ao CIR são suportados por cada Estado-Membro e pela Europol.

As despesas incorridas pela Europol, incluindo as relacionadas com o CIR, são suportadas pela Europol.

Artigo 71.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 72.º. Em caso de alterações da 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 72.º, n.º 1, alínea b), artigo 72.º, n.º 2, alínea b), artigo 72.º, n.º 3, alínea b), artigo 72.º, n.º 4 alínea b), artigo 72.º, n.º 5, alínea b) e artigo 72.º, n.º 6 alínea b).

3. A unidade central ETIAS deve notificar à Comissão a conclusão com êxito do período transitório estabelecido no artigo 69.º.

4. A Comissão deve disponibilizar as informações comunicadas nos termos do n.º 1 aos Estados-Membros e ao público, através de um sítio público constantemente atualizado.

Artigo 72.º

Início das operações

1. A Comissão deve fixar a data a partir da qual o ESP entra em funcionamento por meio de um ato de execução, logo que estejam preenchidas 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, e o artigo 43.º, n.º 5;

b) A eu-LISA tiver declarado a conclusão com êxito de um teste global do ESP, que deve ser efetuado pela eu-LISA em cooperação com as autoridades dos Estados-Membros e as agências da União suscetíveis de utilizar o ESP;

c) A eu-LISA tiver validado as disposições técnicas e jurídicas para a recolha e transmissão dos dados a que se referem o artigo 8.º, n.º 1, e procedido à notificação da Comissão;

O ESP só pode consultar as bases de dados da Interpol se as disposições técnicas permitirem o cumprimento dos requisitos referidos no artigo 9.º, n.º 5. A impossibilidade de cumprimento desse artigo implica que o ESP não pode consultar as bases de dados da Interpol, mas não pode atrasar o início das operações do ESP.

A Comissão fixa a data a que se refere o primeiro parágrafo, que não pode ser posterior a 30 dias após a data de adoção do ato de execução.

2. A Comissão deve fixar a data a partir da qual o serviço partilhado BMS entra em funcionamento, por meio de um ato de execução, logo que estejam preenchidas as seguintes condições:

a) Tiverem sido adotadas as medidas a que se referem o artigo 13.º, n.º 5, e o artigo 43.º, n.º 5;

b) A eu-LISA tiver declarado a conclusão com êxito de um teste global do BMS, a realizar pela eu-LISA em cooperação com as autoridades dos Estados-Membros;

c) A eu-LISA tiver validado as disposições técnicas e jurídicas para a recolha e transmissão dos dados nos termos do artigo 13.º e procedido à notificação da Comissão;

d) A eu-LISA tiver notificado a conclusão com êxito do teste referido no n.º 5, alínea b).

A Comissão fixa a data a que se refere o primeiro parágrafo, que não pode ser posterior a 30 dias após a data de adoção do ato de execução.

3. A Comissão deve fixar a data a partir da qual o CIR entra em funcionamento, por meio de um ato de execução, logo que estejam preenchidas as seguintes condições:

a) Tiverem sido adotadas as medidas a que se referem o artigo 43, n.º 5, e o artigo 78.º, n.º 10;

b) A eu-LISA tiver declarado a conclusão com êxito de um teste global do CIR, a realizar em cooperação com as autoridades dos Estados-Membros;

c) A eu-LISA tiver validado as disposições técnicas e jurídicas para a recolha e transmissão dos dados a que se refere o artigo 18.º e procedido à notificação da Comissão;

d) A eu-LISA tiver notificado a conclusão com êxito do teste referido no n.º 5, alínea b).

A Comissão fixa a data a que se refere o primeiro parágrafo, que não pode ser posterior a 30 dias após a data de adoção do ato de execução.

4. A Comissão deve fixar a data a partir da qual o MID entra em funcionamento, por meio de um ato de execução, logo que estejam preenchidas as seguintes condições:

a) Tiverem sido adotadas as medidas a que se referem o artigo 28.º, n.º 5 e n.º 7, o artigo 32.º, n.º 5, o artigo 33.º, n.º 6, o artigo 43.º, n.º 5, e o artigo 49.º, n.º 6;

b) A eu-LISA tiver declarado a conclusão com êxito de um teste global do MID, que deve ser efetuado pela eu-LISA em cooperação com as autoridades dos Estados-Membros e a unidade central do ETIAS;

c) A eu-LISA tiver validado as disposições técnicas e jurídicas para a recolha e transmissão dos dados previstos no artigo 34.º e procedido à notificação da Comissão;

d) A unidade central ETIAS tiver notificado a Comissão, nos termos do artigo 71.º, n.º 3;

e) A eu-LISA tiver declarado a conclusão com êxito dos testes referidos no n.º 1, alínea b), no n.º 2, alínea b), no n.º 3, alínea b) e no n.º 5, alínea b).

A Comissão fixa a data a que se refere o primeiro parágrafo, que não pode ser posterior a 30 dias após a data de adoção do ato de execução.

5. A Comissão deve fixar por meio de atos de execução a data a partir da qual os mecanismos e procedimentos automatizados de controlo da qualidade, os indicadores comuns de qualidade dos dados e as normas mínimas de qualidade devem ser utilizados, logo que estejam preenchidas as seguintes condições:

a) Tiverem sido adotadas as medidas previstas no artigo 37.º, n.º 4;

b) A eu-LISA tiver declarado a conclusão com êxito de um teste global dos mecanismos e procedimentos automatizados de controlo da qualidade, dos indicadores comuns de qualidade dos dados e das normas mínimas de qualidade, que deve ser efetuado em cooperação com as autoridades dos Estados-Membros.

A Comissão fixa a data a que se refere o primeiro parágrafo, que não pode ser posterior a 30 dias após a data de adoção do ato de execução.

6. A Comissão deve fixar a data a partir da qual o CRRS entra em funcionamento, por meio de um ato de execução, logo que estejam preenchidas as seguintes condições:

a) Tiverem sido adotadas as medidas previstas no artigo 39.º, n.º 5, e no artigo 43.º, n.º 5;

b) A eu-LISA tiver declarado a conclusão com êxito de um teste global do CRRS, a realizar pela eu-LISA em cooperação com as autoridades dos Estados-Membros;

c) A eu-LISA tiver validado as disposições técnicas e jurídicas para a recolha e transmissão dos dados a que se refere o artigo 39.º e procedido à notificação da Comissão.

A Comissão fixa a data a que se refere o primeiro parágrafo, que não pode ser posterior a 30 dias após a data de adoção do ato de execução.

7. A Comissão deve informar o Parlamento Europeu e o Conselho dos resultados dos testes efetuados nos termos do n.º 1, alínea b), o n.º 2, alínea b), o n.º 3, alínea b), o n.º 4, alínea b), o n.º 5, alínea b) e o n.º 6, alínea b).

8. Os Estados-Membros, a unidade central ETIAS e a Europol devem começar a utilizar os componentes de interoperabilidade a partir da data determinada pela Comissão nos termos dos n.ºs 1, 2, 3 e 4, respetivamente.

Artigo 73.º

Exercício da delegação

1. O poder de adotar atos delegados é conferido à Comissão nas condições estabelecidas no presente artigo.

2. O poder de adotar atos delegados referido no artigo 28.º, n.º 5, no artigo 39.º, n.º 5, no artigo 49.º, n.º 6, no artigo 67.º, n.º 2, e no artigo 69.º, n.º 8, é conferido à Comissão por um prazo de cinco anos a contar de 11 de junho de 2019. A Comissão elabora um relatório relativo à delegação de poderes pelo menos nove meses antes do final do prazo de cinco anos. A delegação de poderes é tacitamente prorrogada por períodos de igual duração, salvo se o Parlamento Europeu ou o Conselho a tal se opuserem pelo menos três meses antes do final de cada prazo.

3. A delegação de poderes referida no artigo 28.º, n.º 5, no artigo 39.º, n.º 5, no artigo 49.º, n.º 6, no artigo 67.º, n.º 2, e no artigo 69.º, n.º 8 pode ser revogada em qualquer momento pelo Parlamento Europeu ou pelo Conselho. A decisão de revogação põe termo à delegação dos poderes nela especificados. A decisão de revogação produz efeitos a partir do dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia* ou de uma data posterior nela especificada. A decisão de revogação não afeta os atos delegados já em vigor.

4. Antes de adotar um ato delegado, a Comissão consulta os peritos designados por cada Estado-Membro de acordo com os princípios estabelecidos no Acordo Interinstitucional, de 13 de abril de 2016, legislar melhor.

5. Assim que adotar um ato delegado, a Comissão notifica-o simultaneamente ao Parlamento Europeu e ao Conselho.

6. Os atos delegados adotados nos termos do artigo 28.º, n.º 5, no artigo 39.º, n.º 5, no artigo 49.º, n.º 6, no artigo 67.º, n.º 2, e no artigo 69.º, n.º 8 só entram em vigor se não tiverem sido formuladas objeções pelo Parlamento Europeu ou pelo Conselho no prazo de quatro meses a contar da notificação do ato ao Parlamento Europeu e ao Conselho, ou se, antes do termo desse prazo, o Parlamento Europeu e o Conselho tiverem informado a Comissão de que não têm objeções a formular. O referido prazo é prorrogável por dois meses por iniciativa do Parlamento Europeu ou do Conselho.

Artigo 74.º

Procedimento de comité

1. A Comissão é assistida por um comité. Este comité é um comité na aceção do Regulamento (UE) n.º 182/2011.

2. Caso se remeta para o presente número, aplica-se o artigo 5.º do Regulamento (UE) n.º 182/2011.

Na falta de parecer do comité, a Comissão não adota o projeto de ato de execução, aplicando-se o artigo 5.º, n.º 4, terceiro parágrafo, do Regulamento (UE) n.º 182/2011.

Artigo 75.º

Grupo consultivo

A eu-LISA deve criar um grupo consultivo de interoperabilidade. Durante a fase de conceção e desenvolvimento dos componentes de interoperabilidade, deve aplicar-se o artigo 54.º, n.ºs 4, 5 e 6.

Artigo 76.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 2018/1726.

As autoridades dos Estados-Membros e as agências da União devem ministrar ao seu pessoal autorizado a tratar dados dos componentes de interoperabilidade um programa de formação adequado sobre a segurança dos dados, a qualidade dos dados, as regras em matéria de proteção de dados, os procedimentos relativos ao tratamento dos dados e as obrigações de informação nos termos do artigo 32.º, n.º 4, 33.º, n.º 4 e do artigo 47.º.

Se for caso disso, devem ser organizados, a nível da União, cursos de formação comuns sobre estes temas para reforçar a cooperação e o intercâmbio de boas práticas entre o pessoal das autoridades dos Estados-Membros e os organismos da União que estão autorizadas a tratar dados dos componentes de interoperabilidade. Deve ser dada especial atenção ao processo de deteção de identidades múltiplas, incluindo a verificação das ligações e a necessidade concomitante de garantir as salvaguardas em relação aos direitos fundamentais.

Artigo 77.º

Manual prático

A Comissão, em estreita cooperação com os Estados-Membros, com a eu-LISA e com outras agências da União competentes, 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 78.º

Acompanhamento e avaliação

1. A eu-LISA deve assegurar que são criados procedimentos para acompanhar o desenvolvimento de componentes de interoperabilidade e a ligação à interface uniforme nacional 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 12 de dezembro de 2019 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 e da sua ligação à interface uniforme nacional. Quando a fase de desenvolvimento estiver concluída, 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. Quatro anos após o início do funcionamento de cada componente de interoperabilidade nos termos do artigo 72.º 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.

4. Além disso, um ano após cada relatório da eu-LISA, a Comissão deve apresentar uma avaliação global dos componentes de interoperabilidade, incluindo uma:

a) Avaliação da aplicação do presente regulamento;

b) Uma análise dos resultados obtidos comparativamente aos objetivos fixados pelo presente regulamento e ao impacto nos direitos fundamentais, incluindo, em particular, uma avaliação do impacto dos componentes de interoperabilidade no direito à não discriminação;

c) Avaliação do funcionamento do portal Web, incluindo os dados relativos à utilização do portal Web e ao número de pedidos que foram resolvidos;

d) Avaliação da continuidade da validade dos princípios subjacentes aos componentes de interoperabilidade;

e) Avaliação da segurança dos componentes de interoperabilidade;

f) Avaliação da utilização do CIR para fins de identificação;

g) Avaliação da utilização do CIR para efeitos de prevenção, deteção ou investigação de infrações terroristas ou outras infrações penais graves;

h) 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 geral da União;

i) Avaliação da consulta das bases de dados da Interpol através do ESP, incluindo informações sobre o número de correspondências positivas a consultas das bases de dados da Interpol e sobre quaisquer problemas encontrados.

A avaliação global a que se refere o primeiro parágrafo do presente número devem incluir quaisquer recomendações necessárias. A Comissão deve transmitir a avaliação ao Parlamento Europeu, ao Conselho, à Autoridade Europeia para a Proteção de Dados e à Agência dos Direitos Fundamentais da União Europeia.

5. Até 12 de junho de 2020 e todos os anos após essa data até à adoção de atos de execução da Comissão a que se refere o artigo 72.º, a Comissão apresenta ao Parlamento Europeu e ao Conselho um relatório sobre o ponto da situação dos preparativos para a plena execução do presente regulamento. Esse relatório deve também conter informações pormenorizadas sobre os custos incorridos e informações sobre quaisquer riscos que possam ter um impacto sobre os custos globais.

6. Dois anos após o início do funcionamento do MID nos termos do artigo 72.º, n.º 4, a Comissão deve proceder a uma análise do impacto do MID no direito à não discriminação. Na sequência desse primeiro relatório, a análise do impacto do MID no direito à não discriminação deve fazer parte do exame referido no n.º 4, alínea b), do presente artigo.

7. Os Estados-Membros e a Europol devem fornecer à eu-LISA e à Comissão as informações necessárias para a elaboração dos relatórios referidos nos n.os 3 a 6. 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.

8. A eu-LISA deve comunicar à Comissão as informações necessárias à elaboração das avaliações referidas no n.º 4.

9. Respeitando as disposições de direito nacional sobre a publicação de informações sensíveis, e sem prejuízo das limitações necessárias para proteger a segurança e a ordem pública, prevenir a criminalidade e garantir que qualquer investigação nacional não seja posta em causa, cada Estado-Membro e a Europol devem elaborar relatórios anuais sobre a eficácia do acesso aos dados armazenados no CIR para efeitos de prevenção, deteção ou investigação de infrações terroristas ou outros crimes graves, contendo informações e estatísticas sobre:

a) As finalidades exatas da consulta, incluindo o tipo de infração terrorista ou outro crime grave;

b) Motivos razoáveis de suspeita fundamentada de que o suspeito, autor ou vítima está abrangido pelo Regulamento (UE) 2017/2226, o Regulamento (CE) n.º 767/2008 ou o Regulamento (UE) 2018/1240;

c) O número de pedidos de acesso ao CIR para efeitos de prevenção, deteção ou investigação de infrações terroristas ou outros crimes graves;

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 posterior realizada pelo ponto central de acesso.

Os relatórios anuais elaborados pelos Estados-Membros e pela Europol devem ser transmitidos à Comissão até 30 de junho do ano seguinte.

10. É disponibilizada aos Estados-Membros uma solução técnica para gerir os pedidos de acesso dos utilizadores referidos no artigo 22.º e facilitar a recolha dos dados enumerados nos n.os 7 e 9, do presente artigo, para efeitos de produção de relatórios e de estatísticas referidas nesses números. A Comissão adota atos de execução relativos às especificações da solução técnica. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 74.º, n.º 2.

Artigo 79.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*.

As disposições do presente regulamento relacionadas com o ESP, são aplicáveis a partir da data fixada pela Comissão nos termos do artigo 72.º, n.º 1.

As disposições do presente regulamento relacionadas com o serviço partilhado BMS, são aplicáveis a partir da data fixada pela Comissão nos termos do artigo 72.º, n.º 2.

As disposições do presente regulamento relacionadas com o CIR, são aplicáveis a partir da data fixada pela Comissão nos termos do artigo 72.º, n.º 3.

As disposições do presente regulamento relacionadas com o MID, são aplicáveis a partir da data fixada pela Comissão nos termos do artigo 72.º, n.º 4.

As disposições do presente regulamento relacionadas com os mecanismos e procedimentos automatizados de controlo da qualidade dos dados, os indicadores comuns de qualidade dos dados e as normas mínimas de qualidade, são aplicáveis a partir da data fixada pela Comissão nos termos do artigo 72.º, n.º 5.

As disposições do presente regulamento relacionadas com o CRRS são aplicáveis a partir da data fixada pela Comissão nos termos do artigo 72.º, n.º 6.

Os artigos 6.º, 12.º, 17.º, 25.º, 38.º, 42.º, 54.º, 56.º, 57.º, 70.º, 71.º, 73.º, 74.º, 75.º, 77.º e 78.º, n.º 1, são aplicáveis a partir de 11 de junho de 2019.

O presente regulamento é aplicável ao Eurodac a partir da data em que a reformulação do Regulamento (UE) n.º 603/2013 se tornar aplicável.

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável nos Estados-Membros em conformidade com os Tratados.

Feito em Bruxelas, em 20 de maio de 2019.

Pelo Parlamento Europeu	*Pelo Conselho*
O Presidente	*O Presidente*
A. TAJANI	G. CIAMBA

REGULAMENTO (UE) 2019/818 DO PARLAMENTO EUROPEU E DO CONSELHO

de 20 de maio de 2019

relativo à criação de um regime de interoperabilidade entre os sistemas de informação da UE no domínio da cooperação policial e judiciária, asilo e migração, e que altera os Regulamentos (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816

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, o artigo 78.º, n.º 2, alínea e), o artigo 79.º, n.º 2, alínea c), o artigo 82.º, n.º 1, alínea d), o artigo 85.º, n.º 1, o artigo 87.º, n.º 2, alínea a), e o artigo 88.º, n.º 2,

Tendo em conta a proposta da Comissão Europeia,

Após transmissão do projeto de ato legislativo aos parlamentos nacionais,

Tendo em conta o parecer do Comité Económico e Social Europeu ([1]),

Após consulta ao Comité das Regiões,

Deliberando de acordo com o processo legislativo ordinário ([2]),

Considerando o seguinte:

(1) Na comunicação, de 6 de abril de 2016, intitulada Sistemas de informação mais sólidos e inteligentes para controlar as fronteiras e garantir a segurança, 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 deu início a 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 têm as informações necessárias à sua disposição.

(2) No Roteiro para intensificar o intercâmbio e a gestão de informações, incluindo soluções de interoperabilidade no domínio da Justiça e Assuntos Internos de 6 de junho de 2016, 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 resolução de 6 de julho de 2016 sobre as prioridades estratégicas do Programa de Trabalho da Comissão para 2017 ([3]), 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) Nas conclusões de 15 de dezembro de 2016, o Conselho Europeu apelou a que se continuasse a trabalhar no sentido de alcançar a interoperabilidade dos sistemas de informação e das bases de dados da UE.

(5) No relatório final de 11 de maio de 2017, 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 a interoperabilidade pode, em princípio, gerar ganhos operacionais e ser estabelecidas em conformidade com os requisitos em matéria de proteção de dados.

(6) Na comunicação de 16 de maio de 2017 intitulada Sétimo relatório sobre os progressos alcançados rumo à criação de uma União da Segurança genuína e eficaz, a Comissão definiu, em conformidade com a sua Comunicação de 6 de abril de 2016, e nas conclusões e recomendações do grupo de peritos de alto nível sobre sistemas de informação e interoperabilidade, uma nova abordagem em matéria de gestão de dados para fins de controlo das fronteiras, segurança e migração segundo a qual todos os sistemas de informação da UE para a segurança, gestão de fronteiras e migração são interoperáveis no pleno respeito dos direitos fundamentais.

([1]) JO C 283 de 10.8.2018, p. 48.
([2]) Posição do Parlamento Europeu de 16 de abril de 2019 (ainda não publicada no Jornal Oficial) e decisão do Conselho de 14 de maio de 2019.
([3]) JO C 101 de 16.3.2018, p. 116.

(7) Nas suas conclusões de 9 de junho de 2017 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) Nas conclusões de 23 de junho de 2017, o Conselho Europeu 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 com base nas propostas apresentadas pelo grupo de peritos de alto nível sobre sistemas de informação e interoperabilidade.

(9) A fim de melhorar a eficácia e a eficiência dos controlos nas fronteiras externas, contribuir para a prevenção e o combate à imigração ilegal e contribuir para um nível de segurança elevado no domínio da liberdade, da segurança e da justiça da União, incluindo a manutenção da segurança e da ordem pública e a salvaguarda da segurança nos territórios dos Estados-Membros, melhorar a aplicação da política comum em matéria de vistos, prestar assistência no âmbito do exame dos pedidos de proteção internacional, contribuir para a prevenção, deteção e investigação de infrações terroristas ou de outras infrações penais graves, ajudar na identificação de pessoas desconhecidas que não são capazes de se identificar ou de restos mortais humanos não identificados em caso de catástrofes naturais, acidentes ou ataques terroristas, com vista a preservar a confiança dos cidadãos no sistema de migração e asilo da União, nas medidas de segurança da União e nas capacidades da UE para gerir as fronteiras externas, deverá 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, respeitando simultaneamente os direitos fundamentais das pessoas, em particular o direito à proteção dos dados pessoais. Para concretizar este objetivo, é necessário criar um portal europeu de pesquisa (ESP), um serviço partilhado de correspondências biométricas (serviço partilhado 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 que esses sistemas se complementem mutuamente a fim de facilitar a correta identificação de pessoas, nomeadamente pessoas desconhecidas que não são capazes de se identificar ou restos mortais humanos não identificados, 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, reforçar 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 prevenção, deteção ou investigação de infrações terroristas ou de outras infrações penais graves 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 ECRIS-TCN.

(11) Os componentes de interoperabilidade deverão abranger o SES, o VIS, o ETIAS, o Eurodac, o SIS e o ECRIS-TCN. Os referidos componentes deverão igualmente abranger os dados da Europol, mas apenas na medida em que os dados da Europol possam ser consultados em simultâneo com esses sistemas de informação da UE.

(12) Os componentes de interoperabilidade deverão processar os dados pessoais de pessoas cujos dados pessoais sejam tratados nos sistemas de informação subjacentes da UE e pela Europol.

(13) O ESP deverá ser criado para facilitar, tecnicamente, o acesso de forma rápida, contínua, eficiente, sistemática e controlada pelas autoridades dos Estados-Membros e pelas agências da União aos sistemas de informação da UE, aos dados da Europol, bem como às bases de dados da Organização Internacional de Polícia Criminal (Interpol), na medida em que tal seja necessário ao desempenho das suas funções, em conformidade com os respetivos direitos de acesso. O ESP deverá ser criado para apoiar os objetivos do SES, do VIS, do ETIAS, do Eurodac, do SIS, do ECRIS-TCN e dos dados da Europol. Ao permitir a consulta de todos os sistemas de informação da UE pertinentes, bem como dos dados da Europol e das bases de dados da Interpol em paralelo, 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 em matéria de controlo de acessos e de proteção de dados dos sistemas subjacentes.

(14) A conceção do ESP não deverá permitir que, ao consultar as bases de dados da Interpol, os dados utilizados por um utilizador do ESP na sua consulta sejam partilhados com os titulares dos dados da Interpol. A conceção do ESP deverá igualmente garantir que as bases de dados da Interpol só sejam consultadas nos termos do direito da União e nacional aplicável.

(15) Os utilizadores do ESP que têm direito de aceder aos dados da Europol ao abrigo do Regulamento (UE) 2016/794 do Parlamento Europeu e do Conselho ([4]) deverão poder consultar os dados da Europol ao mesmo tempo que os sistemas de informação da UE a que têm acesso. Qualquer tratamento de dados subsequente a uma tal consulta deverá ter lugar nos termos do Regulamento (UE) 2016/794, incluindo as restrições relativas ao acesso ou utilização impostas pelo fornecedor de dados.

(16) O ESP deverá ser desenvolvido e configurado de modo que, na consulta, apenas seja possível utilizar dados que estejam relacionados com pessoas ou documentos de viagem, ou que estejam presentes num sistema de informação da UE, nos dados da Europol ou nas bases de dados da Interpol.

(17) A fim de assegurar a utilização sistemática dos sistemas de informação pertinentes da UE, o ESP deverá ser utilizado para consultar o CIR, o SES, o VIS, o ETIAS, o Eurodac e o ECRIS-TCN. No entanto, deverá manter-se a ligação nacional aos diferentes sistemas de informação da UE a fim de proporcionar uma alternativa técnica. O ESP deverá ser igualmente utilizado pelas agências da União para consultar o SIS Central, em conformidade com os respetivos direitos de acesso e para o desempenho das suas funções. O ESP deverá constituir um meio suplementar de consulta do SIS Central, dos dados da Europol e das bases de dados da Interpol, complementando as interfaces específicas existentes.

(18) 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 BMS deverá constituir 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 serviço partilhado BMS deverá consistir na facilitação da identificação de uma pessoa que possa estar registada em várias bases de dados, procurando correspondências com os seus dados biométricos nos diferentes sistemas e baseando-se num único componente tecnológico em vez de em diversos componentes, em cada um dos sistemas subjacentes. O serviço partilhado BMS trará vantagens em termos de segurança, bem como em termos financeiros, de manutenção e operacionais. 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 serviço partilhado BMS deverá reunir e armazenar todos estes modelos biométricos — separados, segundo um método lógico, de acordo com o sistema de informação de que provêm os dados — num único local, facilitando assim as comparações entre sistemas, mediante utilização de modelos biométricos, e permitindo economias de escala no desenvolvimento e manutenção de sistemas centrais da UE.

(19) Os modelos biométricos armazenados no serviço partilhado BMS deverão ser constituídos por dados provenientes de uma extração de características de amostras biométricas reais e ser obtidos de forma a não permitir a reversão do processo de extração. Os modelos biométricos deverão ser obtidos a partir de dados biométricos, mas não deverá ser possível obter os mesmos dados biométricos a partir dos modelos biométricos. Uma vez que os dados relativos a impressões palmares e os perfis de ADN só são armazenados no SIS e não podem ser utilizados para fins de verificações cruzadas com os dados contidos noutros sistemas de informação, em conformidade com os princípios da necessidade e da proporcionalidade, o serviço partilhado BMS não deverá armazenar os perfis de ADN nem os modelos biométricos obtidos a partir dos dados relativos a impressões palmares.

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

(21) O SES, o VIS, o ETIAS, o Eurodac e o ECRIS-TCN exigem a correta identificação das pessoas cujos dados pessoais aí se encontram armazenados. O CIR deverá, por conseguinte, facilitar e apoiar a correta identificação das pessoas registadas nesses sistemas.

(22) Os dados pessoais armazenados naqueles sistemas de informação da UE podem respeitar às mesmas pessoas, mas sob diferentes identidades ou incompletas. Os Estados-Membros dispõem de meios eficazes para identificar os seus cidadãos ou residentes permanentes registados no seu território. A interoperabilidade entre os sistemas de informação da UE deverá contribuir para a correta identificação das pessoas presentes nesses sistemas. O CIR deverá armazenar os dados pessoais necessários para permitir uma identificação mais exata dos indivíduos, cujos dados estão armazenados nesses sistemas, incluindo a sua identidade, dados sobre 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 não poderão ser conservados por mais tempo do que o estritamente necessário para efeitos dos sistemas subjacentes e deverão ser automaticamente eliminados quando os dados forem eliminados nos respetivos sistemas, de acordo com a sua separação lógica.

([4]) Regulamento (UE) 2016/794 do Parlamento Europeu e do Conselho, de 11 de maio de 2016, que cria a Agência da União Europeia para a Cooperação Policial (Europol) e que substitui e revoga as Decisões 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI e 2009/968/JAI do Conselho (JO L 135 de 24.5.2016, p. 53).

(23) A nova operação de tratamento que consiste no armazenamento desses dados no 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, os dados dos documentos de viagem e os dados biométricos serem armazenados no CIR não deverá levantar qualquer obstáculo ao tratamento de dados para efeitos do SES, VIS, ETIAS, Eurodac ou ECRIS-TCN, na medida em que o CIR será um novo componente partilhado desses sistemas subjacentes.

(24) É, por conseguinte, necessário criar um processo individual no CIR para cada pessoa registada no SES, no VIS, no ETIAS, no Eurodac ou no ECRIS-TCN, para atingir o objetivo da correta identificação de pessoas no espaço Schengen, e apoiar o MID com o duplo objetivo de facilitar os controlos de identidade de viajantes de boa-fé e combater a fraude de identidade. O processo individual deverá armazenar toda a informação sobre a identidade ligada a uma pessoa num único local e ser de acesso autorizado aos utilizadores finais.

(25) O CIR deverá, por isso, facilitar e simplificar o acesso das autoridades responsáveis pela prevenção, deteção ou investigação de infrações terroristas ou de outras infrações penais graves aos sistemas de informação da UE que não foram estabelecidos exclusivamente para efeitos de prevenção, deteção ou de investigação de crimes graves.

(26) O CIR deverá prever um recipiente partilhado para dados de identificação, dados dos documentos de viagem e dados biométricos das pessoas registadas no SES, no VIS, no ETIAS, no Eurodac e no ECRIS-TCN. O CIR deverá fazer parte da arquitetura técnica destes sistemas e funcionar como o componente partilhado entre eles para o armazenamento e consulta dos dados de identificação, dos dados dos documentos de viagem e dos dados biométricos por si tratados.

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

(28) Quando uma autoridade policial de um Estado-Membro não estiver em condições de identificar uma pessoa devido à falta de um documento de viagem ou de outro documento credível que comprove a sua identidade ou quando haja dúvidas quanto aos dados de identificação fornecidos por essa pessoa ou quanto à autenticidade do documento de viagem ou à identidade do seu titular, ou se a pessoa for incapaz de cooperar ou se recusar a fazê-lo, essa autoridade policial deverá poder consultar o CIR a fim de identificar a pessoa em causa. Para o efeito, as autoridades policiais deverão recolher impressões digitais através de técnicas de recolha de impressões digitais por meio de digitalização direta desde que o procedimento tenha sido iniciado na presença da pessoa. Tais consultas do CIR não poderão ser permitidas para fins de identificação de menores de 12 anos, salvo se forem feitas no interesse superior da criança.

(29) Caso não seja possível utilizar os dados biométricos de uma pessoa, ou se a consulta desses dados falhar, a consulta deverá 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 CIR, as autoridades dos Estados-Membros deverão ter acesso ao sistema para consultar os dados de identificação e os dados dos documentos de viagem dessa pessoa, sem que o CIR forneça nenhuma indicação quanto ao sistema de informação da UE ao qual os dados pertencem.

(30) Os Estados-Membros deverão adotar medidas legislativas nacionais, no sentido de designar as autoridades competentes para efetuar controlos de identidade recorrendo à utilização do 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, deverá ser objeto de legislação nacional.

(31) O presente regulamento deverá também introduzir uma nova possibilidade de simplificação do acesso a dados, para além dos dados de identificação ou dos dados dos documentos de viagem existentes no SES, no VIS, no ETIAS ou no Eurodac, por parte das autoridades responsáveis pela prevenção, deteção ou investigação de infrações terroristas ou de outras infrações penais graves dos Estados-Membros e da Europol. Esses dados podem ser necessários para efeitos de prevenção, deteção ou investigação das infrações terroristas ou de outras infrações penais graves num caso específico, sempre que existam motivos razoáveis para considerar que a consulta contribuirá para a prevenção, deteção ou investigação das infrações terroristas ou outras infrações penais graves, em especial quando exista uma suspeita de que o suspeito, o autor ou a vítima de uma infração terrorista ou de outra infração penal grave é uma pessoa cujos dados estão armazenados no SES, no VIS, no ETIAS ou no Eurodac.

(32) O pleno acesso aos dados contidos nos sistemas de informação da UE, necessários para fins de prevenção, deteção ou investigação de infrações terroristas ou outras infrações penais graves, para além do acesso aos dados de identificação ou aos dados do documento de viagem conservados pelo CIR, deverá continuar a ser regido pelos atos jurídicos aplicáveis. As autoridades designadas responsáveis pela prevenção, deteção ou investigação de infrações terroristas ou de outras infrações penais graves 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 deverá, por conseguinte, ser autorizado a ver em qual dos sistemas de informação da UE estão registados os dados correspondentes aos resultados da consulta. O sistema em causa seria, assim, assinalado na sequência da verificação automática da presença de uma correspondência no sistema (a chamada funcionalidade de indicadores de correspondência).

(33) Neste contexto, a resposta do CIR não deverá ser interpretada ou utilizada como fundamento ou motivo para tirar conclusões sobre uma pessoa ou tomar medidas relativamente à mesma, devendo ser utilizada apenas para efeitos de apresentação de um pedido de acesso aos sistemas de informação subjacentes da UE, em conformidade com as condições e os procedimentos estabelecidos nos atos jurídicos pertinentes que regem esse acesso. Tal pedido de acesso deverá estar sujeito ao capítulo VII do presente regulamento e, se for caso disso ano Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ([5]), à Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho ([6]) ou ao Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho ([7]).

(34) Regra geral, quando um indicador de correspondência revele que os dados estão registados no Eurodac, as autoridades designadas ou a Europol deverão solicitar o pleno acesso a, pelo menos, um dos sistemas de informação da UE em causa. Se, excecionalmente, não for solicitado o pleno acesso, por exemplo, porque as autoridades designadas ou a Europol já obtiveram os dados por outros meios, ou porque a obtenção dos dados já não é permitida pela legislação nacional, deverá ser registada a justificação da decisão de não solicitar o acesso.

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

(36) A consulta do CIR pelas autoridades designadas e pela Europol a fim de obter uma resposta com indicador de correspondência 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 correspondência não deverá 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 correspondência. Por conseguinte, o acesso do utilizador final a um indicador de correspondência terá uma interferência muito limitada no direito à proteção de dados pessoais da pessoa em causa e permite que a autoridade designada e a Europol requeiram o acesso aos dados pessoais de forma mais eficaz.

(37) O MID deverá ser criado para apoiar o funcionamento do CIR e para apoiar os objetivos do SES, do VIS, do ETIAS, do Eurodac, do SIS e do ECRIS-TCN. Para que esses objetivos sejam atingidos, é conveniente dispor da identificação precisa das pessoas cujos dados pessoais estão armazenados nesses sistemas de informação UE.

(38) Para melhor atingir os objetivos dos sistemas de informação da UE, as autoridades que utilizam esses sistemas deverão poder realizar verificações suficientemente fiáveis de identidade das pessoas cujos dados estão armazenados em sistemas diferentes. O conjunto dos dados de identificação ou dos dados do documento de

([5]) 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).

([6]) 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).

([7]) Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (JO L 295 de 21.11.2018, p. 39).

viagem armazenados num determinado sistema individual podem ser incorretos, incompletos ou fraudulentos, e atualmente não existe qualquer forma de detetar dados de identificação ou dados do documento de viagem incorretos, incompletos ou fraudulentos 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 das pessoas para estes fins.

(39) O MID deverá 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 deverá conter apenas as ligações entre os dados das pessoas presentes em mais de um sistema de informação da UE. A ligação de dados deverá ser estritamente limitada aos dados necessários para verificar se uma pessoa está registada de forma justificada ou injustificada sob diferentes identidades em sistemas diferentes, ou para clarificar situações em que duas pessoas com dados de identificação semelhantes podem não ser a mesma pessoa. O tratamento de dados através do ESP e do serviço partilhado BMS com o objetivo de estabelecer ligações entre os processos individuais nos diferentes sistemas deverá ser limitado ao mínimo e, por conseguinte, deverá apenas abranger a deteção de identidades múltiplas a realizar no momento em que são adicionados dados novos a um dos sistemas que tenha dados armazenados no CIR ou adicionados no SIS. O MID deverá dispor de salvaguardas contra eventuais discriminações e decisões desfavoráveis para pessoas com identidades múltiplas lícitas.

(40) 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 da União Europeia. 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 e pela aplicação eficaz das políticas de asilo e de vistos da União.

(41) Sempre que uma autoridade nacional ou uma agência da União cria ou carrega novos registos, o ESP e o serviço partilhado BMS deverão comparar os dados referentes a pessoas existentes no CIR e no SIS. Esta comparação deverá 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 deverão utilizar o ESP para detetar eventuais ligações com base em dados alfanuméricos. O CIR e o SIS deverão ser capazes de identificar dados idênticos ou dados semelhantes sobre as pessoas armazenados em vários sistemas. Sempre que se aplique, deverá criar-se uma ligação indicando que se trata da mesma pessoa. O CIR e o SIS deverão ser configurados de forma a que os pequenos erros de transliteração ou ortográficos detetados não criem qualquer obstáculo injustificado à pessoa em causa.

(42) A autoridade nacional ou agência da União que registou os dados no respetivo sistema de informação da UE deverá confirmar ou alterar estas ligações. Esta autoridade nacional ou agência da União deverá ter acesso aos dados armazenados no CIR ou no SIS e no MID para efeitos da verificação manual das diferentes identidades.

(43) A verificação manual das diferentes identidades deverá ser assegurada pela autoridade que cria ou atualiza os dados que desencadearam uma correspondência, resultando numa ligação com dados armazenados noutro sistema de informação da UE. A autoridade responsável pela verificação manual das diferentes identidades deverá analisá-las para determinar se se referem à mesma pessoa de forma justificada ou injustificada. Essa análise deverá ser efetuada, sempre que possível, na presença das pessoas e, quando necessário, solicitando esclarecimentos ou informações adicionais. Essa análise deverá ser efetuada sem demora, em conformidade com as obrigações legais quanto à exatidão das informações ao abrigo do direito da União e do direito nacional.

(44) Para as ligações obtidas através do 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 ou sobre pessoas para efeitos de vigilância discreta ou controlos de verificação ou controlos específicos, a autoridade responsável pela verificação manual das diferentes identidades deverá ser o gabinete SIRENE do Estado-Membro que criou a indicação. Essas categorias de indicações do SIS são sensíveis e

não deverão ser necessariamente partilhadas com as autoridades que criam ou atualizam os dados ligados a essas categorias 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 nos termos dos Regulamentos (UE) 2018/1860 ([8]), (UE) 2018/1861 ([9]) e (UE) 2018/1862 ([10]) do Parlamento Europeu e do Conselho.

(45) A criação dessas ligações exige transparência em relação às pessoas afetadas. A fim de facilitar a aplicação das salvaguardas necessárias nos termos das regras aplicáveis da União em matéria de proteção de dados, as pessoas que tenham uma ligação branca ou vermelha após a verificação manual das diferentes identidades deverão ser informadas por escrito, sem prejuízo das limitações para proteger a segurança e a ordem pública, prevenir a criminalidade e assegurar que as investigações nacionais não sejam comprometidas. Essas pessoas deverão receber um número de identificação único que lhes permita identificar a autoridade à qual deverão dirigir-se para exercerem os seus direitos.

(46) Caso seja criada uma ligação amarela, a autoridade responsável pela verificação manual das diferentes identidades deverá ter acesso ao MID. Caso exista uma ligação vermelha, as autoridades dos Estados-Membros e as agências da União com acesso a, pelo menos, um dos sistemas de informação da UE incluídos no CIR ou ao SIS, deverão ter acesso ao MID. A ligação vermelha deverá indicar que a pessoa utiliza diferentes identidades de forma injustificada ou que a pessoa utiliza a identidade de outrem.

(47) Caso exista uma ligação verde ou branca entre os dados de dois sistemas de informação da UE, as autoridades dos Estados-Membros e as agências da União deverão ter acesso ao MID nos casos em que a autoridade ou a agência em causa tenha acesso a ambos os sistemas de informação. Esse acesso deverá ser concedido unicamente com o propósito de permitir que essa autoridade ou agência detete potenciais casos em que os dados tenham sido incorretamente ligados ou tratados no MID, no CIR e no SIS em violação do presente regulamento e de tomar as medidas para corrigir a situação e atualizar ou apagar a ligação.

(48) A Agência europeia para a gestão operacional de sistemas informáticos de grande escala no espaço da liberdade, segurança e justiça (eu-LISA) deverá criar mecanismos automatizados de controlo de qualidade de dados e indicadores comuns da qualidade dos dados. A eu-LISA deverá ser responsável por desenvolver uma capacidade central de monitorização da qualidade dos dados, bem como por elaborar periodicamente relatórios de análise de dados para melhorar o controlo da aplicação dos sistemas de informação da UE por parte dos Estados-Membros. Os indicadores comuns de qualidade deverão 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.

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

(50) O Formato de Mensagem Universal (UMF) deverá constituir a norma para o intercâmbio estruturado de informações transfronteiriço entre os sistemas de informação, autoridades e/ou organizações no domínio da Justiça e Assuntos Internos. O UMF deverá 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.

(51) A aplicação da norma UMF poderá ser tida em consideração no VIS, no SIS e em quaisquer outros modelos de intercâmbio de informações transfronteiriço e sistemas de informação, existentes ou novos, no domínio da Justiça e Assuntos Internos, desenvolvidos pelos Estados-Membros.

([8]) Regulamento (UE) 2018/1860 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo à utilização do Sistema de Informação de Schengen para efeitos de regresso dos nacionais de países terceiros em situação irregular (JO L 312 de 7.12.2018, p. 1).

([9]) Regulamento (UE) 2018/1861 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen (SIS) no domínio dos controlos de fronteira, e que altera a Convenção de Aplicação do Acordo de Schengen e altera e revoga o Regulamento (CE) n.º 1987/2006 (JO L 312 de 7.12.2018, p. 14).

([10]) Regulamento (UE) 2018/1862 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen (SIS) no domínio da cooperação policial e da cooperação judiciária em matéria penal, e que altera e revoga a Decisão 2007/533/JAI do Conselho e revoga o Regulamento (CE) n.º 1986/2006 do Parlamento Europeu e do Conselho e a Decisão 2010/261/UE da Comissão (JO L 312 de 7.12.2018, p. 56).

(52) 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, nos termos dos atos jurídicos aplicáveis. A eu-LISA deverá criar, aplicar e alojar o CRRS nos seus sítios técnicos. A eu-LISA deverá conter dados estatísticos anonimizados dos sistemas de informação da UE, do CIR, do MID e do serviço partilhado BMS. Os dados contidos no CRRS não deverão permitir identificar pessoas. A eu-LISA deverá tornar os dados anónimos de forma automatizada e deverá registar esses mesmos dados anonimizados no CRRS. O processo de tornar os dados anónimos deverá ser automatizado e o pessoal da eu-LISA não deverá ter acesso direto aos dados pessoais armazenados nos sistemas de informação da UE ou nos componentes de interoperabilidade.

(53) O Regulamento (UE) 2016/679 aplica-se ao tratamento de dados pessoais para efeitos de interoperabilidade 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.

(54) Caso o tratamento de dados pessoais pelos Estados-Membros para efeitos de interoperabilidade nos termos do presente regulamento seja efetuado pelas autoridades competentes para efeitos de prevenção, deteção ou investigação de infrações terroristas ou de outras infrações penais graves, aplica-se a Diretiva (UE) 2016/680.

(55) O Regulamento (UE) 2016/679, o Regulamento (UE) 2018/1725 ou, se for caso disso, a Diretiva (UE) 2016/680 deverão aplicar-se igualmente às transferências de dados pessoais para países terceiros ou organizações internacionais realizadas nos termos do presente regulamento. Sem prejuízo dos motivos da transferência nos termos do capítulo V do Regulamento (UE) 2016/679 ou, se for caso disso, da Diretiva (UE) 2016/680, qualquer decisão de um órgão jurisdicional ou de uma autoridade administrativa de um país terceiro que exija a um responsável pelo tratamento dos dados ou a um subcontratante a transferência ou a divulgação de dados pessoais só deverá ser reconhecida ou executada, seja de que forma for, com base num acordo internacional em vigor entre o país terceiro requerente e a União ou um Estado-Membro.

(56) As disposições específicas sobre proteção de dados do Regulamento (UE) 2018/1862 e do Regulamento (UE) 2019/816 do Parlamento Europeu e do Conselho ([11]) aplicam-se ao tratamento de dados pessoais nos sistemas regidos por esses regulamentos.

(57) O Regulamento (UE) 2018/1725 aplica-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 se aplica ao tratamento de dados pessoais pela Europol.

(58) As autoridades de controlo referidas no Regulamento (UE) 2016/679 ou na Diretiva (UE) 2016/680 deverão controlar a legalidade do tratamento dos dados pessoais pelos Estados-Membros. A Autoridade Europeia para a Proteção de Dados deverá 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. Para que a Autoridade Europeia para a Proteção de Dados cumpra as tarefas que lhe são confiadas por força do presente regulamento, são necessários meios suficientes, nomeadamente humanos e financeiros.

(59) 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 do Parlamento Europeu e do Conselho ([12]) e emitiu parecer em 16 de abril de 2018 ([13]).

(60) O Grupo do Artigo 29.º para a Proteção de Dados formulou um parecer em 11 de abril de 2018.

(61) Os Estados-Membros e a eu-LISA deverão 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 deverá igualmente assegurar a utilização contínua das mais recentes evoluções tecnológicas necessárias para garantir a integridade dos dados no contexto do desenvolvimento, conceção e gestão dos componentes de interoperabilidade. As obrigações da eu-LISA neste domínio deverão incluir a adoção das medidas necessárias para impedir o acesso de

([11]) Regulamento (UE) 2019/816 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, que cria um sistema centralizado para a determinação dos Estados-Membros que possuem informações sobre condenações de nacionais de países terceiros e de apátridas (ECRIS-TCN) tendo em vista completar o Sistema Europeu de Informação sobre Registos Criminais e que altera o Regulamento (UE) 2018/1726 (ver página 1 do presente Jornal Oficial).

([12]) 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).

([13]) JO C 233 de 4.7.2018, p. 12.

pessoas não autorizadas, como pessoal de prestadores de serviços externos, aos dados pessoais tratados através dos componentes de interoperabilidade. Na adjudicação de contratos de prestação de serviços, os Estados-Membros e a eu-LISA deverão ter em consideração todas as medidas necessárias para garantir o cumprimento da legislação ou da regulamentação relativa à proteção dos dados pessoais e da privacidade das pessoas ou para salvaguardar interesses essenciais em matéria de segurança, em conformidade com o Regulamento (UE) 2018/1046 do Parlamento Europeu e do Conselho ([14]) e as convenções internacionais aplicáveis. A eu-LISA deverá aplicar os princípios da privacidade desde a conceção e por defeito durante o desenvolvimento dos componentes de interoperabilidade.

(62) Para efeitos de estatísticas e para a elaboração de relatórios, é necessário autorizar o acesso ao pessoal autorizado das autoridades, instituições e agências da União competentes a que se refere o presente regulamento para consulta de determinados dados relacionados com determinados componentes de interoperabilidade, sem permitir a identificação das pessoas.

(63) Para as autoridades dos Estados-Membros e as agências da União se adaptarem aos novos requisitos de utilização do ESP, é necessário prever um período transitório. De igual modo, a fim de permitir o funcionamento coerente e ótimo do MID, deverão ser estabelecidas medidas transitórias para a sua entrada em funcionamento.

(64) Atendendo a que o objetivo do presente regulamento, a saber, a criação de um regime de interoperabilidade entre os sistemas de informação da UE, não pode ser suficientemente alcançado pelos Estados-Membros, mas pode, devido à dimensão e aos efeitos da ação, ser mais bem alcançado ao nível da União, a União pode tomar medidas, em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do Tratado da União Europeia (TUE). Em conformidade com o princípio da proporcionalidade, consagrado no mesmo artigo, o presente regulamento não excede o necessário para alcançar esse objetivo.

(65) O montante remanescente no orçamento reservado às fronteiras inteligentes no Regulamento (UE) n.º 515/2014 do Parlamento Europeu e do Conselho ([15]) deverá ser reafetado ao presente regulamento, nos termos do artigo 5.º, n.º 5, alínea b), do Regulamento (UE) n.º 515/2014, para cobrir os custos de desenvolvimento dos componentes de interoperabilidade.

(66) A fim de completar determinados aspetos técnicos pormenorizados do presente regulamento, o poder de adotar atos nos termos do artigo 290.º do Tratado sobre o Funcionamento da União Europeia (TFUE) deverá ser delegado na Comissão no que diz respeito a:

— prorrogar o período transitório para a utilização do ESP;

— prorrogar o período transitório para a utilização do detetor de identidades múltiplas da unidade central do ETIAS;

— procedimentos para determinar os casos em que os dados de identificação podem ser considerados idênticos ou similares;

— normas relativas ao funcionamento do CRRS, incluindo as garantias específicas para o tratamento dos dados pessoais e as normas de segurança aplicáveis ao repositório; e

— regras pormenorizadas de funcionamento do portal Web.

É particularmente importante que a Comissão proceda às consultas adequadas durante os trabalhos preparatórios, inclusive ao nível de peritos, e que essas consultas sejam conduzidas de acordo com os princípios estabelecidos no Acordo Interinstitucional, de 13 de abril de 2016, sobre legislar melhor ([16]). Em particular, a fim de assegurar a igualdade de participação na preparação dos atos delegados, o Parlamento Europeu e o Conselho recebem todos os documentos ao mesmo tempo do que os peritos dos Estados-Membros, e os respetivos peritos têm sistematicamente acesso às reuniões dos grupos de peritos da Comissão que tratem da preparação dos atos delegados.

(67) A fim de assegurar condições uniformes para a execução do presente regulamento, deverão ser atribuídas competências de execução à Comissão para fixar as datas a partir das quais o ESP, o serviço partilhado BMS, o CIR, o MID e o CRRS entram em funcionamento.

([14]) Regulamento (UE, Euratom) 2018/1046 do Parlamento Europeu e do Conselho, de 18 de julho de 2018, relativo às disposições financeiras aplicáveis ao orçamento geral da União, que altera os Regulamentos (UE) n.º 1296/2013, (UE) n.º 1301/2013, (UE) n.º 1303/2013, UE n.º 1304/2013, (UE) n.º 1309/2013, (UE) n.º 1316/2013, (UE) n.º 223/2014 e (UE) n.º 283/2014, e a Decisão n.º 541/2014/UE, e revoga o Regulamento (UE, Euratom) n.º 966/2012 (JO L 193 de 30.7.2018, p. 1).

([15]) 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).

([16]) JO L 123 de 12.5.2016, p. 1.

(68) Deverão ser ainda atribuídas competências de execução à Comissão para a adoção de regras específicas sobre: os pormenores técnicos dos perfis dos utilizadores ESP; as especificações da solução técnica para facilitar a consulta dos sistemas de informação da UE, dos dados da Europol e das bases de dados da Interpol pelo ESP e o formato das respostas do ESP; as normas técnicas para a criação de ligações no MID entre dados de diferentes sistemas de informação da UE; o conteúdo e apresentação do formulário para informação do titular dos dados em caso de criação de uma ligação vermelha; os requisitos de desempenho e monitorização do desempenho do serviço partilhado BMS; os mecanismos, procedimentos e indicadores automatizados de controlo da qualidade dos dados; o desenvolvimento da norma UMF; o procedimento de cooperação a utilizar em caso de incidentes de segurança; e as especificações da solução técnica para os Estados-Membros gerirem os pedidos de acesso dos utilizadores. Essas competências deverão ser exercidas nos termos do Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho ([17]).

(69) Uma vez que os componentes de interoperabilidade envolvem o tratamento de quantidades significativas de dados pessoais sensíveis, é importante que as pessoas cujos dados são tratados através desses componentes possam, efetivamente, exercer os seus direitos enquanto titulares dos dados, tal como previsto no Regulamento (UE) 2016/679, na Diretiva (UE) 2016/680 e no Regulamento (UE) 2018/1725. Os titulares dos dados deverão dispor de um portal Web que lhes facilite o exercício dos seus direitos de acesso e de retificação, apagamento e limitação do tratamento dos seus dados pessoais. A criação e a gestão desse portal Web caberá à eu-LISA.

(70) Um dos princípios fundamentais da proteção de dados é a minimização dos dados: ao abrigo do artigo 5.º, n.º 1, alínea c), do Regulamento (UE) 2016/679, o tratamento de dados pessoais deve ser adequado, pertinente e limitado ao que é necessário relativamente às finalidades para as quais são tratados. Por este motivo, os componentes de interoperabilidade não deverão armazenar novos dados pessoais, com exceção das ligações que serão armazenadas no MID e que constituem o mínimo necessário para efeitos do presente regulamento.

(71) O presente regulamento deverá conter disposições claras sobre a responsabilização e o direito a indemnização pelo tratamento ilegal de dados pessoais e por qualquer ato que seja incompatível com o mesmo. As referidas disposições deverão ser aplicáveis, sem prejuízo do direito a indemnização e da responsabilização da pessoa que efetuou o tratamento dos dados ou do subcontratante, nos termos do Regulamento (UE) 2016/679, da Diretiva (UE) 2016/680 e do Regulamento (UE) 2018/1725. A eu-LISA deverá ser responsável pelos danos causados na sua qualidade de subcontratante de dados se não tiver cumprido as obrigações que lhe incumbem por força do presente regulamento ou se não tiver seguido as instruções lícitas do Estado-Membro responsável pelo tratamento dos dados.

(72) O presente regulamento aplica-se sem prejuízo da aplicação da Diretiva 2004/38/CE do Parlamento Europeu e do Conselho ([18]).

(73) Nos termos dos artigos 1.º e 2.º do Protocolo n.º 22, relativo à posição da Dinamarca, anexo ao TUE e ao TFUE, a Dinamarca não participa na adoção do presente regulamento, e não fica a ele vinculada nem sujeita à sua aplicação. Uma vez que o presente regulamento, na medida em que as suas disposições digam respeito ao SIS nos termos do Regulamento (UE) 2018/1862, desenvolve o acervo de Schengen, a Dinamarca decide, nos termos do artigo 4.º do Protocolo acima referido e no prazo de seis meses a contar da data de decisão do Conselho relativa ao presente regulamento, se procede à sua transposição para o seu direito interno.

(74) Na medida em que as suas disposições digam respeito ao SIS nos termos do Regulamento (UE) 2018/1862, o Reino Unido participa no presente regulamento, nos termos do artigo 5.º, n.º 1, do Protocolo n.º 19 relativo ao acervo de Schengen integrado no âmbito da União Europeia, anexo ao TUE e ao TFUE, e do artigo 8.º, n.º 2, da Decisão 2000/365/CE do Conselho ([19]). Além disso, na medida em que as suas disposições digam respeito ao Eurodac e ao ECRIS-TCN, nos termos do artigo 3.º do Protocolo n.º 21, relativo à posição do Reino Unido e da Irlanda em relação ao espaço de liberdade, segurança e justiça, anexo ao TUE e ao TFUE o Reino Unido notificou, por carta em 18 de maio de 2018, a sua intenção de participar na adoção e na aplicação do presente regulamento.

([17]) 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).

([18]) Diretiva 2004/38/CE do Parlamento Europeu e do Conselho, de 29 de abril de 2004, relativa ao direito de livre circulação e residência dos cidadãos da União e dos membros das suas famílias no território dos Estados-Membros, que altera o Regulamento (CEE) n.º 1612/68 e que revoga as Diretivas 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE e 93/96/CEE (JO L 158 de 30.4.2004, p. 77).

([19]) 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).

(75) Na medida em que as suas disposições digam respeito ao SIS nos termos do Regulamento (UE) 2018/1862, a Irlanda poderá participar no presente regulamento, nos termos do artigo 5.º, n.º 1, do Protocolo n.º 19 relativo ao acervo de Schengen integrado no âmbito da União Europeia, anexo ao TUE e ao TFUE, e do artigo 6.º, n.º 2, da Decisão 2002/192/CE do Conselho ([20]). Além disso, na medida em que as suas disposições digam respeito ao Eurodac e ao ECRIS-TCN, nos termos do artigo 1.º e 2.º do Protocolo n.º 21, relativo à posição do Reino Unido e da Irlanda em relação ao espaço de liberdade, segurança e justiça, anexo ao TUE e ao TFUE, e sem prejuízo do artigo 4.º desse protocolo, a Irlanda não participa na sua adoção e não fica a ele vinculada nem sujeita à sua aplicação. Uma vez que, nestas circunstâncias, não é possível assegurar que o presente regulamento seja aplicável na sua integralidade à Irlanda, tal como exigido no artigo 288.º do TFUE, a Irlanda não participa na adoção do presente regulamento e não fica a ele vinculada nem sujeita à sua aplicação, sem prejuízo dos seus direitos ao abrigo dos Protocolos n.ºs 19 e 21.

(76) Em relação à Islândia e à Noruega, o presente regulamento constitui, na medida em que as suas disposições digam respeito ao SIS nos termos do Regulamento (UE) 2018/1862, 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 dos dois Estados à execução, à aplicação e ao desenvolvimento do acervo de Schengen ([21]), que se inserem no domínio a que se refere o artigo 1.º, ponto G, da Decisão 1999/437/CE do Conselho ([22]).

(77) Em relação à Suíça, o presente regulamento constitui, na medida em que as suas disposições digam respeito ao SIS nos termos do Regulamento (UE) 2018/1862, um desenvolvimento das disposições do acervo de Schengen, na aceção do 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 Schengen ([23]), que se inserem no domínio a que se refere o artigo 1.º, ponto G, da Decisão 1999/437/CE, em conjugação com o artigo 3.º da Decisão 2008/149/JAI do Conselho ([24]).

(78) Em relação ao Liechtenstein, o presente regulamento constitui, na medida em que as suas disposições digam respeito ao SIS nos termos do Regulamento (UE) 2018/1862, 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 Listenstaine relativo à adesão do Principado do Listenstaine 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 Schengen ([25]), que se inserem no domínio a que se refere o artigo 1.º, ponto G, da Decisão 1999/437/CE, em conjugação com o artigo 3.º da Decisão 2011/350/UE do Conselho ([26]).

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

(80) Para que o presente regulamento possa ser integrado no regime jurídico vigente, o Regulamento (UE) 2018/1726 do Parlamento Europeu e do Conselho ([27]) e os Regulamentos (UE) 2018/1862 e (UE) 2019/816 deverão ser alterados,

---

([20]) 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).

([21]) JO L 176 de 10.7.1999, p. 36.

([22]) Decisão 1999/437/CE do Conselho, de 17 de maio de 1999, relativa a determinadas regras de aplicação do Acordo celebrado pelo Conselho da União Europeia com a República da Islândia e o Reino da Noruega relativo à associação dos dois Estados à execução, à aplicação e ao desenvolvimento do acervo de Schengen (JO L 176 de 10.7.1999, p. 31).

([23]) JO L 53 de 27.2.2008, p. 52.

([24]) Decisão 2008/149/JAI do Conselho, de 28 de janeiro de 2008, respeitante à celebração, em nome da União Europeia, do 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 Schengen (JO L 53 de 27.2.2008, p. 50).

([25]) JO L 160 de 18.6.2011, p. 21.

([26]) Decisão 2011/350/UE do Conselho, de 7 de março de 2011, respeitante à celebração, em nome da União Europeia, do Protocolo entre a União Europeia, a Comunidade Europeia, a Confederação Suíça e o Principado do Listenstaine relativo à adesão do Principado do Listenstaine 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 Schengen, no que respeita à supressão dos controlos nas fronteiras internas e à circulação das pessoas (JO L 160 de 18.6.2011, p. 19).

([27]) Regulamento (UE) 2018/1726 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo à Agência da União Europeia para a Gestão Operacional de Sistemas Informáticos de Grande Escala no Espaço de Liberdade, Segurança e Justiça (eu-LISA), que altera o Regulamento (CE) n.º 1987/2006 e a Decisão 2007/533/JAI do Conselho, e que revoga o Regulamento (UE) n.º 1077/2011 (JO L 295 de 21.11.2018, p. 99).

ADOTARAM O PRESENTE REGULAMENTO:

CAPÍTULO I

Disposições gerais

Artigo 1.º

Objeto

1. O presente regulamento, juntamente com o Regulamento (UE) 2019/817 do Parlamento Europeu e do Conselho ([28]), estabelece um regime destinado a 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).

2. O regime inclui os seguintes componentes de interoperabilidade:

a) Um portal europeu de pesquisa (ESP);

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

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

d) Um detetor de identidades múltiplas (MID).

3. O presente regulamento inclui também disposições sobre os requisitos de qualidade dos dados, um formato de mensagem universal (UMF), um repositório central para a elaboração de relatórios e estatísticas (CRRS), e 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, ao desenvolvimento e ao funcionamento dos componentes de interoperabilidade.

4. O presente regulamento adapta igualmente os procedimentos e condições que regem o acesso das autoridades designadas e da Agência da União Europeia para a Cooperação Policial (Europol) ao SES, ao VIS, ao ETIAS e ao Eurodac para fins de prevenção, deteção ou investigação de infrações terroristas ou de outras infrações penais graves.

5. O presente regulamento estabelece igualmente um regime de verificação da identidade e da identificação de pessoas.

Artigo 2.º

Objetivos

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

a) Melhorar a eficácia e a eficiência dos controlos de fronteira nas fronteiras externas;

b) Contribuir para a prevenção e o combate à imigração ilegal;

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, salvaguardando a segurança nos territórios dos Estados-Membros;

d) Melhorar a aplicação da política comum de vistos;

e) Auxiliar na análise dos pedidos de proteção internacional;

f) Contribuir para a prevenção, deteção e investigação de infrações terroristas e outras infrações penais graves;

g) Facilitar a identificação de pessoas desconhecidas que não são capazes de se identificar ou de restos mortais humanos não identificados em caso de catástrofes naturais, acidentes ou ataque terroristas.

2. Os objetivos referidos no n.º 1 devem ser alcançados mediante:

a) A garantia de correta identificação das pessoas;

b) O contributo para combater a fraude de identidade;

([28]) Regulamento (UE) 2019/817 do Parlamento Europeu e do Conselho, de 20 de maio de 2019, relativo à criação de um regime de interoperabilidade entre os sistemas de informação da UE no domínio das fronteiras e vistos e que altera os Regulamentos (CE) n.º 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 do Parlamento Europeu e do Conselho, e as Decisões 2004/512/CE e 2008/633/JAI do Conselho (ver página 27 do presente Jornal Oficial).

c) A melhoria da qualidade dos dados e a harmonização dos requisitos de qualidade dos dados armazenados nos sistemas de informação da UE, respeitando simultaneamente os requisitos previstos nos atos jurídicos que regem o tratamento de dados dos sistemas individuais, bem como as normas e os princípios em matéria de proteção de dados;

d) A facilitação da aplicação, por parte dos Estados-Membros, dos aspetos técnicos e operacionais dos sistemas de informação da UE eu e o apoio a essa aplicação;

e) O reforço, a simplificação e a maior uniformidade das condições de segurança e de proteção dos dados que regem os respetivos sistemas de informação da UE, sem prejuízo da proteção especial e das salvaguardas concedidas a determinadas categorias de dados;

f) A racionalização das condições de acesso das autoridades designadas ao SES, VIS, ETIAS e Eurodac, assegurando simultaneamente as condições necessárias e proporcionadas para esse acesso;

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

Artigo 3.º

Âmbito de aplicação

1. O presente regulamento aplica-se ao Eurodac, ao SIS e ao ECRIS-TCN.

2. O presente regulamento aplica-se aos dados da Europol na medida em que permita consultá-los em simultâneo com os sistemas de informação da UE a que se refere o n.º 1.

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

Artigo 4.º

Definições

Para efeitos do presente regulamento, entende-se por:

1) «Fronteiras externas», as fronteiras externas, na aceção do artigo 2.º, ponto 2, do Regulamento (UE) 2016/399 do Parlamento Europeu e do Conselho ([29]);

2) «Controlos de fronteira», os controlos de fronteira, na aceção do artigo 2.º, ponto 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 a que se refere o artigo 51.º, n.º 1, do Regulamento (UE) 2016/679 e a autoridade de controlo a que se refere o artigo 41.º, n.º 1, da Diretiva (UE) 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) «Dados alfanuméricos», os dados representados por letras, dígitos, carateres especiais, espaços e sinais de pontuação;

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

9) «Dados dactiloscópicos», as imagens das impressões digitais e as imagens das impressões digitais latentes que, devido ao seu caráter único e aos pontos de referência que contêm, permitem comparações rigorosas e fiáveis sobre a identidade de uma pessoa;

([29]) 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 (Código das Fronteiras Schengen) (JO L 77 de 23.3.2016, p. 1).

10) «Imagem facial», a imagem digitalizada do rosto de uma pessoa;

11) «Dados biométricos», os dados dactiloscópicos e a imagem facial ou ambos;

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

13) «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;

14) «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;

15) «Sistemas de informação da UE», o SES, o VIS, o ETIAS, o Eurodac, o SIS e o ECRIS-TCN;

16) «Dados da Europol», os dados pessoais tratados pela Europol para os fins previstos no artigo 18.º, n.º 2, alíneas a), b) e c), do Regulamento (UE) 2016/794;

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

18) «Correspondência», existência de uma correspondência em resultado de uma comparação automatizada de dados pessoais registados, ou a ser registados, num sistema de informação ou numa base de dados;

19) «Autoridade policial», uma «autoridade competente», na aceção do artigo 3.º, ponto 7, da Diretiva (UE) 2016/680;

20) «Autoridades designadas», as autoridades designadas dos Estados-Membros na aceção do artigo 3.º, n.º 1, ponto 26, do Regulamento (UE) 2017/2226 do Parlamento Europeu e do Conselho ([30]), do artigo 2.º, n.º 1, alínea e), da Decisão 2008/633/JAI do Conselho ([31]) e do artigo 3.º, n.º 1, ponto 21, do Regulamento (UE) 2018/1240 do Parlamento Europeu e do Conselho ([32]);

21) «Infração terrorista», uma infração prevista na legislação nacional que corresponda ou seja equivalente a uma das infrações referidas na Diretiva (UE) 2017/541 do Parlamento Europeu e do Conselho ([33]);

22) «Infração penal grave», uma infração que corresponda ou seja equivalente a uma das infrações referidas no artigo 2.º, n.º 2, da Decisão-Quadro 2002/584/JAI do Conselho ([34]), 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;

23) «Sistema de Entrada/Saída» ou «SES», o Sistema de Entrada/Saída, criado pelo Regulamento (UE) 2017/2226;

24) «Sistema de Informação sobre Vistos» ou «VIS», o Sistema de Informação sobre Vistos criado pelo Regulamento (UE) n.º 767/2008 do Parlamento Europeu e do Conselho ([35]);

25) «Sistema Europeu de Informação e Autorização de Viagem» ou «ETIAS», o Sistema Europeu de Informação e Autorização de Viagem criado pelo Regulamento (UE) 2018/1240;

([30]) 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, que determina as condições de acesso ao SES para efeitos de aplicação da lei, e que altera a Convenção de Aplicação do Acordo de Schengen e os Regulamentos (CE) n.º 767/2008 e (UE) n.º 1077/2011 (JO L 327 de 9.12.2017, p. 20).

([31]) Decisão 2008/633/JAI do Conselho, de 23 de junho de 2008, relativa ao acesso para consulta ao Sistema de Informação sobre Vistos (VIS) por parte das autoridades designadas dos Estados-Membros e por parte da Europol para efeitos de prevenção, deteção e investigação de infrações terroristas e outras infrações penais graves (JO L 218 de 13.8.2008, p. 129).

([32]) Regulamento (UE) 2018/1240 do Parlamento Europeu e do Conselho, de 12 de setembro de 2018, que cria um Sistema Europeu de Informação e Autorização de Viagem (ETIAS) e altera os Regulamentos (UE) n.º 1077/2011, (UE) n.º 515/2014, (UE) 2016/399, (UE) 2016/1624 e (UE) 2017/2226 (JO L 236 de 19.9.2018, p. 1).

([33]) Diretiva (UE) 2017/541 do Parlamento Europeu e do Conselho, de 15 de março de 2017, relativa à luta contra o terrorismo e que substitui a Decisão-Quadro 2002/475/JAI do Conselho e altera a Decisão 2005/671/JAI do Conselho (JO L 88 de 31.3.2017, p. 6).

([34]) Decisão-Quadro 2002/584/JAI do Conselho, de 13 de junho de 2002, relativa ao mandado de detenção europeu e aos processos de entrega entre os Estados-Membros (JO L 190 de 18.7.2002, p. 1).

([35]) 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).

26) «Eurodac», Eurodac criado pelo Regulamento (UE) n.º 603/2013 do Parlamento Europeu e do Conselho ([36]);

27) «Sistema de Informação Schengen» ou «SIS», o Sistema de Informação Schengen criado pelos Regulamentos (UE) 2018/1860, (UE) 2018/1861 e (UE) 2018/1862;

28) «ECRIS-TCN», o sistema centralizado de identificação de Estados-Membros que possui informações sobre condenações de nacionais de países terceiros e de apátridas, criado pelo Regulamento (UE) 2019/816.

Artigo 5.º

Não discriminação e direitos fundamentais

O tratamento de dados pessoais para efeitos do presente regulamento não pode originar discriminação de pessoas em razão do género, da raça, da cor, da origem étnica ou social, das características genéticas, da língua, da religião ou crença, das opiniões políticas ou de outra natureza, da pertença a uma minoria nacional, do património, do nascimento, da deficiência, da idade ou da orientação sexual. O respeito pela dignidade e integridade humanas e pelos direitos fundamentais, incluindo o direito ao respeito pela vida privada e à proteção dos dados pessoais, deve ser integralmente assegurado. Deve ser dispensada especial atenção às crianças, aos idosos, às pessoas com deficiência e às pessoas com necessidade de proteção internacional. O interesse superior da criança deve ser uma consideração primordial.

CAPÍTULO II

Portal europeu de pesquisa

Artigo 6.º

Portal europeu de pesquisa

1. É criado um portal europeu de pesquisa (ESP) para facilitar o acesso rápido, contínuo, eficiente, sistemático e controlado das autoridades dos Estados-Membros e das agências da União aos sistemas de informação da UE, aos dados da Europol e às bases de dados da Interpol para o desempenho das suas funções e em conformidade com os respetivos direitos de acesso ao SES, ao VIS, ao ETIAS, ao Eurodac, ao SIS e ao ECRIS-TCN e com os objetivos e finalidades dos mesmos.

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 as agências da União que têm o direito de utilizar o ESP;

c) Uma infraestrutura de comunicação segura entre o ESP e o SES, o VIS, o ETIAS, o Eurodac, o SIS Central, o ECRIS-TCN, os dados da Europol e as bases de dados da Interpol, bem como entre o ESP e as infraestruturas centrais do CIR e do MID.

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 às agências da União que dispõem de acesso a, pelo menos, um dos sistemas de informação da UE, de acordo com os atos jurídicos que regem esses sistemas de informação da UE, ao CIR, ao MID, de acordo com o presente regulamento, aos dados da Europol de acordo com o Regulamento (UE) 2016/794 ou às bases de dados da Interpol de acordo com o direito da União ou o direito nacional aplicável ao referido acesso.

As referidas autoridades dos Estados-Membros e agências da União podem utilizar o ESP e os dados por ele fornecidos unicamente para os objetivos e finalidades previstos nos atos jurídicos que regem esses sistemas de informação da UE, no Regulamento (UE) 2016/794 e no presente regulamento.

([36]) Regulamento (UE) n.º 603/2013 do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativo à criação do sistema «Eurodac» de comparação de impressões digitais para efeitos da aplicação efetiva do Regulamento (UE) n.º 604/2013, que estabelece os critérios e mecanismos de determinação do Estado-Membro responsável pela análise de um pedido de proteção internacional apresentado num dos Estados-Membros por um nacional de um país terceiro ou um apátrida, e de pedidos de comparação com os dados Eurodac apresentados pelas autoridades responsáveis dos Estados-Membros e pela Europol para fins de aplicação da lei e que altera o Regulamento (UE) n.º 1077/2011 que cria uma Agência europeia para a gestão operacional de sistemas informáticos de grande escala no espaço de liberdade, segurança e justiça (JO L 180 de 29.6.2013, p. 1).

2. As autoridades dos Estados-Membros e as agências da União 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 Eurodac e do ECRIS-TCN, em conformidade com os seus direitos de acesso, como referido nos atos jurídicos que regem esses sistemas de informação da UE e no direito nacional. Essas autoridades e agências 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 nos Regulamentos (UE) 2018/1860 e (UE) 2018/1861.

4. Quando previsto pelo direito da União, as agências da União a que se refere o n.º 1 devem utilizar o ESP para pesquisar dados relativos a pessoas ou aos seus documentos de viagem no SIS Central.

5. As autoridades dos Estados-Membros e as agências da União referidas no n.º 1 podem utilizar o ESP para pesquisar dados relativos a pessoas ou aos seus documentos de viagem nos dados da Europol, 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, em cooperação com os Estados-Membros, um perfil baseado na categoria de utilizador do ESP e nas finalidades das consultas, em conformidade com os pormenores técnicos e os direitos de acesso a que se refere o n.º 2. Cada perfil deve incluir, nos termos do direito da União e do direito nacional, a seguinte informação:

a) Os campos de dados a utilizar 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;

c) Os dados específicos contidos nos sistemas de informação da UE, os dados da Europol e as bases de dados da Interpol que podem ser consultados;

d) As categorias de dados que podem ser fornecidos em cada resposta.

2. A Comissão deve adotar atos de execução, a fim de especificar os pormenores técnicos dos perfis referidos no n.º 1 em conformidade com os direitos de acesso dos utilizadores do ESP, conforme previsto nos atos jurídicos que regem os sistemas de informação da UE e de acordo com o direito nacional. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 70.º, n.º 2.

3. Os perfis referidos no n.º 1 devem ser revistos periodicamente pela eu-LISA, em cooperação com os Estados-Membros, pelo menos uma vez por ano e, se necessário, atualizados.

Artigo 9.º

Consultas

1. Os utilizadores do ESP iniciam uma consulta introduzindo dados alfanuméricos ou biométricos no ESP. Ao iniciar-se uma consulta, o ESP consulta o SES, o ETIAS, o VIS, o SIS, o Eurodac, o ECRIS-TCN e o CIR, os dados da Europol e as bases de dados da Interpol, utilizando simultaneamente os dados introduzidos pelo utilizador do ESP e de acordo com o perfil do utilizador.

2. As categorias de dados utilizados para iniciar uma consulta através do ESP correspondem às categorias 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 atos jurídicos que lhes são aplicáveis.

3. A eu-LISA deve desenvolver, em cooperação com os Estados-Membros, um documento de controlo das interfaces para o ESP baseado no UMF referido no artigo 38.º.

4. Em resposta a uma consulta de um utilizador do ESP, o SES, o ETIAS, o VIS, o SIS, o Eurodac, o ECRIS-TCN, o CIR e o MID, os dados da Europol e as bases de dados da Interpol, devem responder à consulta, fornecendo os dados em sua posse.

Sem prejuízo do artigo 20.º, a resposta do ESP deve indicar qual o sistema de informação ou base de dados da UE a que os dados pertencem.

O ESP não fornece informações relativas aos dados dos sistemas de informação da UE, aos dados da Europol e nem às bases de dados da Interpol aos quais o utilizador não tem acesso nos termos do direito da União e do direito nacional aplicáveis.

5. As consultas das bases de dados da Interpol lançadas através do ESP devem ser efetuadas de molde a não revelar qualquer informação ao proprietário do alerta da Interpol.

6. O ESP deve fornecer respostas ao utilizador assim que os dados de um dos sistemas de informação da UE, os dados da Europol ou as bases de dados da Interpol estiverem disponíveis. Essas respostas devem conter apenas os dados aos quais o utilizador tem acesso ao abrigo do direito da União e do direito nacional.

7. A Comissão deve adotar um ato de execução para especificar o procedimento técnico para as consultas do ESP nos sistemas de informação da UE, nos dados da Europol e nas bases de dados da Interpol e o formato das respostas do ESP. O referido ato de execução é adotado pelo procedimento de exame a que se refere o artigo 70.º, n.º 2.

Artigo 10.º

Manutenção de registos

1. Sem prejuízo do disposto nos artigos 12.º e 18.º do Regulamento (UE) 2018/1862, no artigo 29.º do Regulamento (UE) 2019/816 e no artigo 40.º do Regulamento (UE) 2016/794, a eu-LISA deve conservar registos de todas as operações de tratamento de dados realizadas no ESP. Esses registos devem incluir o seguinte:

a) O Estado-Membro ou a agência da União que lança a consulta e o perfil de ESP utilizado;

b) A data e a hora da consulta;

c) Os sistemas de informação da UE e os dados da Europol consultados.

2. Cada Estado-Membro deve manter registos das consultas feitas pelas suas autoridades e pelo pessoal devidamente autorizado dessas autoridades a utilizar o ESP. Cada agência da União deve manter registos das consultas feitas pelo seu pessoal devidamente autorizado a utilizar o ESP.

3. Os registos referidos no n.º 1 e no n.º 2 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 e a integridade dos dados. Esses registos devem estar protegidos por medidas adequadas contra acesso não autorizado e ser apagados um ano após a sua criação. Se, no entanto, forem necessários para procedimentos de controlo que já tenham sido iniciados, devem, nesse caso, ser apagados logo que deixarem de ser necessários para o efeito.

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 ou o CIR, devido a uma falha do ESP, os utilizadores do ESP devem ser notificados pela eu-LISA de forma automatizada.

2. Em caso de impossibilidade técnica de utilizar o ESP para consultar um ou vários sistemas de informação da UE ou o CIR, devido a uma falha da infraestrutura nacional de um Estado-Membro, esse Estado-Membro deve notificar a eu-LISA e a Comissão de forma automatizada.

3. Nos casos referidos nos n.os 1 ou 2 do presente artigo, e até que a falha técnica seja resolvida, a obrigação referida no artigo 7.º, n.os 2 e 4, não se aplica e os Estados-Membros devem aceder aos sistemas de informação da UE ou ao CIR diretamente, caso o direito da União ou o direito nacional o preveja.

4. Em caso de impossibilidade técnica de utilizar o ESP para consultar um ou vários sistemas de informação da União ou o CIR, devido a uma falha da infraestrutura de uma agência da União, a agência em causa notifica a eu-LISA e a Comissão de forma automatizada.

CAPÍTULO III

Serviço partilhado de correspondências biométricas

Artigo 12.º

Serviço partilhado de correspondências biométricas

1. É criado um serviço partilhado de correspondências biométricas (serviço partilhado BMS) onde são armazenados modelos biométricos obtidos com base nos dados biométricos referidos no artigo 13.º armazenados no CIR e no SIS, e que permite consultar vários sistemas de informação da UE usando dados biométricos, para efeitos de apoio do CIR e do MID e dos objetivos do SES, do VIS, do Eurodac, do SIS e do ECRIS-TCN.

2. O serviço partilhado BMS é composto por:

a) Uma infraestrutura central que substitui os sistemas centrais, respetivamente, do SES, do VIS, do SIS, do Eurodac e do ECRIS-TCN, na medida em que armazena modelos biométricos e permite buscas de dados biométricos;

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

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

Artigo 13.º

Armazenamento de modelos biométricos no serviço partilhado de correspondências biométricas

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

a) Os dados referidos no artigo 20.º, n.º 3, alíneas w) e y), à exceção dos dados relativos a impressões palmares, do Regulamento (UE) 2018/1862;

b) Os dados referidos no artigo 5.º, n.º 1, alínea b) e no n.º 2 do Regulamento (UE) 2019/816.

Os modelos biométricos são armazenados no serviço partilhado BMS, separados de forma lógica de acordo com o sistema de informação de onde provêm os dados.

2. Para cada conjunto de dados a que se refere o n.º 1, o serviço partilhado BMS inclui em cada modelo biométrico uma referência aos sistemas de informação da UE onde estão armazenados os dados biométricos correspondentes e uma referência aos registos efetivos nesses sistemas de informação da UE.

3. Os modelos biométricos são introduzidos no serviço partilhado BMS somente após um controlo automatizado da qualidade dos dados biométricos adicionados a um dos sistemas de informação da UE. Esse controlo é efetuado pelo serviço partilhado 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.

5. A Comissão deve estabelecer, por meio de um ato de execução, requisitos de desempenho e disposições práticas para monitorizar o desempenho do serviço partilhado BMS, a fim de assegurar que a eficácia das pesquisas biométricas respeita os procedimentos urgentes, como os controlos nas fronteiras e as identificações. O referido ato de execução é adotado pelo procedimento de exame a que se refere o artigo 70.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 serviço partilhado BMS. As consultas com dados biométricos devem ser efetuadas em conformidade com os fins previstos no presente regulamento e nos Regulamentos (CE) n.º 767/2008, (UE) 2017/2226, (UE) 2018/1860, (UE) 2018/1861, (UE) 2018/1862 e (UE) 2019/816.

Artigo 15.º

Conservação de dados no serviço partilhado de correspondências biométricas

Os dados referidos no artigo 13.º, n.ºs 1 e 2, devem ser conservados no serviço partilhado BMS unicamente enquanto os dados biométricos correspondentes estiverem armazenados no CIR ou no SIS. Os dados devem ser apagados do serviço partilhado BMS de forma automatizada.

Artigo 16.º

Manutenção de registos

1. Sem prejuízo do disposto nos artigos 12.º e 18.º do Regulamento (UE) 2018/1862 e no artigo 29.º do Regulamento (UE) 2019/816, a eu-LISA deve conservar registos de todas as operações de tratamento de dados realizadas no serviço partilhado BMS. Esses registos devem incluir o seguinte:

a) O Estado-Membro ou a agência da União que inicia a consulta;

b) O histórico da criação e o armazenamento de modelos biométricos;

c) Os sistemas de informação da UE consultados utilizando os modelos biométricos armazenados no serviço partilhado BMS;

d) A data e a hora da consulta;

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

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

2. Cada Estado-Membro deve manter registos das consultas feitas pelas suas autoridades e pelo pessoal devidamente autorizado dessas autoridades a utilizar o serviço partilhado BMS. Cada agência da União deve manter registos das consultas feitas pelo seu pessoal devidamente autorizado a utilizar o serviço partilhado BMS.

3. Os registos referidos no n.º 1 e no n.º 2 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 e a integridade dos dados. Esses registos devem estar protegidos por medidas adequadas contra acesso não autorizado e ser apagados um ano após a sua criação. No entanto, caso sejam necessários para procedimentos de controlo que já tenham sido iniciados, devem ser apagados logo que deixarem de ser necessários para esse efeito.

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 ECRIS-TCN e contém 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 ECRIS-TCN, nos termos do artigo 20.º, de apoiar o funcionamento do MID nos termos do artigo 21.º e de facilitar e simplificar o acesso das autoridades designadas e da Europol ao SES, ao VIS, ao ETIAS e ao Eurodac, sempre que tal for necessário para efeitos de prevenção, deteção ou investigação de infrações terroristas ou outras infrações penais graves nos termos do artigo 22.º.

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 ECRIS-TCN na medida em que armazena os dados referidos no artigo 18.º;

b) Um canal de comunicação seguro entre o CIR, os Estados-Membros e as agências da União que têm o direito de utilizar o CIR nos termos do direito da União e do direito nacional;

c) Uma infraestrutura de comunicação segura entre o CIR e o SES, o VIS, o ETIAS, o Eurodac e o ECRIS-TCN, bem como com as infraestruturas centrais do ESP, do serviço partilhado BMS e do MID.

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

4. Caso seja tecnicamente impossível consultar o CIR, devido a uma falha do CIR, para efeitos de identificação de uma pessoa nos termos do artigo 20.º, de deteção de identidades múltiplas nos termos do artigo 21.º ou de prevenção, deteção ou investigação de infrações terroristas ou outras infrações penais graves nos termos do artigo 22.º, os utilizadores do CIR devem ser notificados pela eu-LISA de forma automatizada.

5. A eu-LISA deve, em cooperação com os Estados-Membros, desenvolver para o CIR um documento de controlo das interfaces baseado no UMF referido no artigo 38.º.

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: os dados referidos no artigo 5.º, n.º 1, alínea b) e n.º 2, e os seguintes dados do artigo 5.º, n.º 1, alínea a), do Regulamento (UE) 2019/816: apelidos; nomes próprios, data de nascimento, local de nascimento (localidade e país), nacionalidade ou nacionalidades, sexo, nomes anteriores e, se aplicável, pseudónimos ou outros nomes, bem como, se estiverem disponíveis, informações sobre os documentos de viagem.

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

3. As autoridades que acedem ao CIR devem fazê-lo em conformidade com os seus direitos de acesso, tal como referido nos atos jurídicos que regem os sistemas de informação da UE e no direito nacional e em conformidade com os seus direitos de acesso nos termos do presente regulamento para os efeitos referidos nos artigos 20.º, 21.º e 22.º.

4. Para cada série de dados a que se refere o n.º 1, o CIR deve incluir uma referência ao registo efetivo nos sistemas de informação da UE a que os dados pertencem.

5. 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 Eurodac ou no ECRIS-TCN, 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. Caso seja criada uma ligação branca ou vermelha no MID nos termos dos 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. As consultas do CIR devem ser realizadas por uma autoridade policial nos termos dos n.ºs 2 e 5 apenas nas seguintes circunstâncias:

a) Caso uma autoridade policial não consiga identificar uma pessoa devido à falta de um documento de viagem ou de outro documento credível que comprove a identidade dessa pessoa;

b) Em caso de dúvidas sobre os dados de identificação fornecidos por uma pessoa;

c) Em caso de dúvidas sobre a autenticidade do documento de viagem ou de outro documento credível fornecido por uma pessoa;

d) Em caso de dúvidas sobre a identidade do titular de um documento de viagem ou de outro documento credível; ou

e) Caso a pessoa não possa ou se recuse a cooperar.

Essas consultas não são autorizadas quando se trate de menores de 12 anos, salvo se forem feitas no superior interesse da criança.

2. Sempre que se verifique uma das circunstâncias previstas no n.º 1 e uma autoridade policial tenha sido habilitada para o efeito por medidas legislativas nacionais, tal como referido no n.º 5, pode, exclusivamente para efeitos de identificação de uma pessoa, consultar o CIR usando os dados biométricos dessa pessoa que foram obtidos em tempo real durante um controlo de identidade, desde que o procedimento tenha sido iniciado na presença dessa pessoa.

3. Sempre que a consulta indicar que os dados relativos a essa pessoa estão armazenados no CIR, a autoridade policial 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.

4. Sempre que uma autoridade policial tenha sido habilitada para o efeito por medidas legislativas nacionais, a que se refere o n.º 6, pode, em caso de catástrofe natural, de acidente ou de um atentado terrorista, e exclusivamente para efeitos de identificação de pessoas desconhecidas que não sejam capazes de se identificar ou de restos mortais humanos não identificados, consultar o CIR usando os dados biométricos dessas pessoas.

5. Os Estados-Membros que pretendam usar a possibilidade prevista no n.º 2 devem adotar medidas legislativas nacionais. Ao fazê-lo, os Estados-Membros devem ter em conta a necessidade de evitar qualquer discriminação contra nacionais de países terceiros. Essas medidas legislativas devem especificar exatamente os objetivos da identificação referidos no artigo 2.º, n.º 1, alíneas b) e c), designar as autoridades policiais competentes e estabelecer os procedimentos, as condições e os critérios desses controlos de identidade.

6. Os Estados-Membros que pretendam aplicar o n.º 4 devem adotar medidas legislativas nacionais que estabeleçam os procedimentos, as condições e os critérios para o efeito.

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, nos termos do artigo 28.º, n.º 4, a autoridade responsável pela verificação manual das diferentes identidades, nos termos do artigo 29.º, deve ter acesso, unicamente para efeitos dessa verificação, aos dados referidos no artigo 18.º, n.ºs 1 e 2, armazenados no CIR associados a uma ligação amarela.

2. Sempre que uma consulta do CIR se traduzir numa ligação vermelha, nos termos do 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 referidos no artigo 18.º, n.ºs 1 e 2, armazenados no CIR associados a uma ligação vermelha.

Artigo 22.º

Consulta do repositório comum de dados de identificação para efeitos de prevenção, deteção ou investigação de infrações terroristas ou outras infrações penais graves

1. Num caso específico, sempre que existam motivos razoáveis para crer que a consulta dos sistemas de informação da UE contribuirá para a prevenção, deteção ou investigação de infrações terroristas ou outras infrações penais graves, nomeadamente caso haja indícios de que o suspeito, autor ou vítima de uma infração terrorista ou de outras infrações penais graves é uma pessoa cujos dados estão armazenados no Eurodac, as autoridades designadas e a Europol podem consultar o CIR para obter informações sobre se existem dados sobre uma determinada pessoa no Eurodac.

2. Sempre que, em resposta a uma consulta, o CIR indicar a presença de dados sobre essa pessoa no Eurodac, o CIR deve fornecer às autoridades designadas e à Europol uma resposta sob a forma de uma referência a que se refere o artigo 18.º, n.º 2, indicando que o Eurodac contém os dados das correspondências. O CIR deve responder de forma a não comprometer a segurança dos dados.

A resposta com a indicação de que existem dados relativos a essa pessoa no Eurodac só pode ser utilizada para efeitos de apresentação de um pedido de acesso pleno, no respeito das condições e dos procedimentos definidos nos atos jurídicos que regem esse acesso.

Em caso de correspondência ou de correspondências múltiplas, a autoridade designada ou a Europol devem solicitar um acesso pleno a, pelo menos, um dos sistemas de informação para os quais foi gerada uma correspondência.

No caso, excecional, de não ser solicitado esse acesso pleno, as autoridades designadas devem registar a justificação fornecida para não efetuar o pedido, a qual deve ser rastreável até ao processo nacional. A Europol deve registá-la no processo correspondente.

3. O pleno acesso aos dados contidos no Eurodac para efeitos de prevenção, deteção ou investigação de infrações terroristas ou outras infrações penais graves continua sujeito às condições e procedimentos estabelecidos nos atos jurídicos que regem esse acesso.

Artigo 23.º

Conservação de dados no repositório comum de dados de identificação

1. Os dados referidos no artigo 18.º, n.os 1, 2 e 4 devem ser eliminados do CIR de uma forma automatizada em conformidade com as disposições em matéria de conservação de dados do Regulamento (UE) 2019/816.

2. O processo individual deve permanecer armazenado no CIR apenas enquanto os dados correspondentes permanecerem armazenados em, pelo menos, um dos sistemas de informação da UE 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 29.º do Regulamento (UE) 2019/816, a eu-LISA deve conservar registos de todas as operações de tratamento de dados realizadas no CIR nos termos dos n.os 2, 3 e 4 do presente artigo.

2. A eu-LISA deve conservar, nos termos do artigo 20.º, registos de todas as operações de tratamento de dados realizadas no CIR. Esses registos devem incluir o seguinte:

a) O Estado-Membro ou a agência da União que inicia a consulta;

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

c) A data e a hora da consulta;

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

e) Os resultados da consulta.

3. A eu-LISA deve conservar, nos termos do artigo 21.º, registos de todas as operações de tratamento de dados realizadas no CIR. Esses registos devem incluir o seguinte:

a) O Estado-Membro ou a agência da União que inicia a consulta;

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

c) A data e a hora da consulta;

d) Caso seja criada uma ligação, os dados utilizados para iniciar a consulta e os resultados da consulta com a indicação do sistema de informação da UE do qual foram recebidos os dados.

4. A eu-LISA deve conservar registos, nos termos do artigo 22.º, de todas as operações de tratamento de dados realizadas no CIR. Esses registos devem incluir o seguinte:

a) A data e a hora da consulta;

b) Os dados utilizados para iniciar a consulta;

c) Os resultados da consulta;

d) O Estado-Membro ou a agência da União que consulta o CIR.

Os registos desse acesso devem ser verificados periodicamente pela autoridade de controlo competente, nos termos do artigo 41.º da Diretiva (UE) 2016/680 ou pela Autoridade Europeia para a Proteção de Dados, nos termos do artigo 43.º do Regulamento (UE) 2016/794, a intervalos não superiores a seis meses, a fim de verificar se os procedimentos e condições estabelecidos no artigo 22.º, n.º 1 e n.º 2 do presente regulamento são cumpridos.

5. Cada Estado-Membro deve manter registos das consultas efetuadas pelas suas autoridades e pelo pessoal devidamente autorizado dessas autoridades a utilizar o CIR, nos termos dos artigos 20.º, 21.º e 22.º. Cada agência da União deve manter registos das consultas efetuadas pelo seu pessoal devidamente autorizado a utilizar o CIR, nos termos dos artigos 21.º e 22.º.

Além disso, para qualquer acesso ao CIR nos termos do artigo 22.º, cada Estado-Membro deve conservar os seguintes registos:

a) A referência do processo nacional;

b) A finalidade do acesso;

c) Nos termos das regras nacionais, a identificação de utilizador único do funcionário que efetuou a consulta e do funcionário que ordenou a consulta.

6. Em conformidade com o Regulamento (UE) 2016/794, para qualquer acesso ao CIR nos termos do artigo 22.º do presente regulamento, a Europol deve conservar registos da identificação de utilizador único do funcionário que efetuou a consulta e do funcionário que a ordenou.

7. Os registos referidos nos n.os 2 a 6 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 e a integridade dos dados. Esses registos devem estar protegidos por medidas adequadas contra acesso não autorizado e ser apagados um ano após a sua criação. Se, no entanto, se forem necessários para procedimentos de controlo que já tenham sido iniciados, devem ser apagados logo que deixarem de ser necessários para o efeito.

8. A eu-LISA deve armazenar os registos relacionados com o histórico dos dados nos processos individuais. A eu-LISA deve apagar esses registos de forma automatizada, 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 ficheiros de confirmação da identidade, como referido no artigo 34.º, que contém ligações entre os dados nos sistemas de informação da UE que fazem parte do CIR e do SIS e que permite detetar 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 ECRIS-TCN.

2. O MID é composto por:

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

b) Uma infraestrutura de comunicação segura para ligar o MID ao SIS e as infraestruturas centrais do ESP 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 das diferentes identidades 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) O gabinete SIRENE do Estado-Membro que cria ou atualiza um alerta nos termos do Regulamento (UE) 2018/1862;

b) Autoridades centrais do Estado-Membro de condenação ao registar ou alterar dados no ECRIS-TCN nos termos dos artigos 5.º ou 9.º do Regulamento (UE) 2019/816.

2. As autoridades dos Estados-Membros e as agências da UE que tenham acesso a, pelo menos, um sistema de informação da UE incluído no CIR 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.

3. As autoridades dos Estados-Membros e as agências da União devem ter acesso às ligações brancas a que se refere o artigo 33.º, caso tenham acesso aos dois sistemas de informação da UE que contêm dados entre os quais foi criada a ligação branca.

4. As autoridades dos Estados-Membros e as agências da União devem ter acesso às ligações verdes a que se refere o artigo 31.º, caso tenham acesso aos dois sistemas de informação da UE que contêm dados entre os quais foi criada a ligação verde e uma consulta a esses sistemas de informação tenha revelado uma correspondência com os dois conjuntos de dados ligados.

Artigo 27.º

Deteção de identidades múltiplas

1. Deve ser iniciada uma deteção de identidades múltiplas no CIR e no SIS se:

a) For criada ou atualizada uma indicação no SIS nos termos dos capítulos VI a IX do Regulamento (UE) 2018/1862;

b) For criado ou alterado um registo de dados no ECRIS-TCN, nos termos dos artigos 5.º ou 9.º do Regulamento (UE) 2019/816.

2. Se os dados contidos num sistema de informação da UE a que se refere o n.º 1 contiverem dados biométricos, o CIR e o SIS Central devem utilizar o serviço partilhado BMS a fim de realizar a deteção de identidades múltiplas. O serviço partilhado BMS deve comparar os modelos biométricos obtidos a partir de quaisquer novos dados biométricos com os modelos biométricos já constantes do serviço partilhado BMS para verificar se os dados pertencentes à mesma pessoa 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 ESP para pesquisar os dados armazenados no SIS Central e no CIR, respetivamente, utilizando os seguintes dados:

a) Apelido, nomes próprios, nomes de nascimento, nomes e pseudónimos utilizados anteriormente, local de nascimento, data de nascimento, género, nacionalidade ou nacionalidades a que se refere o artigo 20.º, n.º 3, do Regulamento (UE) 2018/1862;

b) Apelidos, nomes próprios, data de nascimento, local de nascimento (localidade e país), nacionalidade ou nacionalidades e sexo a que se refere o artigo 5.º, n.º 1, alínea a), do Regulamento (UE) 2019/816.

4. Para além do processo a que se referem os n.ºs 2 e 3, o CIR e o SIS Central devem utilizar o ESP para pesquisar os dados armazenados no SIS Central e no CIR, respetivamente, utilizando os dados do documento de viagem.

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

Artigo 28.º

Resultados da deteção de identidades múltiplas

1. Nos casos em que as consultas referidas no artigo 27.º, n.ºs 2, 3 e 4, não indicarem qualquer correspondência, os procedimentos a que se refere o artigo 27.º, n.º 1, devem continuar de acordo com os atos jurídicos que os regem.

2. Se a pesquisa referida no artigo 27.º, n.ºs 2, 3 e 4, indicar uma ou várias respostas, o CIR e, se for caso disso, o SIS devem criar uma ligação entre os dados utilizados para lançar a pesquisa e os dados que desencadearam a correspondência.

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

3. Se a pesquisa referida no artigo 27.º, n.ºs 2, 3 e 4, indicar uma ou várias correspondências e os dados de identificação dos ficheiros ligados forem os mesmos ou semelhantes, deve ser criada uma ligação branca nos termos do artigo 33.º.

4. Se a pesquisa referida no artigo 27.º, n.ºs 2, 3 e 4, detetar uma ou várias correspondências 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.

5. A Comissão deve adotar delegados nos termos do artigo 69.º que estabelecem os procedimentos para determinar os casos em que dados de identificação podem ser considerados os mesmos ou similares

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

7. A Comissão deve estabelecer, em cooperação com a eu-LISA, as regras técnicas necessárias para a criação de ligações entre os dados de diferentes sistemas de informação da UE, através de atos de execução. Os referidos atos de execução são dotados pelo procedimento de exame a que se refere o artigo 70.º, n.º 2.

Artigo 29.º

Verificação manual das diferentes identidades e autoridades responsáveis

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

a) O gabinete SIRENE do Estado-Membro para correspondências que ocorreram aquando da criação ou atualização de uma indicação no SIS em conformidade com o Regulamento (UE) 2018/1862;

b) Autoridades centrais do Estado-Membro de condenação ao registar ou alterar correspondências no ECRIS-TCN nos termos do artigo 5.º ou do artigo 9.º do Regulamento (UE) 2019/816.

O MID deve indicar a autoridade responsável pela verificação manual das diferentes identidades no processo de confirmação da identidade.

2. A autoridade responsável pela verificação manual das diferentes identidades 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 numa indicação relativa a:

a) Pessoas procuradas para efeitos de detenção, entrega ou extradição, tal como referido no artigo 26.º do Regulamento (UE) 2018/1862;

b) Pessoas desaparecidas ou vulneráveis, tal como referido no artigo 32.º do Regulamento (UE) 2018/1862;

c) Pessoas procuradas no âmbito de um processo judicial, tal como referido no artigo 34.º do Regulamento (UE) 2018/1862;

d) Pessoas para efeitos de vigilância discreta, controlo de verificação ou de controlo específico referido no artigo 36.º do Regulamento (UE) 2018/1862.

3. A autoridade responsável pela verificação manual das diferentes identidades deve ter acesso aos dados ligados contidos no ficheiro de confirmação de identidade pertinente e aos dados de identificação ligados nos sistemas de informação pertinentes e, se for caso disso, no SIS. A referida autoridade deve avaliar sem demora as diversas identidades. Uma vez concluída a avaliação, deve 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. No caso de mais de uma ligação, a autoridade responsável pela verificação das diferentes identidades deve avaliar cada ligação separadamente.

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

Artigo 30.º

Ligação amarela

1. Quando a verificação manual das diferentes identidades não tiver sido feita, deve ser classificada a amarelo uma ligação entre os dados de dois ou mais sistemas de informação da UE em qualquer dos seguintes casos:

a) Os dados ligados partilham os mesmos dados biométricos, mas têm dados de identificação similares ou diferentes e;

b) Os dados ligados possuem dados de identificação diferentes mas partilham os mesmos dados do documento de viagem, e pelo menos um dos sistemas de informação da UE não dispõe de dados biométricos da pessoa em causa;

c) Os dados ligados partilham os mesmos dados de identificação, mas têm dados biométricos diferentes;

d) Os dados ligados têm dados de identificação similares ou diferentes e partilham os mesmos dados do documento de viagem, mas têm dados biométricos diferentes.

2. Quando uma ligação é classificada a amarelo, nos termos do 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 da UE deve ser classificada como verde se:

a) Os dados ligados têm dados biométricos diferentes, mas partilham os mesmos dados de identificação e a autoridade responsável pela verificação manual das diferentes identidades concluiu que os dados ligados se referem a duas pessoas diferentes;

b) Os dados ligados têm dados biométricos diferentes, têm dados de identificação similares ou diferentes e partilham os mesmos dados do documento de viagem, e a autoridade responsável pela verificação manual das diferentes identidades concluiu que os dados ligados se referem a duas pessoas diferentes;

c) Os dados ligados têm dados de identificação diferentes, mas partilham os mesmos dados do documento de viagem, pelo menos um dos sistemas de informação da UE não dispõe de dados biométricos sobre a pessoa e a autoridade responsável pela verificação manual das diferentes identidades concluiu que os dados ligados se referem a duas pessoas diferentes.

2. Quando o CIR ou o SIS são consultados e se existe uma ligação verde entre dados em dois ou mais sistemas de informação da UE, o MID indica que os dados de identificação dos dados ligados não correspondem à mesma pessoa.

3. A autoridade de um Estado-Membro deve verificar os dados pertinentes armazenados no CIR e no SIS e, se necessário, retificar ou apagar sem demora a ligação do MID, caso tenha indícios de que uma ligação verde foi registada de forma incorreta no MID, ou que uma ligação verde está desatualizada ou de que foram tratados dados no MID ou nos sistemas de informação da UE em violação do presente regulamento. Essa autoridade do Estado-Membro deve informar sem demora o Estado-Membro responsável pela verificação manual das diferentes identidades.

Artigo 32.º

Ligação vermelha

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

a) Os dados ligados partilham os mesmos dados biométricos, mas apresentam dados de identificação similares ou diferentes e a autoridade responsável pela verificação manual das diferentes identidades concluiu que os dados ligados se referem, de forma injustificada, à mesma pessoa;

b) Os dados ligados possuem os mesmos dados de identificação ou dados de identificação semelhantes ou diferentes e os mesmos dados do documento de viagem, mas dados biométricos diferentes, e a autoridade responsável pela verificação manual das diferentes identidades concluiu que os dados ligados se referem a duas pessoas diferentes em que, pelo menos uma, utiliza o mesmo documento de viagem de forma injustificada.

c) Os dados ligados partilham os mesmos dados de identificação, mas têm dados biométricos diferentes e os dados do documento de viagem são diferentes ou inexistentes, e a autoridade responsável pela verificação manual das diferentes identidades concluiu que os dados ligados se referem, de forma injustificada, a duas pessoas diferentes;

d) Os dados ligados têm dados de identificação diferentes e partilham os mesmos dados de documento de viagem, pelo menos um dos sistemas de informação da UE não dispõe de dados biométricos sobre a pessoa e a autoridade responsável pela verificação manual das diferentes identidades concluiu que os dados ligados se referem, de forma injustificada, à mesma pessoa.

2. Quando o CIR ou o SIS são consultados e existe uma ligação vermelha entre dados de dois ou mais sistemas de informação da UE, o MID indica 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, e as eventuais consequências jurídicas para a pessoa baseiam-se apenas nos dados pertinentes sobre essa pessoa. Nenhuma consequência jurídica deverá advir para a pessoa com base, exclusivamente, na existência de uma ligação vermelha.

3. Nos casos em que é criada uma ligação vermelha entre os dados do SES, do VIS, ETIAS, Eurodac ou do ECRIS-TCN, o processo individual, guardado no CIR deve ser atualizado em conformidade com o artigo 19.º, n.º 2.

4. Sem prejuízo das disposições relativas ao tratamento de indicações no SIS referidas nos Regulamentos (UE) 2018/1860, (UE) 2018/1861 e (UE) 2018/1862, 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 ligação vermelha é criada, a autoridade responsável pela verificação manual das diferentes identidades deve informar a pessoa em causa da existência de múltiplos dados de identificação ilegais e fornecer-lhe, por escrito, um número de identificação único, tal como referido no artigo 34.º, alínea c), do presente regulamento, uma referência à autoridade responsável pela verificação manual das diferentes identidades, tal como referido no artigo 34.º, alínea d), do presente regulamento, e o endereço do portal Web criado nos termos do artigo 49.º do presente regulamento.

5. A informação a que se refere o n.º 4, deve ser dada por escrito pela autoridade responsável pela verificação manual das diferentes identidades por meio de um formulário normalizado. A Comissão determina o conteúdo e apresentação desse formulário através de atos de execução. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 70.º, n.º 2.

6. Nos casos em que uma ligação vermelha é criada, o MID notifica as autoridades responsáveis pelos dados ligados de forma automatizada.

7. Se uma autoridade de um Estado-Membro ou uma agência da União com acesso ao CIR ou ao SIS tiver indícios de que uma ligação vermelha foi registada de forma incorreta no MID ou de que os dados tratados no MID, no CIR ou no SIS foram tratados em violação do presente regulamento, essa autoridade ou agência deve verificar os dados relevantes armazenados no CIR e no SIS e deve:

a) Caso a ligação diga respeito a uma das indicações do SIS a que se refere o artigo 29.º, n.º 2, informar imediatamente o gabinete SIRENE do Estado-Membro que criou a indicação no SIS;

b) Nos restantes casos, retificar ou apagar imediatamente a ligação do MID.

Caso o gabinete SIRENE seja contactado nos termos da alínea a), do primeiro parágrafo, o gabinete deve verificar os elementos de prova fornecidos pela autoridade do Estado-Membro ou a agência da União e, se for caso disso, retificar ou apagar imediatamente a ligação do MID.

A autoridade do Estado-Membro que obtém os elementos de prova deve informar sem demora a autoridade do Estado-Membro responsável pela verificação manual das diferentes identidades, indicando, se for caso disso, uma eventual retificação ou apagamento de uma ligação vermelha.

Artigo 33.º

Ligação branca

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

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

b) Os dados ligados partilham os mesmos dados de identificação ou dados de identificação semelhantes, os mesmos dados do documento de viagem e pelo menos um dos sistemas de informação da UE não dispõe de dados biométricos da pessoa;

c) Os dados ligados partilham os mesmos dados biométricos e os mesmos dados do documento de viagem, e dados de identificação similares;

d) Os dados ligados partilham os mesmos dados biométricos, mas têm dados de identificação similares ou diferentes e a autoridade responsável pela verificação manual das diferentes identidades concluiu que os dados ligados se referem justificadamente à mesma pessoa.

2. Quando o CIR ou o SIS são consultados e existe uma ligação branca entre dados de um ou mais dos sistemas de informação da UE, o MID indica que os dados de identificação de dados ligados correspondem à mesma pessoa. Os sistemas de informação da UE consultados respondem indicando, se for caso disso, todos os dados ligados sobre a pessoa, desencadeando assim uma correspondência 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. Nos casos em que é criada uma ligação branca entre os dados do SES, do VIS, do ETIAS, do Eurodac ou do ECRIS-TCN, o processo individual, guardado no CIR deve ser atualizado em conformidade com o artigo 19.º, n.º 2.

4. Sem prejuízo das disposições relativas ao tratamento de indicações no SIS constantes dos Regulamentos (UE) 2018/1860, (UE) 2018/1861 e (UE) 2018/1862, e sem prejuízo das restrições necessárias para proteger a segurança e a ordem pública, prevenir o crime e garantir que nenhuma investigação nacional será prejudicada, sempre que é criada uma ligação branca na sequência de uma verificação manual das diferentes identidades, a autoridade responsável pela verificação das diferentes identidades deve informar a pessoa em causa sobre a existência de dados de identificação similares ou diferentes e fornecer-lhe um número de identificação único, tal como referido no artigo 34.º, alínea c), do presente regulamento, uma referência à autoridade responsável pela verificação manual das diferentes identidades, tal como referido no artigo 34.º, alínea d), do presente regulamento e o endereço do portal Web criado nos termos do artigo 49.º do presente regulamento.

5. A autoridade de um Estado-Membro deve verificar os dados pertinentes armazenados no CIR e no SIS e, se necessário, retificar ou apagar sem demora a ligação do MID, caso tenha indícios de que uma ligação branca foi registada de forma incorreta no MID, ou que uma ligação branca está desatualizada ou de que foram tratados dados no MID ou nos sistemas de informação da UE em violação do presente regulamento. Essa autoridade do Estado-Membro deve informar sem demora o Estado-Membro responsável pela verificação manual das diferentes identidades.

6. A informação a que se refere o n.º 4 deve ser dada por escrito pela autoridade responsável pela verificação manual das diferentes identidades por meio de um formulário normalizado. A Comissão determina o conteúdo e a apresentação desse formulário através de atos de execução. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 70.º, n.º 2.

Artigo 34.º

Processo de confirmação de identidade

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

a) As ligações, tal como referidas nos artigos 30.º a 33.º;

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

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

d) A autoridade responsável pela verificação manual das diferentes identidades;

e) A data de criação ou de atualização da ligação.

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 MID apenas enquanto os dados permanecerem armazenados em dois ou mais sistemas de informação da UE. Os processos de confirmação de identidade e respetivos dados, devem ser apagados do MID de forma automatizada.

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 o seguinte:

a) O Estado-Membro que inicia a consulta;

b) O objetivo do acesso do utilizador;

c) A data e a hora da consulta;

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

e) A referência aos dados ligados;

f) O histórico do processo de confirmação de identidade.

2. Cada Estado-Membro deve manter registos das consultas feitas pelas suas autoridades e pelo pessoal das autoridades devidamente autorizado a utilizar o MID. Cada agência da União deve manter registos das consultas feitas pelo seu pessoal devidamente autorizado a utilizar o MID.

3. Os registos referidos nos n.os 1 e 2 só podem ser utilizados para controlo da proteção de dados, incluindo a verificação da admissibilidade de uma consulta e da legalidade do tratamento dos dados, bem como para garantir a sua segurança e integridade. Esses registos devem estar protegidos por medidas adequadas contra o acesso não autorizado e apagados um ano após a sua criação. Se, no entanto, forem necessários para procedimentos de controlo que já tenham tido início, esses registos devem ser apagados logo que deixarem de ser necessários para o efeito.

CAPÍTULO VI

Medidas de apoio à interoperabilidade

Artigo 37.º

Qualidade dos dados

1. Sem prejuízo das responsabilidades dos Estados-Membros em matéria de qualidade dos dados introduzidos nos sistemas, a eu-LISA deve criar mecanismos e procedimentos automatizados de controlo de qualidade de dados sobre os dados armazenados no SIS, Eurodac, ECRIS-TCN, serviço partilhado BMS e no CIR.

2. A eu-LISA deve implementar mecanismos para avaliar a exatidão do serviço partilhado BMS, indicadores comuns de qualidade dos dados e as normas mínimas de qualidade para armazenar os dados no SIS, Eurodac, ECRIS-TCN, serviço partilhado BMS e CIR.

Só os dados que cumpram as normas mínimas de qualidade podem ser introduzidos no SIS, Eurodac, ECRIS-TCN, serviço partilhado BMS, no CIR e no 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. A eu-LISA deve também facultar o referido relatório ao Parlamento Europeu e ao Conselho, mediante pedido. Os relatórios apresentados nos termos do presente número não podem conter quaisquer dados pessoais.

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 SIS, Eurodac, ECRIS-TCN, no serviço partilhado BMS e no CIR, em especial no que se refere aos dados biométricos, devem ser estabelecidos em atos de execução. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 70.º, n.º 2.

5. Um ano após a criação dos mecanismos e procedimentos automatizados de controlo da qualidade dos dados, indicadores comuns da qualidade dos dados e normas mínimas de 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, em especial, os problemas de qualidade dos dados devido a dados erróneos armazenados nos sistemas de informação da UE. Os Estados-Membros comunicam periodicamente à Comissão quaisquer progressos na aplicação deste 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, ao Comité Europeu para a Proteção de Dados e à Agência dos Direitos Fundamentais da União Europeia, criada pelo Regulamento (CE) n.º 168/2007 do Conselho ([37]).

Artigo 38.º

Formato de mensagem universal

1. O presente artigo estabelece a norma relativa ao Formato de Mensagem Universal (UMF). A UMF define as normas relativas a determinado conteúdo de intercâmbio de informações transfronteiriço, entre sistemas de informação, autoridades ou organizações no domínio da Justiça e Assuntos Internos.

([37]) 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).

2. A norma UMF deve ser utilizada no desenvolvimento do Eurodac, do ECRIS-TCN, do ESP, do CIR, do MID e, sempre que viável e, se for caso disso, no desenvolvimento pela eu-LISA ou por qualquer outra agência da União de novos modelos de intercâmbio de informações e de sistemas de informação da União no domínio da Justiça e Assuntos Internos.

3. A Comissão deve adotar um ato de execução para estabelecer e desenvolver a norma UMF referida no n.º 1 do presente artigo. O referido ato de execução é adotado pelo procedimento de exame a que se refere o artigo 70.º, n.º 2.

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 Eurodac, do SIS e do ECRIS-TCN, em conformidade com os respetivos atos jurídicos que regem esses sistemas, e para fornecer 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 e as estatísticas referidos no artigo 74.º do Regulamento (UE) 2018/1862 e no artigo 32.º do Regulamento (UE) 2019/816, logicamente separados pelo sistema de informação da UE. O acesso ao CRRS deve ser concedido mediante um acesso seguro 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 74.º do Regulamento (UE) 2018/1862 e o artigo 32.º do Regulamento (UE) 2019/816.

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

Os dados contidos no CRRS não podem permitir a identificação de pessoas.

4. O CRRS é constituído por:

a) Os instrumentos necessários para tornar os dados anónimos;

b) Uma infraestrutura central, constituída por um repositório de dados anónimos;

c) Uma infraestrutura de comunicação segura para ligar o CRRS ao SIS, Eurodac e ao ECRIS-TCN, bem como às infraestruturas centrais do BMS, do CIR e MID.

5. A Comissão deve adotar um ato delegado nos termos do artigo 69.º a fim de 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 do presente artigo e regras de segurança aplicáveis ao repositório.

CAPÍTULO VII

Proteção de dados

Artigo 40.º

Responsável pelo tratamento de dados

1. No que respeita ao tratamento dos dados no serviço partilhado BMS, as autoridades dos Estados-Membros que são responsáveis pelo tratamento de dados do Eurodac, SIS e ECRIS-TCN, respetivamente, devem ser igualmente consideradas responsáveis pelo tratamento dos dados, em conformidade com o artigo 4.º, ponto 7, do Regulamento (UE) 2016/679 ou o artigo 3.º, ponto 8, da Diretiva (UE) 2016/680, no que diz respeito aos modelos biométricos obtidos a partir dos dados referidos no artigo 13.º do presente regulamento introduzidos nos sistemas respetivos, sendo responsáveis pelo tratamento dos modelos biométricos no serviço partilhado BMS.

2. No que respeita ao tratamento de dados no CIR, as autoridades dos Estados-Membros que são responsáveis pelo tratamento de dados para o Eurodac e o ECRIS-TCN, respetivamente, devem ser responsáveis pelo tratamento dos dados, em conformidade com o artigo 4.º, ponto 7, do Regulamento (UE) 2016/679 ou o artigo 3.º, ponto 8 da Diretiva (UE) 2016/680, no respeitante aos dados referidos no artigo 18.º do presente regulamento introduzidos nos sistemas respetivos, sendo responsáveis pelo tratamento desses dados pessoais no CIR.

3. No que respeita ao tratamento dos dados no MID:

a) A Agência Europeia da Guarda de Fronteiras e Costeira é responsável pelo tratamento dos dados na aceção do artigo 3.º, ponto 8, do Regulamento (UE) 2018/1725, 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 responsáveis pelo tratamento, em conformidade com o artigo 4.º, ponto 7, do Regulamento (UE) 2016/679 ou o artigo 3.º, ponto 8, da Diretiva (UE) 2016/680, sendo responsáveis pelo tratamento dos dados pessoais no MID.

4. Para efeitos de controlo da proteção de dados, nomeadamente para verificação da admissibilidade de uma consulta e da legalidade do tratamento dos dados, os responsáveis pelo tratamento devem ter acesso aos registos referidos nos artigos 10.º, 16.º, 24.º e 36.º para fins de autocontrolo, como referido no artigo 44.º.

Artigo 41.º

Subcontratante de dados

No que respeita ao tratamento de dados pessoais no serviço partilhado BMS, no CIR e no MID, a eu-LISA deve ser um subcontratante de dados na aceção do artigo 3.º, ponto 12, alínea a), do Regulamento (UE) 2018/1725.

Artigo 42.º

Segurança do tratamento

1. A eu-LISA, a unidade central do ETIAS, a Europol e as autoridades dos Estados-Membros devem garantir que a segurança do tratamento dos dados pessoais decorre de acordo com o presente regulamento. A eu-LISA, a unidade central do ETIAS, a Europol e as autoridades dos Estados-Membros devem cooperar em tarefas relacionadas com a segurança.

2. Sem prejuízo do artigo 33.º do Regulamento (UE) 2018/1725, 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) Recusar o acesso de pessoas não autorizadas ao equipamento e às instalações de tratamento de dados;

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

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

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

f) Impedir a utilização dos sistemas de tratamento automatizado de dados por pessoas não autorizadas que utilizam equipamentos de comunicação de dados;

g) 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;

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

i) 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;

j) 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;

k) Assegurar que, em caso de interrupção, seja possível restaurar o funcionamento normal dos sistemas instalados;

l) Assegurar a fiabilidade assegurando que as eventuais falhas no funcionamento dos componentes de interoperabilidade sejam devidamente comunicadas;

m) 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 e avaliar essas medidas de segurança à luz dos novos desenvolvimentos tecnológicos.

4. Os Estados-Membros, a Europol e a unidade central do ETIAS 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

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 ou 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 sem demora a Comissão, a eu-LISA, as autoridades de controlo competentes e a Autoridade Europeia para a Proteção de Dados de quaisquer incidentes de segurança.

Sem prejuízo dos artigos 34.º e 35.º do Regulamento (UE) 2018/1725 e do artigo 34.º do Regulamento (UE) 2016/794, a unidade central do ETIAS e a Europol devem notificar sem demora a Comissão, a eu-LISA e a Autoridade Europeia para a Proteção de Dados de quaisquer incidentes de segurança.

Em caso de incidente de segurança em relação aos componentes de interoperabilidade da infraestrutura central, a eu-LISA deve notificar sem demora 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 ou confidencialidade dos dados devem ser facultadas sem demora aos Estados-Membros, à unidade central do ETIAS e à Europol, e comunicadas em conformidade com o plano de gestão de incidentes fornecido pela eu-LISA.

5. Os Estados-Membros em causa, a unidade central do ETIAS, a Europol 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. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 70.º, n.º 2.

Artigo 44.º

Autocontrolo

Os Estados-Membros e as agências competentes da União devem assegurar que cada autoridade com direito de acesso aos componentes de interoperabilidade toma as medidas necessárias para controlar o cumprimento do presente 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 através da verificação dos registos referidos nos artigos 10.º, 16.º, 24.º e 36.º, e cooperar, se necessário, com as autoridades de controlo e a Autoridade Europeia para a Proteção de Dados.

Artigo 45.º

Sanções

Os Estados-Membros asseguram que toda a utilização abusiva de dados, tratamento de dados ou intercâmbio de dados que viole o disposto no presente regulamento seja punível nos termos da legislação nacional. As sanções previstas devem ser efetivas, proporcionadas e dissuasoras.

Artigo 46.º

Responsabilidade

1. Sem prejuízo do direito à indemnização e das obrigações do responsável pelo tratamento dos dados ou do subcontratante nos termos do Regulamento (UE) 2016/679, da Diretiva (UE) 2016/680 e do Regulamento (UE) 2018/1725:

a) Qualquer pessoa ou Estado-Membro que tenha sofrido danos materiais ou imateriais em virtude de uma operação ilícita de tratamento de dados pessoais ou de qualquer outro ato incompatível com o presente regulamento levado a cabo por um Estado-Membro tem direito a ser indemnizado por esse Estado-Membro;

b) Qualquer pessoa ou qualquer Estado-Membro que tenha sofrido um dano material ou imaterial em virtude de um ato incompatível com o presente regulamento levado a cabo pela Europol, a Agência Europeia da Guarda de Fronteiras e Costeira ou a eu-LISA tem direito a ser indemnizado pela agência em causa.

O Estado-Membro em causa, a Europol, a Agência Europeia da Guarda de Fronteiras e Costeira ou a eu-LISA ficam, total ou parcialmente, exonerados da sua responsabilidade por força do primeiro parágrafo, se provarem que o evento que deu origem ao dano não lhes é imputável.

2. Se o incumprimento por um Estado-Membro das obrigações que lhe incumbem por força do presente regulamento causar danos aos componentes de interoperabilidade, esse Estado-Membro é responsável pelos danos, a menos e na medida em que a eu-LISA ou outro Estado-Membro vinculado pelo presente regulamento não tenha tomado medidas razoáveis para prevenir os danos ou minimizar o seu impacto.

3. Os pedidos de indemnização a um Estado-Membro pelos danos referidos nos n.os 1 e 2 são regulados pelo direito interno do Estado-Membro requerido. Os pedidos de indemnização apresentados ao responsável pelo tratamento dos dados ou à eu-LISA pelos danos referidos nos n.os 1 e 2 ficam sujeitos às condições previstas nos Tratados.

Artigo 47.º

Direito à informação

1. A autoridade responsável pela recolha de dados das pessoas cujos dados são conservados no serviço partilhado BMS, no CIR ou no MID deve facultar às pessoas cujos dados são recolhidos as informações previstas nos termos dos artigos 13.º e 14.º do Regulamento (UE) 2016/679, dos artigos 12.º e 13.º da Diretiva (UE) 2016/680 e dos artigos 15.º e 16.º do Regulamento (UE) 2018/1725. A autoridade deve fornecer as informações no momento da recolha desses dados.

2. Todas as informações devem ser disponibilizadas em linguagem clara e simples, numa versão linguística que a pessoa em causa compreenda ou que se espere, de forma razoável, que compreenda. Tal deve incluir o fornecimento de informações de uma maneira adequada à idade dos titulares de dados que sejam menores.

3. As regras sobre o direito à informação constantes das disposições sobre a proteção de dados da União são aplicáveis aos dados pessoais registados no ECRIS-TCN e tratados para efeitos do presente regulamento.

Artigo 48.º

Direito de acesso, de retificação e de apagamento de dados pessoais armazenados no MID, e limitação do tratamento desses dados

1. A fim de exercer os seus direitos ao abrigo dos artigos 15.º a 18.º do Regulamento (UE) 2016/679, dos artigos 17.º a 20.º do Regulamento (UE) 2018/1725 e dos artigos 14.º a 16.º da Diretiva (UE) 2016/680, qualquer pessoa tem o direito de se dirigir à autoridade competente de qualquer Estado-Membro, que deve examinar e responder ao pedido.

2. O Estado-Membro que examina o pedido deve responder sem demora injustificada e, em qualquer caso, no prazo de 45 dias a contar da receção do pedido. Esse prazo pode ser prorrogado por 15 dias, se necessário, tendo em conta a complexidade e o número de pedidos. O Estado-Membro que examina o pedido deve informar o titular dos dados de qualquer prorrogação e dos motivos da demora, no prazo de 45 dias a contar da data de receção do pedido. Os Estados-Membros podem decidir que estas respostas sejam dadas pelos serviços centrais.

3. Se for apresentado um pedido de retificação ou apagamento de dados pessoais a um Estado-Membro diferente do Estado-Membro responsável pela verificação manual das diferentes identidades, o Estado-Membro ao qual foi apresentado o pedido deve contactar as autoridades do Estado-Membro responsável pela verificação manual das diferentes identidades no prazo de sete dias. O Estado-Membro responsável pela verificação manual das diferentes identidades deve verificar a exatidão dos dados e a legalidade do tratamento dos dados sem demora injustificada e, em qualquer caso, no prazo de 30 dias a contar desse contacto. Esse prazo pode ser prorrogado por mais 15 dias, se necessário, tendo em conta a complexidade e o número de pedidos. O Estado-Membro responsável pela verificação manual das diferentes identidades informa o Estado-Membro, ao qual foi apresentado o pedido, da prorrogação do prazo bem como a sua fundamentação. O Estado-Membro que contactou a autoridade do Estado-Membro responsável pela verificação manual das diferentes identidades informa a pessoa em causa sobre o procedimento subsequente.

4. Se for apresentado um pedido de retificação ou apagamento de dados pessoais a um Estado-Membro em que a unidade central do ETIAS foi responsável pela verificação manual das diferentes identidades, o Estado-Membro ao qual foi apresentado o pedido deve contactar a unidade central do ETIAS no prazo de sete dias para solicitar que emita parecer sem demora injustificada. A unidade central do ETIAS emite parecer, sem demora injustificada, qualquer caso, no prazo de 30 dias a contar desse contacto. Esse prazo pode ser prorrogado por mais 15 dias, se necessário, tendo em conta a complexidade e o número de pedidos. O Estado-Membro que contactou a autoridade do Estado-Membro responsável pela verificação manual das diferentes identidades informa a pessoa em causa sobre o procedimento subsequente.

5. Sempre que, na sequência de um exame, se concluir que os dados armazenados no MID são inexatos ou foram registados ilegalmente, o Estado-Membro responsável pela verificação manual das diferentes identidades ou, caso não tenha havido um Estado-Membro responsável pela verificação manual das diferentes identidades ou se a unidade central do ETIAS tiver sido responsável pela verificação manual das diferentes identidades, o Estado-Membro ao qual foi apresentado o pedido, deve proceder à sua retificação ou ao seu apagamento sem demora injustificada. A pessoa em causa deve ser informada por escrito de que os seus dados foram retificados ou apagados.

6. Caso os dados armazenados no MID sejam alterados por um Estado-Membro durante o respetivo período de conservação, esse Estado-Membro 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 correspondência, o Estado-Membro em causa deve apagar os dados do processo de confirmação de identidade. Sempre que o tratamento automatizado comunicar uma ou várias correspondências, o Estado-Membro em causa deve criar ou atualizar a ligação em questão em conformidade com as disposições aplicáveis do presente regulamento.

7. Sempre que o Estado-Membro responsável pela verificação manual das diferentes identidades ou, se for caso disso, o Estado-Membro ao qual foi apresentado o pedido não considerar que os dados armazenados no MID são 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.

8. A decisão a que se refere o n.º 7 deve informar também o interessado sobre a possibilidade de impugnar a decisão tomada relativamente ao pedido de acesso, retificação, apagamento ou limitação do tratamento de dados pessoais 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 de controlo competentes.

9. Qualquer pedido de acesso, retificação, apagamento ou limitação do tratamento de dados pessoais 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 presente artigo, após o que serão imediatamente apagadas.

10. O Estado-Membro responsável pela verificação manual das diferentes identidades ou, se for caso disso, o Estado-Membro ao qual foi apresentado o pedido, deve conservar um registo relativo à apresentação de um pedido de acesso, retificação, apagamento ou limitação do tratamento de dados pessoais, e disponibilizar sem demora esse registo às autoridades de controlo.

11. O presente artigo aplica-se sem prejuízo das limitações e restrições aos direitos previstos no presente artigo nos termos do Regulamento (UE) 2016/679 e da Diretiva (UE) 2016/680.

Artigo 49.º

Portal Web

1. É criado um portal Web com o objetivo de facilitar o exercício dos direitos de acesso, retificação, apagamento ou de limitação do tratamento de dados pessoais.

2. O portal Web deve conter informações sobre os direitos e procedimentos referidos nos artigos 47.º e 48.º e uma interface do utilizador que permita às pessoas cujos dados são tratados através do MID e que foram informadas da presença de uma ligação vermelha, em conformidade com o artigo 32.º, n.º 4, receber os dados de contacto da autoridade competente do Estado-Membro responsável pela verificação manual das identidades diferentes.

3. A fim de obter os dados de contacto da autoridade competente do Estado-Membro responsável pela verificação manual das diferentes identidades, a pessoa cujos dados são tratados através do MID deve inserir a referência à autoridade responsável pela verificação manual das diferentes identidades referidas no artigo 34.º, alínea d). O portal Web deve utilizar esta referência para obter os dados de contacto da autoridade competente do Estado-Membro responsável pela verificação manual das diferentes identidades. O portal Web deve também incluir um modelo de mensagem de correio eletrónico para facilitar a comunicação entre o utilizador do portal e a autoridade competente do Estado-Membro responsável pela verificação manual das diferentes identidades. Essa mensagem deve incluir um campo relativo ao número de identificação único referido no artigo 34.º, alínea c), a fim de permitir à autoridade competente do Estado-Membro responsável pela verificação manual das diferentes identidades a identificação dos dados em causa.

4. Os Estados-Membros devem fornecer à eu-LISA os dados de contacto de todas as autoridades competentes para examinar e responder a qualquer pedido, tal como referido nos artigos 47.º e 48.º, bem como avaliar regularmente se esses dados de contacto estão atualizados.

5. A eu-LISA deve desenvolver o portal Web, ficando responsável pela sua gestão técnica.

6. A Comissão deve adotar um ato delegado, nos termos do artigo 69.º, a fim de estabelecer regras pormenorizadas sobre o funcionamento do portal Web, incluindo a interface do utilizador, as línguas em que o portal deve estar disponível e o modelo de correio eletrónico.

Artigo 50.º

Comunicação de dados pessoais a países terceiros, organizações internacionais e entidades privadas

Sem prejuízo do disposto no artigo 31.º do Regulamento (CE) n.º 767/2008, nos artigos 25.º e 26.º do Regulamento (UE) 2016/794, no artigo 41.º do Regulamento (UE) 2017/2226, no artigo 65.º do Regulamento (UE) 2018/1240 e da consulta das bases de dados da Interpol através do ESP, em conformidade com o artigo 9.º, n.º 5, do presente regulamento, que cumpram as disposições do capítulo V do Regulamento (UE) 2018/1725 e do capítulo V do Regulamento (UE) 2016/679, os dados pessoais armazenados, tratados ou consultados pelos componentes de interoperabilidade não podem ser transferidos nem disponibilizados a países terceiros, organizações internacionais ou entidades privadas.

Artigo 51.º

Fiscalização pelas autoridades de controlo

1. Cada Estado-Membro assegura que as autoridades de controlo controlam de forma independente a licitude do tratamento dos dados pessoais referidos no presente regulamento pelo Estado-Membro em causa, incluindo a sua transmissão aos componentes de interoperabilidade e a partir dos mesmos.

2. Cada Estado-Membro assegura que as disposições nacionais legislativas, regulamentares e administrativas adotadas em virtude da Diretiva (UE) 2016/680 sejam igualmente aplicáveis, se for caso disso, ao acesso aos componentes de interoperabilidade pelas autoridades policiais e pelas autoridades designadas, inclusive no que respeita aos direitos das pessoas a cujos dados se tem assim acesso.

3. As autoridades de controlo devem garantir a realização de uma auditoria às operações de tratamento de dados pessoais pelas autoridades nacionais competentes para efeitos do presente regulamento em conformidade com as normas internacionais de auditoria aplicáveis, pelo menos de quatro em quatro anos.

As autoridades de controlo publicam anualmente o número de pedidos de retificação, apagamento, ou limitação do tratamento de dados pessoais, as medidas subsequentemente tomadas e o número de retificações, apagamentos e limitações de tratamento que tiveram lugar na sequência dos pedidos pelas pessoas em causa.

4. Os Estados-Membros devem assegurar que as autoridades de controlo dispõem dos meios e dos conhecimentos especializados necessários para cumprir as tarefas que lhes são confiadas no âmbito do presente regulamento.

5. Os Estados-Membros comunicam todas as informações solicitadas por qualquer uma das autoridades de controlo referidas no artigo 51.º, n.º 1, do Regulamento (UE) 2016/679 e, em especial, fornecem-lhe informações relativas às atividades desenvolvidas no âmbito das suas responsabilidades estabelecidas pelo presente regulamento. Os Estados-Membros concedem às autoridades de controlo referidas no artigo 51.º, n.º 1, do Regulamento (UE) 2016/679 o acesso aos seus registos referidos nos artigos 10.º, 16.º, 24.º e 36.º, do presente regulamento, às suas justificações referidas no artigo 22.º, n.º 2, do presente regulamento, e permitem-lhes o acesso, a qualquer momento, a todas as suas instalações utilizadas para fins de interoperabilidade.

Artigo 52.º

Auditorias pela Autoridade Europeia para a Proteção de Dados

A Autoridade Europeia para a Proteção de Dados deve garantir a realização de uma auditoria às operações de tratamento de dados pessoais pela eu-LISA, pela unidade central do ETIAS e pela Europol para efeitos do presente regulamento, 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, aos Estados-Membros e à agência da União em causa. Deve ser dada à eu-LISA, à unidade central do ETIAS e à Europol a oportunidade de efetuar comentários antes da adoção dos relatórios.

A eu-LISA, a unidade central do ETIAS e a Europol fornecem as informações solicitadas pela Autoridade Europeia para a Proteção de Dados, concedem à Autoridade Europeia para a Proteção de Dados o acesso a todos os documentos e aos seus registos referidos nos artigos 10.º, 16.º, 24.º e 36.º, e permitem à Autoridade Europeia para a Proteção de Dados o acesso permanente a todas as suas instalações.

Artigo 53.º

Cooperação entre as autoridades de controlo e a Autoridade Europeia para a Proteção de Dados

1. As autoridades de controlo e a Autoridade Europeia para a Proteção de Dados, agindo cada uma no âmbito das respetivas competências, cooperam ativamente no âmbito das respetivas responsabilidades e asseguram a supervisão coordenada da utilização dos componentes de interoperabilidade e a aplicação das restantes disposições do presente regulamento, em particular se a Autoridade Europeia para a Proteção de Dados ou uma autoridade 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.

2. Nos casos referidos no n.º 1 do presente artigo, o controlo coordenado deve ser assegurado nos termos do artigo 62.º do Regulamento (UE) 2018/1725.

3. O Comité Europeu para a Proteção de Dados deve enviar um relatório de atividades nos termos do presente artigo conjunto ao Parlamento Europeu, ao Conselho, à Comissão, à Europol, à Agência Europeia da Guarda de Fronteiras e Costeira e à eu-LISA até 12 de junho de 2021 e, posteriormente, de dois em dois anos. O referido relatório deve incluir um capítulo sobre cada Estado-Membro, elaborado pela respetiva autoridade de controlo.

CAPÍTULO VIII

Responsabilidades

Artigo 54.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 desempenho a que se refere o artigo 55.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, do Eurodac, e do ECRIS-TCN, e o ESP, o serviço partilhado BMS, o CIR, o MID e o CRRS.

Sem prejuízo do disposto no artigo 62.º, não tem acesso a nenhum dos dados pessoais tratados através do ESP, do serviço partilhado BMS, do CIR e do MID.

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 SIS, Eurodac ou ECRIS-TCN 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 no artigo 8.º, n.º 2, artigo 9.º, n.º 7, artigo 28.º, n.ºs 5 e 7, artigo 37.º, n.º 4, artigo 38.º, n.º 3, artigo 39.º, n.º 5, artigo 43.º, n.º 5 e no artigo 74.º, n.º 10.

O desenvolvimento deve consistir na elaboração e implementação das especificações técnicas, nos testes e na gestão e coordenação globais 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. Este 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 71.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 pelo direito da União pelos atos jurídicos que regem o desenvolvimento, o estabelecimento, o funcionamento e a utilização de todos os sistemas de informação da UE e que irão participar nos componentes de interoperabilidade.

5. O Conselho de Gestão do Programa deve reunir-se periodicamente 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 da eu-LISA 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 atos jurídicos que regem o desenvolvimento, o estabelecimento, o funcionamento e a utilização de todos os sistemas de informação da UE e que irão participar nos componentes de interoperabilidade

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

O Grupo Consultivo de Interoperabilidade, referido no artigo 71.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 55.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 dos componentes de interoperabilidade, incluindo a sua manutenção e integração dos desenvolvimentos tecnológicos. Em cooperação com os Estados-Membros, deve assegurar que seja usada 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 e soluções técnicas necessárias para manter o funcionamento dos componentes de interoperabilidade e que prestam serviços ininterruptos aos Estados-Membros e às agências da União 24 horas por dia e 7 dias por semana, em conformidade com o presente regulamento. A gestão técnica dos componentes de interoperabilidade deve incluir 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.

Todos os componentes de interoperabilidade devem ser desenvolvidos e geridos de forma a assegurar um acesso rápido, contínuo, eficiente e controlado, assim como a disponibilidade total e ininterrupta dos componentes e dos dados armazenados no MID, no serviço partilhado BMS e no CIR, e um tempo de resposta adaptado às necessidades operacionais das autoridades dos Estados-Membros e das agências da União.

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 ao 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.

Sem prejuízo do artigo 62.º, a eu-LISA não tem acesso a nenhum dos dados pessoais tratados através do ESP, do serviço partilhado BMS, do CIR e do MID.

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 BMS e no CIR 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 56.º

Responsabilidades dos Estados-Membros

1. Cada Estado-Membro é responsável pela:

a) Ligação à infraestrutura de comunicação do ESP e ao CIR;

b) Integração dos sistemas e infraestruturas nacionais existentes com o ESP, o CIR e o MID;

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 das autoridades nacionais competentes ao ESP, ao CIR e ao MID 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.ºs 5 e 6, a fim de aceder ao CIR para efeitos de identificação;

f) Verificação manual das diferentes identidades a que se refere o artigo 29.º;

g) Cumprimento dos requisitos de qualidade dos dados estabelecidos na legislação da União;

h) Pleno cumprimento das regras de cada sistema de informação da UE para garantir a segurança e a integridade dos dados pessoais;

i) 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 ao CIR.

Artigo 57.º

Responsabilidades da Europol

1. A Europol deve assegurar o tratamento das consultas dos dados da Europol efetuadas pelo ESP. A Europol deve adaptar em consequência a sua interface de interrogação dos sistemas da Europol («Querying Europol Systems» — QUEST) para dados com o nível básico de proteção (BPL).

2. A Europol deve ser responsável pela gestão e disposições relativas à utilização e acesso por parte do pessoal devidamente autorizado ao ESP e ao CIR em conformidade com o presente regulamento, e a criação e atualização periódica de uma lista dos membros do pessoal e respetivos perfis.

Artigo 58.º

Responsabilidades da unidade central do ETIAS

A unidade central do ETIAS é responsável pela:

a) Verificação manual das diferentes identidades, nos termos do artigo 29.º;

b) Realização de uma deteção de identidades múltiplas entre os dados armazenados no SES, VIS, Eurodac e SIS referidos no artigo 65.º.

CAPÍTULO IX

Alteração de outros atos jurídicos da União

Artigo 59.º

Alteração do Regulamento (UE) 2018/1726

O Regulamento (UE) 2018/1726 é alterado do seguinte modo:

1) O artigo 12.º passa a ter a seguinte redação:

«*Artigo 12.º*

Qualidade dos dados

1. Sem prejuízo das responsabilidades dos Estados-Membros em relação aos dados introduzidos nos sistemas sob a responsabilidade operacional da Agência, esta, em estreita cooperação com os seus grupos consultivos, estabelece, para todos os sistemas sob a sua responsabilidade operacional, mecanismos e procedimentos automatizados de controlo da qualidade dos dados, indicadores comuns da qualidade dos dados, bem como as normas mínimas de qualidade para o armazenamento de dados, em conformidade com as disposições pertinentes dos atos jurídicos que regem os sistemas de dados e com o artigo 37.º dos Regulamentos (UE) 2019/817 (*) e (UE) 2019/818 (**) do Parlamento Europeu e do Conselho.

2. A Agência cria um repositório central contendo apenas dados anonimizados para a elaboração de relatórios e estatísticas em conformidade com o artigo 39.º do Regulamento (UE) 2019/817 e (UE) 2019/818, sujeitos a disposições específicas nos atos jurídicos que regem o desenvolvimento, a criação, o funcionamento e a utilização de sistemas informáticos de grande escala geridos pela Agência.

(*) Regulamento (UE) 2019/817 do Parlamento Europeu e do Conselho, de 20 de maio de 2019, relativo à criação de um regime de interoperabilidade entre os sistemas de informação da UE no domínio das fronteiras e vistos e que altera os Regulamentos (CE) n.º 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 do Parlamento Europeu e do Conselho, e as Decisões 2004/512/CE e 2008/633/JAI do Conselho (JO L 135 de 22.5.2019, p. 27).

(**) Regulamento (UE) 2019/818 do Parlamento Europeu e do Conselho, de 20 de maio de 2019, relativo à criação de um regime de interoperabilidade entre os sistemas de informação da UE no domínio da cooperação policial e judiciária, asilo e migração, e que altera os Regulamentos (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816 (JO L 135 de 22.5.2019, p. 85).».

2) No artigo 19.º, o n.º 1 é alterado do seguinte modo:

a) É inserida a seguinte alínea:

«e-ea) Adota relatórios sobre o ponto da situação do desenvolvimento dos componentes de interoperabilidade, nos termos do artigo 78.º, n.º 2, do Regulamento (UE) 2019/817 e do artigo 74.º, n.º 2 do Regulamento (UE) 2019/818.»;

b) A alínea f-f) passa a ter a seguinte redação:

«f-f) Adota relatórios sobre o funcionamento técnico do SIS, nos termos do artigo 60.º, n.º 7, do Regulamento (UE) 2018/1861 do Parlamento Europeu e do Conselho (*) e do artigo 74.º, n.º 8, do Regulamento (UE) 2018/1862 do Parlamento Europeu e do Conselho (**), do VIS, nos termos do artigo 50.º, n.º 3, do Regulamento (CE) n.º 767/2008 e do artigo 17.º, n.º 3, da Decisão 2008/633/JAI, do SES, nos termos do artigo 72.º, n.º 4, do Regulamento (UE) 2017/2226, do ETIAS, nos termos do artigo 92.º, n.º 4, do Regulamento (UE) 2018/1240 relativo ao ECRIS-TCN e à aplicação de referência ECRIS, nos termos do artigo 36.º, n.º 8, do Regulamento (UE) 2019/816 do Parlamento Europeu e do Conselho (***) e dos componentes de interoperabilidade, nos termos do artigo 78.º, n.º 3, do Regulamento (UE) 2019/817 e do artigo 74.º, n.º 3 do Regulamento (UE) 2019/818;

(*) Regulamento (UE) 2018/1861 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen (SIS) no domínio dos controlos de fronteira e que altera a Convenção de Aplicação do Acordo de Schengen e altera e revoga o Regulamento (CE) n.º 1987/2006 (JO L 312 de 7.12.2018, p. 14).

(**) Regulamento (UE) 2018/1862 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen (SIS) no domínio da cooperação policial e da cooperação judiciária em matéria penal, que altera e revoga a Decisão 2007/533/JAI do Conselho e revoga o Regulamento (CE) n.º 1986/2006 do Parlamento Europeu e do Conselho e a Decisão 2010/261/UE da Comissão (JO L 312 de 7.12.2018, p. 56).

(***) Regulamento (UE) 2019/816 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, que cria um sistema centralizado para a determinação dos Estados-Membros que possuem informações sobre condenações de nacionais de países terceiros e de apátridas tendo em vista completar e apoiar o Sistema Europeu de Informação sobre Registos Criminais (ECRIS-TCN) e que altera o Regulamento (UE) 2018/1726 (JO L 135 de 22.5.2019, p. 1).»;

c) A alínea h-h) passa a ter a seguinte redação:

«h-h) Adota observações formais sobre os relatórios da Autoridade Europeia para a Proteção de Dados em matéria de auditoria, nos termos do artigo 56.º, n.º 2, do Regulamento (UE) 2018/1861, do artigo 42.º, n.º 2, do Regulamento (CE) n.º 767/2008, do artigo 31.º, n.º 2, do Regulamento (UE) n.º 603/2013, do artigo 56.º, n.º 2, do Regulamento (UE) 2017/226, do artigo 67.º do Regulamento (UE) 2018/1240, do artigo 29.º, n.º 2, do Regulamento (UE) 2019/816 e do artigo 52.º dos Regulamentos (UE) 2019/817 e (UE) 2019/818, e assegura que seja dado o adequado seguimento a essas auditorias;»;

d) A alínea m-m) passa a ter a seguinte redação:

«m-m) Assegura a publicação anual da lista das autoridades competentes autorizadas a consultar diretamente os dados no SIS, nos termos do artigo 41.º, n.º 8, do Regulamento (UE) 2018/1861 e do artigo 56.º, n.º 7, do Regulamento (UE) 2018/1862, juntamente com a lista dos gabinetes dos sistemas nacionais do SIS (N. SIS) e dos gabinetes SIRENE, em conformidade com o artigo 7.º, n.º 3, do Regulamento (UE) 2018/1861 e o artigo 7.º, n.º 3, do Regulamento (UE) 2018/1862, respetivamente, bem como a lista de autoridades competentes, nos termos do artigo 65.º, n.º 2, do Regulamento (UE) 2017/2226, a lista de autoridades competentes nos termos do artigo 87.º, n.º 2, do Regulamento (UE) 2018/1240, a lista de autoridades centrais nos termos do artigo 34.º, n.º 2, do Regulamento (UE) 2019/816 e a lista de autoridades nos termos do artigo 71.º, n.º 1, do Regulamento (UE) 2019/817 e do artigo 67.º, n.º 1 do Regulamento (UE) 2019/818.».

3) No artigo 22.º, o n.º 4 passa a ter a seguinte redação:

«4. A Europol e a Eurojust podem participar nas reuniões do Conselho de Administração com o estatuto de observador, quando da ordem de trabalhos conste qualquer questão relativa ao SIS II relacionada com a aplicação da Decisão 2007/533/JAI.

A Agência Europeia da Guarda de Fronteiras e Costeira pode participar nas reuniões do Conselho de Administração com o estatuto de observador, quando da ordem de trabalhos conste qualquer questão relativa ao SIS relacionada com a aplicação do Regulamento (UE) 2016/1624.

A Europol pode participar nas reuniões do Conselho de Administração com o estatuto de observador, quando da ordem de trabalhos conste qualquer questão relativa ao VIS relacionada com a aplicação da Decisão 2008/633/JAI, ou qualquer questão relativa ao Eurodac relacionada com a aplicação do Regulamento (UE) n.º 603/2013.

A Europol pode participar nas reuniões do Conselho de Administração com o estatuto de observador, quando da ordem de trabalhos conste qualquer questão relativa ao SES relacionada com a aplicação do Regulamento (UE) 2017/2226 ou uma questão relativa ao ETIAS relacionada com o Regulamento (UE) 2018/1240.

A Agência Europeia da Guarda de Fronteiras e Costeira pode participar nas reuniões do Conselho de Administração com o estatuto de observador, quando da ordem de trabalhos conste qualquer questão relativa ao ETIAS relacionada com aplicação do Regulamento (UE) 2018/1240.

A Eurojust, a Europol e a Procuradoria Europeia podem participar nas reuniões do Conselho de Administração com o estatuto de observador, quando da ordem de trabalhos conste qualquer questão relativa ao Regulamento (UE) 2019/816.

A Europol, a Eurojust e a Agência Europeia da Guarda de Fronteiras e Costeira podem participar nas reuniões do Conselho de Administração com o estatuto de observador, quando da ordem de trabalhos conste qualquer questão relativa aos Regulamentos (UE) 2019/817 e (UE) 2019/818.

O Conselho de Administração pode convidar qualquer outra pessoa, cuja opinião possa ser útil, a participar nas suas reuniões com o estatuto de observador.».

4) No artigo 24.º, n.º 3, a alínea p) passa a ter a seguinte redação:

«p) Sem prejuízo do disposto no artigo 17.º do Estatuto dos Funcionários, o estabelecimento das normas de confidencialidade, em cumprimento do disposto no artigo 17.º do Regulamento (CE) n.º 1987/2006, no artigo 17.º da Decisão 2007/533/JAI, no artigo 26.º, n.º 9, do Regulamento (CE) n.º 767/2008 e no artigo 4.º, n.º 4, do Regulamento (UE) n.º 603/2013; no artigo 37.º, n.º 4, do Regulamento (UE) 2017/2226, no artigo 74.º, n.º 2, do Regulamento (UE) 2018/1240, no artigo 11.º, n.º 16, do Regulamento (UE) 2019/816 e no artigo 55.º, n.º 2, dos Regulamentos (UE) 2019/817 e (UE) 2019/818;».

5) O artigo 27.º é alterado do seguinte modo:

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

«d-A) Grupo Consultivo da Interoperabilidade;»;

b) O n.º 3 passa a ter a seguinte redação:

«3. A Europol, a Eurojust e a Agência Europeia da Guarda de Fronteiras e Costeira podem, cada uma, nomear um representante para o Grupo Consultivo do SIS II.

A Europol pode nomear também um representante para os Grupos Consultivos do VIS e do Eurodac e do SES-ETIAS.

A Agência Europeia da Guarda de Fronteiras e Costeira pode nomear também um representante para o Grupo Consultivo do SES-ETIAS.

A Eurojust, a Europol e a Procuradoria Europeia podem nomear também um representante para o Grupo Consultivo do ECRIS-TCN.

A Europol, a Eurojust e a Agência Europeia da Guarda de Fronteiras e Costeira podem, cada uma, nomear um representante para o Grupo Consultivo da Interoperabilidade.».

Artigo 60.º

Alteração do Regulamento (UE) 2018/1862

O Regulamento (UE) 2018/1862 é alterado do seguinte modo:

1) Ao artigo 3.º, são aditados os seguintes pontos:

«18) "ESP", o portal europeu de pesquisa criado pelo artigo 6.º, n.º 1.º, Regulamento (UE) 2019/818 (*);

19) "serviço partilhado BMS", o serviço partilhado de correspondências biométricas criado pelo artigo 12.º, n.º 1, do Regulamento (UE) 2019/818;

20) "CIR", o repositório comum de dados de identificação criado pelo artigo 17.º, n.º 1, do Regulamento (UE) 2019/818;

21) "MID", o detetor de identidades múltiplas criado pelo artigo 25.º, n.º 1, do Regulamento (UE) 2019/818.

(*) Regulamento (UE) 2019/818 do Parlamento Europeu e do Conselho, de 20 de maio de 2019, relativo à criação de um regime de interoperabilidade entre os sistemas de informação da UE no domínio da cooperação policial e judiciária, asilo e migração, e que altera os Regulamentos (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816 (JO L 135 de 22.5.2019, p. 85).».

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

a) No n.º 1, as alíneas b) e c) passam a ter a seguinte redação:

«b) Um sistema nacional (N.SIS) em cada Estado-Membro, constituído pelos sistemas de dados nacionais que comunicam com o SIS Central, e que inclui, pelo menos, um N.SIS de salvaguarda nacional ou partilhado;

c) Uma infraestrutura de comunicação entre o CS-SIS, o CS-SIS de salvaguarda e a NI-SIS ("infraestrutura de comunicação") que proporciona uma rede virtual cifrada dedicada aos dados do SIS e ao intercâmbio de dados entre os Gabinetes SIRENE a que se refere o artigo 7.º, n.º 2; e

d) Numa infraestrutura de comunicação segura entre o CS-SIS e as infraestruturas centrais do ESP, o serviço partilhado BMS e o MID.»;

b) São aditados os seguintes números:

«8. Sem prejuízo do disposto nos n.ºs 1 a 5, os dados do SIS sobre pessoas e documentos de identidade podem também ser consultados através do ESP.

9. Sem prejuízo do disposto nos n.ºs 1 a 5, os dados do SIS sobre pessoas e documentos de identidade podem também ser transmitidos pela infraestrutura de comunicação segura referida no n.º 1, alínea d). Essas transmissões devem cingir-se aos dados necessários para os objetivos referidos no Regulamento (UE) 2019/818.».

3) No artigo 7.º, é inserido o seguinte número:

«2-A. Os gabinetes SIRENE assumem também a verificação manual das diferentes identidades, em conformidade com o artigo 29.º do Regulamento (UE) 2019/818. Na medida do necessário para executar esta tarefa, os gabinetes SIRENE devem ter acesso aos dados armazenados no CIR e no MID para os efeitos previstos nos artigos 21.º e 26.ºdo Regulamento (UE) 2019/818.».

4) Ao artigo 12.º, n.º 1, é aditado o seguinte parágrafo:

«Os Estados-Membros devem garantir que todos os acessos a dados pessoais pelo ESP fiquem também documentados, a fim de verificar a legalidade da consulta e a legalidade do tratamento de dados, proceder ao auto-controlo e assegurar a integridade e a segurança dos dados.».

5) Ao artigo 44.º, n.º 1, é aditada a seguinte alínea:

«f) Verificação das diferentes identidades e luta contra a fraude de identidade, em conformidade com o capítulo V do Regulamento (UE) 2019/818.».

6) No artigo 74.º, o n.º 7 passa a ter a seguinte redação:

«7. Para os efeitos do artigo 15.º, n.º 4, e dos n.ºs 3, 4 e 6 do presente artigo, a eu-LISA deve armazenar os dados a que se refere o artigo 15.º, n.º 4 e o n.º 3 do presente artigo que não permitam a identificação de pessoas no repositório central para a elaboração de relatórios e estatísticas referido no artigo 39.º do Regulamento (UE) 2019/818.

A eu-LISA permite que a Comissão e os organismos referidos no n.º 6 do presente artigo obtenham relatórios e estatísticas específicas. Mediante pedido, a eu-LISA confere aos Estados-Membros, à Comissão, à Europol e à Agência Europeia da Guarda de Fronteiras e Costeira acesso ao repositório central para a elaboração de relatórios e estatísticas em conformidade com o artigo 39.º do Regulamento (UE) 2019/818.».

Artigo 61.º

Alteração do Regulamento (UE) 2019/816

O Regulamento (UE) 2019/816 é alterado do seguinte modo:

1) No artigo 1.º é inserida a seguinte alínea:

«c) As condições em que o ECRIS-TCN contribui para facilitar e apoiar a identificação correta das pessoas registadas no ECRIS-TCN nas condições e para efeitos do artigo 20.º do Regulamento (UE) 2019/818 do Parlamento Europeu e do Conselho (*), através do armazenamento dados de identificação, documentos de viagem e dados biométricos no CIR.

(*) Regulamento (UE) 2019/818 do Parlamento Europeu e do Conselho, de 20 de maio de 2019, relativo à criação de um regime de interoperabilidade entre os sistemas de informação da UE no domínio da cooperação policial e judiciária, asilo e migração, e que altera os Regulamentos (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816 (JO L 135 de 22.5.2019, p. 85).».

2) O artigo 2.º passa a ter a seguinte redação:

«*Artigo 2.º*

Âmbito de aplicação

O presente regulamento aplica-se ao tratamento dos dados de identificação de nacionais de países terceiros que tenham sido objeto de condenações nos Estados-Membros, a fim de determinar os Estados-Membros onde essas condenações foram proferidas. Com exceção do artigo 5.º, n.º 1, alínea b), subalínea ii), as disposições do presente regulamento aplicáveis aos nacionais de países terceiros aplicam-se igualmente aos cidadãos da União que também tenham a nacionalidade de um país terceiro e que tenham sido objeto de condenações nos Estados-Membros. O presente regulamento facilita e apoia a identificação correta das pessoas, nos termos do presente regulamento e do Regulamento (UE) 2019/818».

3) O artigo 3.º é alterado do seguinte modo:

a) O ponto 8 é suprimido;

b) São aditados os seguintes pontos:

«19) "CIR", o repositório comum de dados de identificação criado pelo artigo 17.º, n.º 1, do Regulamento (UE) 2019/818;

20) "Dados ECRIS-TCN", todos os dados armazenados no Sistema Central e no CIR em conformidade com o artigo 5.º;

21) "ESP", o portal europeu de pesquisa criado pelo artigo 6.º, n.º 1.º, Regulamento (UE) 2019/818».

4) O artigo 4.º, n.º 1, é alterado do seguinte modo:

a) A alínea a) passa a ter a seguinte redação:

«a) Um Sistema Central;»;

b) É inserida a seguinte alínea:

«a-a) O CIR;»;

c) É aditada a seguinte alínea:

«e) Uma infraestrutura de comunicação entre o sistema central e as infraestruturas centrais do ESP.».

5) O artigo 5.º, passa a ter a seguinte redação:

a) No n.º 1, o prémio passa a ter a seguinte redação:

«1. A autoridade central do Estado-Membro de condenação deve criar um registo de dados no ECRIS-TCN, para cada nacional de um país terceiro condenado. O registo de dados deve incluir:»;

b) É inserido o seguinte número:

«1-A. O CIR deve conter os dados referidos no n.º 1, alínea b), e os seguintes dados do n.º 1, alínea a): apelidos, nomes próprios, data de nascimento, local de nascimento (localidade e país), nacionalidade ou nacionalidades, sexo, nomes anteriores e, se aplicável, pseudónimos ou outros nomes, se disponível, o tipo e número dos documentos de viagem da pessoa em causa, bem como o nome da autoridade emissora. O CIR pode conter os dados referidos n.º 3. Os restantes dados do ECRIS-TCN devem ser conservados no Sistema Central.».

6) O artigo 8.º, é alterado do seguinte modo:

a) O n.º 1 passa a ter a seguinte redação:

«1. Cada ficheiro é armazenado no Sistema Central e no CIR enquanto os dados relativos à ou às condenações da pessoa em causa constarem do registo criminal.»;

b) O n.º 2 passa a ter a seguinte redação:

«2. Após o termo do período de conservação referido no n.º 1, a autoridade central do Estado-Membro de condenação deve apagar, sem demora injustificada, o ficheiro do Sistema Central e do CIR, incluindo quaisquer dados de impressões digitais ou imagens faciais. O apagamento é feito automaticamente, quando tal for possível, e em qualquer caso, o mais tardar um mês após o fim do período de conservação.».

7) O artigo 9.º é alterado da seguinte forma:

a) No n.º 1, a expressão «ECRIS-TCN» é substituída pela expressão «sistema central e no CIR»;

b) Nos n.ºs 2, 3 e 4, a expressão «sistema central» é substituída pela expressão «sistema central e no CIR».

8) No artigo 10.º, n.º 1, é suprimida a alínea j).

9) No artigo 12.º, n.º 2, a expressão «sistema central» é substituída pela expressão «sistema central e no CIR».

10) No artigo 13.º, no n.º 2, a expressão «sistema central» é substituída pela expressão «sistema central e do CIR».

11) No artigo 23.º, n.º 2, a expressão «sistema central» é substituída pela expressão «sistema central e no CIR».

12) O artigo 24.º é alterado do seguinte modo:

a) O n.º 1 passa a ter a seguinte redação:

«1. Os dados inseridos no sistema central e no CIR só podem ser tratados para efeitos de identificação dos Estado-Membros que possuem informações sobre o registo criminal de nacionais de países terceiros. Os dados incluídos no CIR devem também ser tratados em conformidade com o Regulamento (UE) 2019/818 para facilitar e apoiar a identificação correta das pessoas inscritas no ECRIS-TCN, em conformidade com o presente regulamento.»;

b) É aditado o seguinte número:

«3. Sem prejuízo do disposto no n.º 2, o acesso para fins de consulta dos dados armazenados no CIR deve ser também reservado ao pessoal devidamente autorizado das autoridades nacionais de cada Estado-Membro e ao pessoal devidamente autorizado das agências da União que são competentes para os efeitos previstos nos artigos 20.º e 21.º do Regulamento (UE) 2019/818. Esse acesso deve ser limitado na medida do necessário à execução das suas funções, em conformidade com as finalidades e proporcionado aos objetivos pretendidos.».

13) No artigo 32.º, o n.º 2 passa a ter a seguinte redação:

«2. Para os efeitos do n.º 1 do presente artigo, a eu-LISA armazena os dados referidos nesse número no repositório central para a elaboração de relatórios e estatísticas referido no artigo 39.º do Regulamento (UE) 2019/818.»;

14) No artigo 33.º, n.º 1, a expressão «sistema central» é substituída pela expressão «sistema central e no CIR».

15) N artigo 41.º, o n.º 2 passa a ter a seguinte redação:

«2. No respeitante às condenações proferidas antes da data de início da introdução dos dados nos termos do artigo 35.º, n.º 1, as autoridades centrais criam os ficheiros individuais no sistema central e no CIR do seguinte modo:

a) Os dados alfanuméricos devem ser introduzidos no sistema central e no CIR até ao final do período referido no artigo 35.º, n.º 2;

b) Os dados dactiloscópicos devem ser introduzidos no sistema central e no CIR o mais tardar dois anos após a entrada em funcionamento, nos termos do artigo 35.º, n.º 4.».

CAPÍTULO X

Disposições finais

Artigo 62.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, unicamente para efeitos da elaboração de relatórios e estatísticas, o número de consultas por utilizador do perfil ESP.

Os dados não podem permitir a identificação de pessoas.

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 CIR, unicamente para efeitos da elaboração de relatórios e estatísticas:

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

b) Nacionalidade, género 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.

Os dados não podem permitir a identificação de pessoas.

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 MID unicamente para efeitos da elaboração de relatórios e estatísticas:

a) Número de consultas efetuadas com e sem dados biométricos;

b) Número de cada tipo de ligação e sistemas de informação da União com os dados da ligação;

c) Período de tempo durante o qual uma ligação amarela e vermelha permaneceu no sistema.

Os dados não podem permitir a identificação de pessoas.

4. O pessoal devidamente autorizado da Agência Europeia da Guarda de Fronteiras e Costeira, deve ter acesso ao sistema para consultar os dados referidos nos n.ºs 1, 2 e 3, do presente artigo, para efeitos de realização de análises de risco e avaliações da vulnerabilidade, tal como referido nos artigos 11.º e 13.º do Regulamento (UE) 2016/1624 do Parlamento Europeu e do Conselho ([38]).

5. O pessoal devidamente autorizado da Europol tem acesso ao sistema para consultar os dados a que se referem os n.ºs 2 e 3, do presente artigo, para efeitos de realização de análises estratégicas, temáticas e operacionais referidas no artigo 18.º, n.º 2, alíneas b) e c), do Regulamento (UE) 2016/794.

6. Para efeitos dos n.ºs 1, 2 e 3, a eu-LISA deve conservar os dados referidos nesses números no CRRS. Os dados incluídos no CRRS não podem permitir a identificação de pessoas, mas devem permitir às autoridades enumeradas nos n.ºs 1, 2 e 3 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.

7. A pedido, a Comissão disponibiliza informações relevantes à Agência da União Europeia dos Direitos Fundamentais, a fim de avaliar o impacto do presente regulamento nos direitos fundamentais.

([38]) 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).

Artigo 63.º

Período transitório aplicável à utilização do portal europeu de pesquisa

1. Durante um prazo 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.

2. Se uma avaliação da aplicação do ESP mostrar que é necessário prorrogar o prazo a que se refere o n.º 1 do presente artigo, em especial devido ao impacto da introdução do ESP na organização e na duração dos controlos de fronteira, a Comissão fica habilitada a adotar um ato delegado, nos termos do artigo 69.º, a fim de alterar o presente regulamento, prorrogando esse prazo uma única vez, por um período não superior a um ano.

Artigo 64.º

Período transitório aplicável às disposições relativas ao acesso ao repositório comum de dados de identificação para efeitos de prevenção, deteção ou investigação de infrações terroristas ou outras infrações penais graves

O artigo 22.º aplica-se a partir da data de início das operações do CIR a que se refere o artigo 68.º, n.º 3.

Artigo 65.º

Período transitório aplicável à deteção de identidades múltiplas

1. Por um período de um ano a contar da notificação pela eu-LISA da conclusão do teste do MID referido no artigo 68.º, n.º 4, alínea b) e antes do início do funcionamento do MID, a unidade central do ETIAS é responsável por efetuar uma deteção de identidades múltiplas entre os dados armazenados no SES, no VIS, no Eurodac e no SIS. As deteções de identidades múltiplas devem ser efetuadas utilizando apenas os dados biométricos.

2. Se a consulta detetar uma ou várias correspondências s 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 correspondências 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 correspondências s, deve ser criada uma ligação para cada elemento de dados que desencadeou a correspondência.

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

4. Quando for criada uma ligação a uma indicação no SIS, que não seja um alerta nos termos do artigo 3.º do Regulamento (UE) 2018/1860, dos artigos 24.º e 25.º do Regulamento (UE) 2018/1861 ou do artigo 38.º do Regulamento (UE) 2018/1862, o MID deve facultar ao gabinete SIRENE do Estado-Membro que criou a indicação acesso aos dados de identificação presentes nos diferentes sistemas de informação.

5. A unidade central ETIAS ou, nos casos previstos no n.º 4 do presente artigo, 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 unidade central do ETIAS notifica apenas a Comissão, em conformidade com o artigo 67.º, n.º 3, logo que todas as ligações amarelas tenham sido verificadas manualmente e o seu estado tenha sido atualizado em ligações verdes, brancas ou vermelhas.

7. Os Estados-Membros devem apoiar a unidade central do ETIAS, se for caso disso, na realização da deteção de identidades múltiplas referida no presente artigo.

8. A Comissão fica habilitada a adotar um ato delegado, nos termos do artigo 69.º, a fim de alterar o presente regulamento e prorrogar o prazo referido no n.º 1 do presente artigo por um período de seis meses, renovável duas vezes por seis meses de cada vez. Essa prorrogação só é concedida se uma avaliação do prazo previsto para a conclusão da deteção de identidades múltiplas a que se refere o presente artigo evidenciar que a deteção de identidades múltiplas não pode ser concluída antes do termo do período previsto no n.º 1 do presente artigo ou da eventual prorrogação por razões alheias à vontade da unidade central do ETIAS e que não podem ser aplicadas quaisquer medidas corretivas. Essa avaliação é realizada o mais tardar três meses antes do termo desse prazo ou da prorrogação em curso.

Artigo 66.º

Custos

1. Os custos decorrentes da criação e funcionamento do ESP, do serviço partilhado BMS, do CIR e do MID ficam a cargo do 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. Sem prejuízo de outros financiamento para este efeito a partir de outras fontes do orçamento geral da União Europeia, será mobilizado um montante de 32 077 000 EUR a partir da dotação de 791 000 000 EUR prevista no artigo 5.º, n.º 5, alínea b), do Regulamento (UE) n.º 515/2014, para cobrir os custos de aplicação do presente regulamento, tal como previsto nos n.ºs 1 e 2 do presente artigo.

4. A partir do montante referido no n.º 3, 22 861 000 EUR são atribuídos à eu-LISA, 9 072 000 EUR são atribuídos à Europol e 144 000 EUR à Agência da União Europeia para a Formação Policial (CEPOL), para apoiar estas agências no desempenho das respetivas funções, em conformidade com os requisitos do presente regulamento. Esse financiamento é executado em regime de gestão indireta.

5. Os custos incorridos pelas autoridades designadas 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.

As despesas incorridas pela Europol, incluindo as relacionadas com o CIR, são suportadas pela Europol.

Artigo 67.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 68.º. Em caso de alterações da 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 68.º, n.º 1, alínea b), n.º 2, alínea b), n.º 3, alínea b), n.º 4, alínea b), n.º 5, alínea b) e n.º 6, alínea b).

3. A unidade central ETIAS deve notificar à Comissão a conclusão com êxito do período transitório estabelecido no artigo 65.º.

4. A Comissão deve disponibilizar as informações comunicadas nos termos do n.º 1 aos Estados-Membros e ao público, através de um sítio público constantemente atualizado.

Artigo 68.º

Início das operações

1. A Comissão deve fixar a data a partir da qual o ESP entra em funcionamento por meio de um ato de execução, logo que estejam preenchidas 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, e artigo 43.º, n.º 5;

b) A eu-LISA tiver declarado a conclusão com êxito de um teste global do ESP, que deve ser efetuado pela eu-LISA em cooperação com as autoridades dos Estados-Membros e as agências da União suscetíveis de utilizar o ESP;

c) A eu-LISA tiver validado as disposições técnicas e jurídicas para a recolha e transmissão dos dados a que se referem o artigo 8.º, n.º 1, e procedido à notificação da Comissão;

O ESP só pode consultar as bases de dados da Interpol se as disposições técnicas permitirem o cumprimento do artigo 9.º, n.º 5. A impossibilidade de cumprimento desse artigo implica que a ESP não pode consultar as bases de dados da Interpol, mas não deve atrasar o início das operações do ESP.

A Comissão fixa a data a que se refere o primeiro parágrafo, que não pode ser posterior a 30 dias após da data de adoção do ato de execução.

2. A Comissão deve determinar a data a partir da qual o serviço partilhado BMS entra em funcionamento, por meio de um ato de execução, logo que estejam preenchidas as seguintes condições:

a) Tiverem sido adotadas as medidas a que se referem o artigo 13.º, n.º 5, e o artigo 43.º, n.º 5;

b) A eu-LISA tiver declarado a conclusão com êxito de um teste global do BMS, a realizar pela eu-LISA em cooperação com as autoridades dos Estados-Membros;

c) A eu-LISA tiver validado as disposições técnicas e jurídicas para a recolha e transmissão dos dados nos termos do artigo 13.º e procedido à notificação da Comissão;

d) A eu-LISA tiver notificado a conclusão com êxito do teste referido no n.º 5, alínea b).

A Comissão fixa a data a que se refere o primeiro parágrafo, que não pode ser posterior a 30 dias após a data de adoção do ato de execução.

3. A Comissão deve fixar a data a partir da qual o CIR entra em funcionamento, por meio de um ato de execução, logo que estejam preenchidas as seguintes condições:

a) Tiverem sido adotadas as medidas a que se referem o artigo 43, n.º 5, e o artigo 74.º, n.º 10;

b) A eu-LISA tiver declarado a conclusão com êxito de um teste global do CIR, a realizar em cooperação com as autoridades dos Estados-Membros;

c) A eu-LISA tiver validado as disposições técnicas e jurídicas para a recolha e transmissão dos dados a que se refere o artigo 18.º e procedido à notificação da Comissão;

d) A eu-LISA tiver notificado a conclusão com êxito do teste referido no n.º 5, alínea b).

A Comissão fixa a data a que se refere o primeiro parágrafo, que não pode ser posterior a 30 dias após a data de adoção do ato de execução.

4. A Comissão deve fixar a data a partir da qual o MID entra em funcionamento, por meio de um ato de execução, logo que estejam preenchidas as seguintes condições:

a) Tiverem sido adotadas as medidas a que se referem o artigo 28.º, n.ºs 5 e 7, o artigo 32.º, n.º 5, o artigo 33.º, n.º 6, o artigo 43.º, n.º 5, e o artigo 49.º, n.º 6;

b) A eu-LISA tiver declarado a conclusão com êxito de um teste global do MID, que deve ser efetuado pela eu-LISA em cooperação com as autoridades dos Estados-Membros e a unidade central do ETIAS;

c) A eu-LISA tiver validado as disposições técnicas e jurídicas para a recolha e transmissão dos dados previstos no artigo 34.º e procedido à notificação da Comissão;

d) A unidade central ETIAS tiver notificado a Comissão, conforme referido no artigo 67.º, n.º 3;

e) A eu-LISA tiver declarado a conclusão com êxito dos testes referidos no n.º 1, alínea b), no n.º 2, alínea b), no n.º 3, alínea b) e no n.º 5, alínea b).

A Comissão fixa a data a que se refere o primeiro parágrafo, que não pode ser posterior a 30 dias após a data de adoção do ato de execução.

5. A Comissão deve fixar por meio de atos de execução a data a partir da qual os mecanismos e procedimentos automatizados de controlo da qualidade, os indicadores comuns de qualidade dos dados e as normas mínimas de qualidade devem ser utilizados, logo que estejam reunidas as seguintes condições:

a) Tiverem sido adotadas as medidas previstas no artigo 37.º, n.º 4;

b) A eu-LISA tiver declarado a conclusão com êxito de um teste global dos mecanismos e procedimentos automatizados de controlo da qualidade, dos indicadores comuns de qualidade dos dados e das normas mínimas de qualidade dos dados, que deve ser efetuado em cooperação com as autoridades dos Estados-Membros.

A Comissão fixa a data a que se refere o primeiro parágrafo, que não pode ser posterior a 30 dias após a data de adoção do ato de execução.

6. A Comissão deve fixa a data a partir da qual o CRRS entra em funcionamento, por meio de um ato de execução, logo que reunidas as seguintes condições:

a) Tiverem sido adotadas as medidas previstas no artigo 39.º, n.º 5, e no artigo 43.º, n.º 5;

b) A eu-LISA tiver declarado a conclusão com êxito de um teste global do CRRS, a realizar em cooperação com as autoridades dos Estados-Membros;

c) A eu-LISA tiver validado as disposições técnicas e jurídicas para a recolha e transmissão dos dados a que se refere o artigo 39.º e procedido à notificação da Comissão.

A Comissão fixa a data a que se refere o primeiro parágrafo, que não pode ser posterior a 30 dias após a data de adoção do ato de execução.

7. A Comissão deve informar o Parlamento Europeu e o Conselho dos resultados do teste efetuado em conformidade com o n.º 1, alínea b), o n.º 2, alínea b), o n.º 3, alínea b), o n.º 4, alínea b), o n.º 5, alínea b) e o n.º 6, alínea b).

8. Os Estados-Membros, a unidade central ETIAS e a Europol devem começar a utilizar os componentes de interoperabilidade a partir da data determinada pela Comissão em conformidade com os n.ºs 1, 2, 3 e 4, respetivamente.

Artigo 69.º

Exercício da delegação

1. O poder de adotar atos delegados é conferido à Comissão nas condições estabelecidas no presente artigo.

2. O poder de adotar atos delegados referido no artigo 28.º, n.º 5, no artigo 39.º, n.º 5, no artigo 49.º, n.º 6, no artigo 63.º, n.º 2, e no artigo 65.º, n.º 8, é conferido à Comissão por um período de cinco anos a contar de 11 de junho de 2019. A Comissão elabora um relatório relativo à delegação de poderes pelo menos nove meses antes do final do prazo de cinco anos. A delegação de poderes é tacitamente prorrogada por períodos de igual duração, salvo se o Parlamento Europeu ou o Conselho a tal se opuserem o mais tardar três meses antes do final de cada período.

3. A delegação de poderes referida no artigo 28.º, n.º 5, no artigo 39.º, n.º 5, no artigo 49.º, n.º 6, no artigo 63.º, n.º 2, e no artigo 65.º, n.º 8 pode ser revogada em qualquer momento pelo Parlamento Europeu ou pelo Conselho. A decisão de revogação põe termo à delegação dos poderes nela especificados. A decisão de revogação produz efeitos a partir do dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia* ou de uma data posterior nela especificada. A decisão de revogação não afeta os atos delegados já em vigor.

4. Antes de adotar um ato delegado, a Comissão consulta os peritos designados por cada Estado-Membro, em conformidade com os princípios estabelecidos no Acordo Interinstitucional, 13 de abril de 2016, sobre legislar melhor.

5. Assim que adotar um ato delegado, a Comissão notifica-o simultaneamente ao Parlamento Europeu e ao Conselho.

6. Os atos delegados adotados em aplicação do disposto no artigo s termos do artigo 28.º, n.º 5, no artigo 39.º, n.º 5, no artigo 49.º, n.º 6, no artigo 63.º, n.º 2, e no artigo 65.º, n.º 8 só entram em vigor se nem o Parlamento Europeu nem o Conselho formularem objeções no prazo de quatro meses a contar da notificação do ato a estas duas instituições ou se, antes do termo desse prazo, o Parlamento Europeu e o Conselho informarem a Comissão de que não formularão objeções. O referido prazo pode ser prorrogado por dois meses por iniciativa do Parlamento Europeu ou do Conselho.

Artigo 70.º

Procedimento de comité

1. A Comissão é assistida por um comité. O referido comité é um comité na aceção do Regulamento (UE) n.º 182/2011.

2. Sempre que se remeta para o presente número, aplica-se o artigo 5.º do Regulamento (UE) n.º 182/2011.

Na falta de parecer do comité, a Comissão não adota o projeto de ato de execução, aplicando-se o artigo 5.º, n.º 4, terceiro parágrafo, do Regulamento (UE) n.º 182/2011.

Artigo 71.º

Grupo consultivo

A eu-LISA deve criar um grupo consultivo de interoperabilidade. Durante a fase de conceção e desenvolvimento dos componentes de interoperabilidade, deve aplicar-se o artigo 54.º, n.º 4, n.º 5 e n.º 6.

Artigo 72.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) 2018/1726.

As autoridades dos Estados-Membros e as agências da União devem ministrar ao seu pessoal autorizado a tratar dados dos componentes de interoperabilidade um programa de formação adequado sobre a segurança dos dados, a qualidade dos dados, as regras em matéria de proteção de dados, os procedimentos relativos ao tratamento dos dados e as obrigações de informação nos termos dos artigos 32.º, n.º 4, 33.º, n.º 4 e 47.º.

Se for caso disso, devem ser organizados, a nível da União, cursos de formação comuns sobre estes temas para reforçar a cooperação e o intercâmbio de boas práticas entre o pessoal das autoridades dos Estados-Membros e as agências da União que estão autorizadas a tratar dados dos componentes de interoperabilidade. Deve ser dada especial atenção ao processo de deteção de identidades múltiplas, incluindo a verificação manual das diferentes identidades e a necessidade concomitante de garantir as salvaguardas em relação aos direitos fundamentais.

Artigo 73.º

Manual prático

A Comissão, em estreita cooperação com os Estados-Membros, com a eu-LISA e com outros organismos da União competentes, 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 74.º

Acompanhamento e avaliação

1. A eu-LISA deve assegurar que são criados procedimentos para acompanhar o desenvolvimento de componentes de interoperabilidade e a ligação à interface uniforme nacional 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 12 de dezembro de 2019 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 e da sua ligação à interface uniforme nacional. Quando a fase de desenvolvimento estiver concluída, 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. Quatro anos após o início do funcionamento de cada componente de interoperabilidade nos termos do artigo 68.º 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.

4. Além disso, um ano após cada relatório da eu-LISA, a Comissão deve apresentar uma avaliação global dos componentes da interoperabilidade, incluindo uma:

a) Avaliação da aplicação do presente regulamento;

b) Uma análise dos resultados obtidos comparativamente aos objetivos fixados pelo presente regulamento e ao impacto nos direitos fundamentais, incluindo, em particular, uma avaliação do impacto dos componentes de interoperabilidade no direito à não discriminação;

c) Avaliação do funcionamento do portal Web, incluindo os dados relativos à utilização do portal Web e ao número de pedidos que foram resolvidos;

d) Avaliação da continuidade da validade dos princípios subjacentes aos componentes de interoperabilidade;

e) Avaliação da segurança dos componentes de interoperabilidade;

f) Avaliação da utilização do CIR para fins de identificação;

g) Avaliação da utilização do CIR para efeitos de prevenção, deteção ou investigação de infrações terroristas ou outras infrações penais graves;

h) 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 geral da União;

i) Avaliação da consulta das bases de dados da Interpol através do ESP, incluindo informações sobre o número de correspondências s a consultas das bases de dados da Interpol e sobre quaisquer problemas encontrados.

A avaliação global a que se refere o primeiro parágrafo do presente número deve incluir quaisquer recomendações necessárias. A Comissão deve transmitir a avaliação ao Parlamento Europeu, ao Conselho, à Autoridade Europeia para a Proteção de Dados e à Agência dos Direitos Fundamentais da União Europeia.

5. Até 12 de junho de 2020 e todos os anos após essa data até à adoção dos atos de execução da Comissão a que se refere o artigo 68.º, a Comissão apresenta ao Parlamento Europeu e ao Conselho um relatório sobre o ponto da situação dos preparativos para a plena execução do presente regulamento. Esse relatório deve também conter informações pormenorizadas sobre os custos incorridos e informações sobre quaisquer riscos que possam ter um impacto sobre os custos globais.

6. Dois anos após o início do funcionamento do MID nos termos do artigo 68.º, n.º 4, a Comissão deve proceder a uma análise do impacto do MID no direito à não discriminação. Na sequência desse primeiro relatório, a análise do impacto do MID no direito à não discriminação deve fazer parte do exame referido no n.º 4, alínea b), do presente artigo.

7. Os Estados-Membros e a Europol devem fornecer à eu-LISA e à Comissão as informações necessárias para a elaboração dos relatórios referidos nos n.ºs 3 a 6. 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.

8. A eu-LISA deve comunicar à Comissão as informações necessárias à elaboração das avaliações referidas no n.º 4.

9. Respeitando as disposições de direito nacional sobre a publicação de informações sensíveis, e sem prejuízo das limitações necessárias para proteger a segurança e a ordem pública, prevenir a criminalidade e garantir que qualquer investigação nacional não seja posta em causa, cada Estado-Membro e a Europol devem elaborar relatórios anuais sobre a eficácia do acesso aos dados armazenados no CIR para efeitos de prevenção, deteção ou investigação de infrações terroristas ou outros crimes graves, contendo informações e estatísticas sobre:

a) A finalidade exata da consulta, incluindo o tipo de infração terrorista ou crime grave;

b) Motivos razoáveis de suspeita fundamentada de que o suspeito, autor ou vítima está abrangido pelo Regulamento (UE) n.º 603/2013;

c) O número de pedidos de acesso ao CIR para efeitos de prevenção, deteção ou investigação de infrações terroristas ou outros crimes graves;

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 posterior realizada pelo ponto central de acesso.

Os relatórios anuais elaborados pelos Estados-Membros e pela Europol devem ser transmitidos à Comissão até 30 de junho do ano seguinte.

10. É disponibilizada aos Estados-Membros uma solução técnica para gerir os pedidos de acesso dos utilizadores referidos no artigo 22.º e facilitar a recolha dos dados enumerados nos n.ºs 7 e 9, do presente artigo, para efeitos de produção de relatórios e das estatísticas referidas nesses números. A Comissão adota atos de execução relativos às especificações da solução técnica. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 70.º, n.º 2.

Artigo 75.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*.

As disposições do presente regulamento relacionadas com o ESP, são aplicáveis a partir da data fixada pela Comissão nos termos do artigo 68.º, n.º 1.

As disposições do presente regulamento relacionadas com o serviço partilhado BMS, são aplicáveis a partir da data fixada pela Comissão nos termos do artigo 68.º, n.º 2.

As disposições do presente regulamento relacionadas com o CIR, são aplicáveis a partir da data fixada pela Comissão nos termos do artigo 68.º, n.º 3.

As disposições do presente regulamento relacionadas com o MID, são aplicáveis a partir da data fixada pela Comissão nos termos do artigo 68.º, n.º 4.

As disposições do presente regulamento relacionadas com os mecanismos e procedimentos automatizados de controlo da qualidade dos dados, os indicadores comuns de qualidade dos dados e as normas mínimas de qualidade dos dados, são aplicáveis a partir da data fixada pela Comissão nos termos do artigo 68.º, n.º 5.

As disposições do presente regulamento relacionadas com o CRRS são aplicáveis a partir da data fixada pela Comissão, nos termos do artigo 68.º, n.º 6.

Os artigos 6.º, 12.º, 17.º, 25.º, 38.º, 42.º, 54.º, 56.º, 58.º, 66.º, 67.º, 69.º, 70.º, 71.º, 73.º e 74.º, n.º 1, são aplicáveis a partir de 11 de junho de 2019.

O presente regulamento é aplicável ao Eurodac a partir da data em que a reformulação do Regulamento (UE) n.º 603/2013 se tornar aplicável.

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável nos Estados-Membros em conformidade com os Tratados.

Feito em Bruxelas, em 20 de maio de 2019.

Pelo Parlamento Europeu	*Pelo Conselho*
O Presidente	*O Presidente*
A. TAJANI	G. CIAMBA

ISSN 1977-0774 (edição eletrónica)
ISSN 1725-2601 (edição em papel)

Serviço das Publicações da União Europeia
2985 Luxemburgo
LUXEMBURGO

PT