



Bruxelas, 21.12.2016  
COM(2016) 883 final

2016/0409 (COD)

Proposta de

**REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO**

**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 o Regulamento (UE) n.º 515/2014 e revoga o Regulamento (CE) n.º 1986/2006, a Decisão 2007/533/JAI do Conselho e a Decisão 2010/261/UE da Comissão**

## EXPOSIÇÃO DE MOTIVOS

### 1. CONTEXTO DA PROPOSTA

#### • **Justificação e objetivos da proposta**

Ao longo dos últimos dois anos, a União Europeia tem vindo a trabalhar simultaneamente para enfrentar os desafios da gestão da migração, a gestão integrada das fronteiras externas da União Europeia e a luta contra o terrorismo e a criminalidade transnacional. Um intercâmbio eficaz de informações entre os Estados-Membros, e entre estes e as agências competentes da UE, é essencial para responder com firmeza aos desafios referidos e realizar uma União da Segurança genuína e eficaz.

O Sistema de Informação de Schengen (SIS) é o instrumento que melhores resultados apresenta na cooperação eficaz entre as autoridades de imigração, policiais, aduaneiras e judiciárias na UE e nos países associados de Schengen. É necessário que as autoridades competentes nos Estados-Membros, nomeadamente os serviços de polícia, guardas de fronteira e agentes aduaneiros, tenham acesso a informações de elevada qualidade sobre as pessoas ou os objetos que controlam, com instruções claras quanto aos procedimentos a efetuar em cada caso. Este sistema de informação de larga escala está no cerne da cooperação Schengen, desempenhando um papel crucial na viabilização da livre circulação de pessoas no espaço Schengen. Permite que as autoridades competentes insiram e consultem dados relativos a pessoas procuradas, pessoas que possam não ter o direito de entrar ou permanecer na UE, pessoas desaparecidas, especialmente crianças, e objetos que possam ter sido roubados, desviados ou perdidos. O SIS contém não só informações acerca de determinada pessoa ou objeto, mas também instruções claras, destinadas às autoridades competentes, quanto aos procedimentos a efetuar uma vez encontrada essa pessoa ou objeto.

Em 2016, a Comissão realizou uma avaliação exaustiva<sup>1</sup> do SIS, três anos após a entrada em funcionamento da sua segunda geração. A avaliação demonstrou que o SIS tem sido um verdadeiro êxito no plano operacional. Em 2015, as autoridades nacionais competentes efetuaram verificações respeitantes a pessoas e objetos a partir de dados que figuravam no SIS em quase 2,9 mil milhões de ocasiões e trocaram mais de 1,8 milhões de elementos de informação suplementares. Todavia, conforme anunciado no programa de trabalho da Comissão para 2017, partindo desta experiência positiva, importará reforçar a eficácia e eficiência do sistema. Tendo em vista este objetivo, a Comissão apresenta um primeiro conjunto de três propostas destinadas a melhorar e alargar a utilização do SIS, como consequência da avaliação, ao mesmo tempo que prossegue os seus trabalhos, a fim de aumentar a interoperabilidade dos sistemas de aplicação coerciva da lei e de gestão das fronteiras existentes e futuros, dando seguimento aos trabalhos atualmente desenvolvidos pelo Grupo de Peritos de Alto Nível em matéria de Sistemas de Informação e Interoperabilidade.

As referidas propostas abrangem a utilização do sistema relativamente: a) à gestão das fronteiras; b) à cooperação policial e à cooperação judiciária em matéria penal; e c) ao regresso dos nacionais de países terceiros em situação irregular. As duas primeiras propostas formam conjuntamente a base jurídica do estabelecimento, do funcionamento e da utilização

---

<sup>1</sup> Relatório ao Parlamento Europeu e ao Conselho sobre a avaliação do Sistema de Informação de Schengen de segunda geração (SIS II) em conformidade com o artigo 24.º, n.º 5, o artigo 43.º, n.º 5 e o artigo 50.º, n.º 5, do Regulamento (CE) n.º 1987/2006, e com o artigo 59.º, n.º 3, e o artigo 65.º, n.º 5, da Decisão 2007/533/JAI e o documento de trabalho correspondente dos serviços da Comissão (JO...).

do SIS. A proposta relativa à utilização do SIS para efeitos de regresso dos nacionais de países terceiros em situação irregular complementa a proposta relativa à gestão das fronteiras e completa as disposições desta última. Prevê uma nova categoria de indicações e contribui para a aplicação e o acompanhamento da Diretiva 2008/115/CE<sup>2</sup>.

Em virtude da geometria variável da participação dos Estados-Membros nas políticas da UE em matéria de liberdade, segurança e justiça, é necessário adotar três instrumentos jurídicos distintos que, apesar disso, sejam executados conjuntamente, de forma harmoniosa, para permitir um funcionamento e uma utilização abrangentes do sistema.

Paralelamente, com vista a reforçar e melhorar a gestão de informações ao nível da UE, em abril de 2016, a Comissão deu início a um processo de reflexão sobre «sistemas de informação mais sólidos e mais inteligentes para controlar as fronteiras e garantir a segurança»<sup>3</sup>. O principal objetivo é assegurar que as autoridades competentes disponham sistematicamente das informações necessárias a partir de diferentes sistemas de informação. No sentido de alcançar este objetivo, a Comissão tem vindo a rever a arquitetura dos sistemas de informação existentes para identificar lacunas e falhas de informação que resultam das deficiências nas funcionalidades dos sistemas existentes, bem como da fragmentação na arquitetura global de gestão de dados da UE. No intuito de apoiar este trabalho, a Comissão instituiu um Grupo de Peritos de Alto Nível em matéria de Sistemas de Informação e Interoperabilidade, cujas conclusões preliminares serviram igualmente de base a este primeiro conjunto de propostas no que respeita às questões de qualidade dos dados<sup>4</sup>. O discurso do Presidente Jean-Claude Juncker sobre o estado da União, de setembro de 2016, fez igualmente referência à importância de corrigir as atuais deficiências na gestão das informações e de melhorar a interoperabilidade e a interconexão dos sistemas de informação existentes.

No seguimento das conclusões do referido grupo, as quais serão apresentadas na primeira metade de 2017, a Comissão irá examinar, em meados de 2017, um segundo conjunto de propostas que procurarão aperfeiçoar a interoperabilidade do SIS com outros sistemas de informação. A revisão do Regulamento (UE) n.º 1077/2011<sup>5</sup>, que cria uma Agência europeia para a gestão operacional de sistemas informáticos de grande escala no espaço de liberdade, segurança e justiça (eu-LISA), é um elemento igualmente importante deste trabalho, sendo provável que venha a ser objeto de propostas distintas da Comissão, também em 2017. Investir na rapidez, eficácia e qualidade do intercâmbio e da gestão de informações e assegurar a interoperabilidade das bases de dados e dos sistemas de informação da UE são aspetos importantes da resposta aos desafios de segurança atuais.

A presente proposta integra um primeiro conjunto de propostas<sup>6</sup> destinadas a melhorar o funcionamento do SIS, bem como a sua exploração e utilização nos domínios da cooperação policial e da cooperação judiciária em matéria penal. O regulamento proposto dá execução:

---

<sup>2</sup> Diretiva 2008/115/CE do Parlamento Europeu e do Conselho, de 16 de dezembro de 2008, relativa a normas e procedimentos comuns nos Estados-Membros para o regresso de nacionais de países terceiros em situação irregular (JO L 348 de 24.12.2008, p. 98).

<sup>3</sup> COM(2016) 205 final de 6.4.2016.

<sup>4</sup> Decisão 2016/C 257/03 da Comissão de 17.6.2016.

<sup>5</sup> Regulamento (UE) n.º 1077/2011 do Parlamento Europeu e do Conselho, de 25 de outubro de 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 286 de 1.11.2011, p. 1).

<sup>6</sup> Regulamento (UE) 2018/xxx [controles das fronteiras] e Regulamento (UE) 2018/xxx [regresso dos nacionais de países terceiros em situação irregular].

- (1) ao anúncio, feito pela Comissão, da sua intenção de aumentar o valor acrescentado do SIS para efeitos de aplicação coerciva da lei<sup>7</sup>, em resposta às novas ameaças;
- (2) à consolidação dos resultados dos trabalhos relativos à execução do SIS, realizados nos últimos três anos, que englobam modificações técnicas do SIS Central destinadas a alargar algumas das categorias de indicações existentes e a acrescentar novas funcionalidades;
- (3) a recomendações sobre modificações técnicas e processuais, decorrentes de uma avaliação exaustiva do SIS<sup>8</sup>;
- (4) aos pedidos dos utilizadores finais do SIS no sentido de introduzir aperfeiçoamentos técnicos; e
- (5) às conclusões preliminares do Grupo de Peritos de Alto Nível em matéria de Sistemas de Informação e Interoperabilidade<sup>9</sup> no que respeita à qualidade dos dados.

Atendendo ao facto de a presente proposta estar intrinsecamente ligada à proposta da Comissão de regulamento relativo ao estabelecimento, ao funcionamento e à utilização do SIS no domínio da cooperação policial e da cooperação judiciária em matéria penal, existem várias disposições comuns a ambos os textos. Estão em causa medidas que abrangem a utilização de extremo a extremo do SIS, incluindo não apenas o funcionamento dos sistemas central e nacionais, mas também as necessidades dos utilizadores finais; medidas reforçadas de continuidade das operações; medidas que visam a qualidade, a proteção e a segurança dos dados; e disposições relativas às modalidades de acompanhamento, avaliação e elaboração de relatórios. As duas propostas alargam também a utilização de informações biométricas<sup>10</sup>.

O atual quadro jurídico da segunda geração do SIS, que respeita à sua utilização para fins de cooperação policial e cooperação judiciária em matéria penal, tem por base um instrumento anteriormente inserido no terceiro pilar, a Decisão 2007/533/JAI do Conselho<sup>11</sup>, bem como um instrumento anteriormente inserido no primeiro pilar, o Regulamento (CE) n.º 1986/2006<sup>12</sup>. A presente proposta consolida o conteúdo dos instrumentos em vigor e, paralelamente, adita novas disposições, por forma a:

- harmonizar melhor os procedimentos nacionais relativos à utilização do SIS, em especial quanto aos crimes relacionados com o terrorismo e os riscos de rapto parental de crianças;

---

<sup>7</sup> Ver Comunicação intitulada «Dar cumprimento à Agenda Europeia para a Segurança para combater o terrorismo e abrir caminho à criação de uma União da Segurança genuína e eficaz», p. 4 e seguintes [COM(2016) 230 final de 20.4.2016].

<sup>8</sup> Relatório ao Parlamento Europeu e ao Conselho sobre a avaliação do Sistema de Informação de Schengen de segunda geração (SIS II) em conformidade com o artigo 24.º, n.º 5, o artigo 43.º, n.º 5 e o artigo 50.º, n.º 5, do Regulamento (CE) n.º 1987/2006, e com o artigo 59.º, n.º 3, e o artigo 65.º, n.º 5, da Decisão 2007/533/JAI e o documento de trabalho correspondente dos serviços da Comissão (JO...).

<sup>9</sup> Grupo de Peritos de Alto Nível – Relatório intercalar do Presidente de 21 de dezembro de 2016.

<sup>10</sup> Ver na secção 5 «Outros elementos» uma explicação pormenorizada das alterações incluídas na presente proposta.

<sup>11</sup> 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).

<sup>12</sup> Regulamento (CE) n.º 1986/2006 do Parlamento Europeu e do Conselho, de 20 de dezembro de 2006, relativo ao acesso ao Sistema de Informação de Schengen de segunda geração (SIS II) dos serviços dos Estados-Membros competentes para a emissão dos certificados de matrícula dos veículos (JO L 381 de 28.12.2006, p. 1).

- alargar o âmbito de aplicação do SIS mediante a introdução de novos elementos relativos a identificadores biométricos nas indicações existentes;
- introduzir alterações técnicas destinadas a melhorar a segurança e ajudar a reduzir a carga administrativa, determinando a obrigatoriedade de cópias nacionais e normas técnicas comuns de execução;
- tratar a total utilização de extremo a extremo do SIS, cobrindo não só os sistemas central e nacionais, mas também garantindo que os utilizadores finais recebem todos os dados necessários para o desempenho das suas funções e respeitam todas as normas de segurança no tratamento de dados do SIS.

• **Coerência com outras políticas da União e com os instrumentos jurídicos existentes e futuros**

A presente proposta está intimamente associada a outras políticas da União, que complementa, ou seja:

- (1) A **segurança interna**, no sentido de, tal como sublinhado na Agenda Europeia para a Segurança<sup>13</sup> e nos trabalhos da Comissão para a criação de uma União da Segurança genuína e eficaz<sup>14</sup>, prevenir, detetar, investigar e julgar crimes terroristas e outros crimes graves, dando às autoridades com funções coercivas a possibilidade de tratar dados pessoais de indivíduos suspeitos de estarem implicados em atos terroristas ou crimes graves;
- (2) A **proteção dos dados**, na medida em que a presente proposta garante a proteção dos direitos fundamentais dos indivíduos cujos dados pessoais são tratados no SIS.

A presente proposta está também intimamente ligada à legislação em vigor da União, que complementa, a saber:

- (3) A **Guarda Europeia de Fronteiras e Costeira** no que se refere ao seu acesso ao SIS para efeitos do Sistema Europeu de Informação e Autorização de Viagem (ETIAS) proposto<sup>15</sup>, bem como à disponibilização de uma interface técnica de acesso ao SIS por parte das equipas da Guarda Europeia de Fronteiras e Costeira, das equipas envolvidas em operações de regresso e dos membros da equipa de apoio à gestão da migração, para que, no âmbito dos seus mandatos, possam aceder e pesquisar dados introduzidos no SIS;
- (4) A **Europol**, na medida em que a presente proposta confere à Europol direitos adicionais de acesso e consulta, no âmbito do seu mandato, de dados que tenham sido introduzidos no SIS;
- (5) **Prüm**, na medida em que os desenvolvimentos da presente proposta com vista a permitir a identificação de pessoas com base em impressões digitais (assim como imagens faciais e perfis de ADN) complementem as disposições em vigor do Tratado de Prüm<sup>16</sup> relativamente ao acesso mútuo transfronteiras em linha a fontes nacionais

---

<sup>13</sup> COM(2015) 185 final.

<sup>14</sup> COM(2016) 230 final.

<sup>15</sup> COM(2016) 731 final.

<sup>16</sup> Decisão 2008/615/JAI do Conselho, de 23 de junho de 2008, relativa ao aprofundamento da cooperação transfronteiras, em particular no domínio da luta contra o terrorismo e a criminalidade transfronteiras (JO L 210 de 6.8.2008, p. 1); e Decisão 2008/616/JAI do Conselho, de 23 de junho de 2008, referente à execução da Decisão 2008/615/JAI, relativa ao aprofundamento da cooperação transfronteiras, em

de bases de dados designadas de perfis de ADN e aos sistemas automatizados de identificação por impressões digitais.

A presente proposta está também intimamente associada à legislação futura da União, que complementa, a saber:

- (6) A **gestão das fronteiras externas**. A proposta complementa o novo princípio que se prevê inserir no Código das Fronteiras Schengen, que consiste em controlos sistemáticos por confronto com as bases de dados pertinentes, de todos os viajantes, incluindo cidadãos da UE, à entrada e à saída do espaço Schengen, como resposta ao fenómeno dos combatentes terroristas estrangeiros;
- (7) **O Sistema de Entrada/Saída**. A proposta procura refletir a utilização sugerida de uma combinação de impressões digitais e imagens faciais enquanto identificadores biométricos para o correto funcionamento do Sistema de Entrada/Saída (EES);
- (8) **O ETIAS**. A proposta tem em conta o sistema ETIAS já proposto, que prevê uma avaliação rigorosa à luz dos riscos para a segurança, incluindo uma verificação no SIS, dos nacionais de países terceiros isentos da obrigação de visto que pretendem viajar para a UE.

## 2. BASE JURÍDICA, SUBSIDIARIEDADE E PROPORCIONALIDADE

### • Base jurídica

As disposições respeitantes à cooperação policial e à cooperação judiciária em matéria penal da presente proposta têm por base 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, alínea a), do Tratado sobre o Funcionamento da União Europeia.

### • Geometria variável

A presente proposta desenvolve as disposições do acervo de Schengen relativas à cooperação policial e à cooperação judiciária em matéria penal. Por conseguinte, devem ser tidas em conta as consequências seguidamente descritas relativamente aos vários protocolos e acordos celebrados com os países associados.

Dinamarca: nos termos do artigo 4.º do Protocolo n.º 22, relativo à posição da Dinamarca, anexo aos Tratados, a Dinamarca deve decidir, no prazo de seis meses após o Conselho ter adotado uma decisão sobre o presente regulamento, que constitui um desenvolvimento do acervo de Schengen, se procede à respetiva transposição para o seu direito interno.

Reino Unido: nos termos do artigo 5.º do Protocolo que integra o acervo de Schengen no âmbito da União Europeia, anexo ao Tratado da União Europeia e ao Tratado sobre o Funcionamento da União Europeia, e do artigo 8.º, n.º 2, da Decisão 2000/365/CE do Conselho, de 29 de maio de 2000, sobre o pedido do Reino Unido da Grã-Bretanha e Irlanda do Norte para participar em algumas das disposições do acervo de Schengen<sup>17</sup>, o Reino Unido fica vinculado pelo presente regulamento.

Irlanda: nos termos do artigo 5.º do Protocolo que integra o acervo de Schengen no âmbito da União Europeia, anexo ao Tratado da União Europeia e ao Tratado sobre o Funcionamento da

---

particular no domínio da luta contra o terrorismo e da criminalidade transfronteiras (JO L 210 de 6.8.2008, p. 12).

<sup>17</sup> JO L 131 de 1.6.2000, p. 43.

União Europeia, e do artigo 6.º, n.º 2, da 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<sup>18</sup>, a Irlanda fica vinculada pelo presente regulamento.

Bulgária e Roménia: o presente regulamento constitui um ato baseado no acervo de Schengen ou de algum modo com ele relacionado, na aceção do artigo 4.º, n.º 2, do Ato de Adesão de 2005. O presente regulamento deve ser conjugado com a Decisão do Conselho 2010/365/UE, de 29 de junho de 2010<sup>19</sup>, que tornou aplicáveis, sob reserva de determinadas restrições, as disposições do acervo de Schengen respeitantes ao Sistema de Informação Schengen na Bulgária e na Roménia.

Chipre e Croácia: o presente regulamento constitui um ato baseado no acervo de Schengen ou de algum modo com ele relacionado, na aceção, respetivamente, do artigo 3.º, n.º 2, do Ato de Adesão de 2003, e do artigo 4.º, n.º 2, do Ato de Adesão de 2011.

Países associados; com base nos acordos de associação da Islândia, Noruega, Suíça e Liechtenstein à execução, à aplicação e ao desenvolvimento do acervo de Schengen, estes Estados ficam vinculados pelo regulamento proposto.

- **Subsidiariedade**

A presente proposta desenvolverá e terá por base o SIS existente, que se encontra em funcionamento desde 1995. O quadro intergovernamental inicial foi substituído por instrumentos da União em 9 de abril de 2013 [Regulamento (CE) n.º 1987/2006 e Decisão 2007/533/JAI do Conselho]. Foram realizadas anteriormente análises completas da subsidiariedade; esta iniciativa visa um aperfeiçoamento suplementar das disposições em vigor, colmatando as lacunas identificadas e melhorando os procedimentos operacionais.

O nível considerável de intercâmbio de informações entre os Estados-Membros através do SIS não pode ser alcançado por meio de soluções descentralizadas. Em virtude da dimensão, dos efeitos e dos impactos das medidas a tomar, a presente proposta poderá ter melhores resultados ao nível da União.

Os objetivos da presente proposta englobam, entre outros aspetos, melhorias técnicas com vista a promover a eficiência do SIS, bem como esforços no sentido de harmonizar a utilização do sistema em todos os Estados-Membros participantes. Devido à natureza transnacional destas metas e dos desafios relativos a um intercâmbio de informações eficaz que combata as ameaças em constante mutação, a UE está bem posicionada para propor soluções para estas questões, algo que não poderá ser suficientemente realizado pelos Estados-Membros isoladamente.

Se as atuais limitações do SIS não forem ultrapassadas, a sua máxima eficácia e o valor acrescentado da UE arriscam-se a ser desperdiçados, além de poderem verificar-se «ângulos mortos» suscetíveis de impedir o trabalho das autoridades competentes. A título de exemplo, a falta de regras harmonizadas quanto à supressão de indicações redundantes dentro do sistema poderá causar entraves à livre circulação das pessoas, que constitui um princípio fundamental da União.

---

<sup>18</sup> JO L 64 de 7.3.2002, p. 20.

<sup>19</sup> Decisão do Conselho, de 29 de junho de 2010, relativa à aplicação das disposições do acervo de Schengen respeitantes ao Sistema de Informação Schengen na República da Bulgária e na Roménia (JO L 166 de 1.7.2010, p. 17).

- **Proporcionalidade**

O artigo 5.º do Tratado da União Europeia estabelece que a ação da União não deve exceder o necessário para alcançar os objetivos previstos no Tratado. A forma escolhida para esta ação da UE deve permitir que a proposta alcance o seu objetivo e seja aplicada com a maior eficácia possível. A iniciativa proposta constitui uma revisão do SIS em relação à cooperação policial e à cooperação judiciária em matéria penal.

A proposta é norteada pelos princípios da *privacidade desde a conceção*. No que se refere ao direito à proteção dos dados pessoais, a presente proposta é proporcionada, dado que estabelece regras específicas de supressão de indicações e não exige a recolha e o armazenamento de dados por um período superior ao estritamente necessário para permitir que o sistema funcione e cumpra os seus objetivos. Tendo por base uma consideração dos requisitos operacionais, a presente proposta reduz o período de conservação das indicações relativas a objetos, uniformizando-o com as indicações relativas a pessoas (uma vez que dizem frequentemente respeito a dados pessoais, tais como documentos de identidade pessoais ou chapas de matrícula). A experiência dos serviços policiais neste domínio demonstra que os bens roubados podem ser recuperados num espaço de tempo relativamente curto, pelo que um prazo de 10 anos para as indicações relativas a objetos se afigura desnecessariamente extenso.

As indicações do SIS apenas incluem os dados necessários para identificar e localizar uma pessoa ou um objeto e para permitir a adoção das medidas operacionais adequadas. Todas as restantes informações adicionais são facultadas por intermédio dos Gabinetes SIRENE que permitem o intercâmbio de informações suplementares.

Além disso, a proposta determina a implementação de todas as garantias e mecanismos necessários para a proteção efetiva dos direitos fundamentais dos titulares dos dados, especialmente a proteção da sua vida privada e dados pessoais. Inclui adicionalmente disposições concebidas especificamente para reforçar a segurança dos dados pessoais das pessoas singulares conservados no SIS.

Não serão necessários outros processos ou harmonizações ao nível da UE para garantir o funcionamento do sistema. A medida prevista é proporcionada, pois não excede o estritamente necessário em termos de ação ao nível da UE para atingir os objetivos definidos.

- **Escolha do instrumento**

A revisão proposta assumirá a forma de regulamento e substituirá a Decisão 2007/533/JAI do Conselho, embora mantendo grande parte do seu conteúdo. A Decisão 2007/533/JAI foi adotada enquanto instrumento do chamado «terceiro pilar», ao abrigo do anterior Tratado da União Europeia. Estes instrumentos do «terceiro pilar» eram adotados pelo Conselho, sem a participação do Parlamento Europeu enquanto colegislador. A base jurídica da presente proposta consta do Tratado sobre o Funcionamento da União Europeia (TFUE), pois a estrutura em pilares deixou de existir com a entrada em vigor do Tratado de Lisboa em 1 de dezembro de 2009. A base jurídica pressupõe a aplicação do processo legislativo ordinário. Deve ser escolhida a forma de regulamento (do Parlamento Europeu e do Conselho), já que as disposições terão de ser vinculativas e diretamente aplicáveis em todos os Estados-Membros.

A proposta tem por base e desenvolve um sistema centralizado existente, através do qual os Estado-Membros cooperam entre si, o que exige uma arquitetura comum e regras operacionais vinculativas. Além disso, estabelece regras obrigatórias relativas ao acesso ao sistema, nomeadamente para efeitos de aplicação coerciva da lei, as quais serão uniformes



para todos os Estados-Membros e para a Agência europeia para a gestão operacional de sistemas informáticos de grande escala no espaço de liberdade, segurança e justiça<sup>20</sup> (eu-LISA). Desde 9 de maio de 2013, a eu-LISA é responsável pela gestão operacional do SIS Central, que engloba todas as atribuições necessárias para assegurar o pleno funcionamento do SIS Central, 24 horas por dia e sete dias por semana. A presente proposta consolida as responsabilidades da eu-LISA em relação ao SIS.

Por outro lado, a proposta prevê regras diretamente aplicáveis que possibilitam aos titulares dos dados o acesso aos seus próprios dados e vias de recurso, sem que sejam requeridas medidas de execução adicionais a este respeito.

Por conseguinte, o instrumento jurídico escolhido só pode ser um regulamento.

### **3. RESULTADOS DAS AVALIAÇÕES *EX POST*, DAS CONSULTAS DAS PARTES INTERESSADAS E DAS AVALIAÇÕES DE IMPACTO**

#### **• Avaliações *ex post*/balanços de qualidade da legislação existente**

Em conformidade com o Regulamento (UE) n.º 1987/2006 e a Decisão 2007/533/JAI do Conselho, três anos após a sua entrada em funcionamento, a Comissão realizou uma avaliação global do SIS II Central, bem como do intercâmbio bilateral e multilateral de informações suplementares entre os Estados-Membros.

Os resultados da avaliação frisaram a necessidade de proceder a alterações na base jurídica do SIS, a fim de responder melhor aos novos desafios de segurança e de migração. Entre estas alterações incluem-se, por exemplo, uma proposta de tomada em conta da utilização do SIS de extremo a extremo, regulando a sua utilização pelos utilizadores finais e fixando normas de segurança dos dados que lhes sejam igualmente aplicáveis, o reforço do sistema para fins de luta contra o terrorismo, prevendo uma nova conduta a adotar para o efeito, a clarificação da situação das crianças que enfrentam a ameaça de rapto parental, bem como o alargamento da lista dos identificadores biométricos disponíveis no sistema.

Os resultados da avaliação evidenciaram igualmente a necessidade de alterações jurídicas para melhorar o funcionamento técnico do sistema e simplificar os procedimentos nacionais. Estas medidas permitirão uma maior eficiência e eficácia do SIS, ao facilitar a sua utilização e reduzir os encargos desnecessários. Outras medidas destinam-se a promover a qualidade dos dados e a transparência do sistema, através de uma descrição mais clara das competências específicas dos Estados-Membros e da eu-LISA em matéria de elaboração de relatórios.

Os resultados dessa avaliação exaustiva (o relatório de avaliação e o correspondente documento de trabalho dos serviços da Comissão foram aprovados em 21 de dezembro de 2016<sup>21</sup>) constituíram a base das medidas contidas na presente proposta.

#### **• Consulta das partes interessadas**

Durante a avaliação do SIS por parte da Comissão, foram solicitadas observações e sugestões às partes interessadas, incluindo aos delegados do Comité SIS-VIS, no âmbito do

---

<sup>20</sup> Estabelecida pelo Regulamento (UE) n.º 1077/2011 do Parlamento Europeu e do Conselho, de 25 de outubro de 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 286 de 1.11.2011, p. 1).

<sup>21</sup> Relatório ao Parlamento Europeu e ao Conselho sobre a avaliação do Sistema de Informação de Schengen de segunda geração (SIS II) em conformidade com o artigo 24.º, n.º 5, o artigo 43.º, n.º 5 e o artigo 50.º, n.º 5, do Regulamento (CE) n.º 1987/2006, e com o artigo 59.º, n.º 3, e o artigo 65.º, n.º 5, da Decisão 2007/533/JAI e o documento de trabalho correspondente dos serviços da Comissão

procedimento previsto no artigo 67.º da Decisão 2007/533/JAI do Conselho. Este comité conta com os representantes dos Estados-Membros quer para questões operacionais ligadas às SIRENE (cooperação transfronteiriça em relação ao SIS) quer para as questões técnicas respeitantes ao desenvolvimento e à manutenção do SIS e da correspondente aplicação SIRENE.

Os delegados responderam a questionários pormenorizados, no quadro do processo de avaliação. Sempre que foram necessários esclarecimentos ou o assunto carecia de desenvolvimento, recorreu-se a trocas de correspondência eletrónica ou a entrevistas seletivas. Este processo iterativo permitiu suscitar questões de forma abrangente e transparente. Ao longo de 2015 e 2016, os delegados do Comité SIS-VIS analisaram estas questões em reuniões e sessões de trabalho temáticas.

A Comissão também consultou especificamente as autoridades nacionais de proteção de dados nos Estados-Membros e os membros do Grupo de Coordenação e Supervisão do SIS II no domínio da proteção de dados. Os Estados-Membros partilharam as suas experiências relativas aos pedidos de acesso por titulares dos dados, bem como o trabalho das autoridades nacionais de proteção de dados, respondendo a um questionário temático. As respostas a este questionário, de junho de 2015, serviram de base à elaboração da presente proposta.

Internamente, a Comissão criou um grupo diretor interserviços, que inclui o Secretariado-Geral e as Direções-Gerais da Migração e dos Assuntos Internos, da Justiça e dos Consumidores, dos Recursos Humanos e da Segurança, e da Informática. Este grupo diretor acompanhou o processo de avaliação e formulou orientações sempre que necessário.

As conclusões da avaliação tiveram igualmente em conta os elementos factuais recolhidos durante as visitas de avaliação no terreno aos Estados-Membros, examinando em pormenor a forma como o SIS é utilizado na prática. Neste contexto, foram realizados encontros e entrevistas com os técnicos, pessoal dos gabinetes SIRENE e autoridades nacionais competentes.

Atendendo às observações recebidas, a presente proposta prevê medidas destinadas a melhorar a eficiência e eficácia nos planos técnico e operacional do sistema.

- **Recolha e utilização de conhecimentos especializados**

Além das consultas das partes interessadas, a Comissão também recorreu a conhecimentos especializados externos, materializados em quatro estudos, cujas conclusões foram incorporadas na elaboração da presente proposta:

- *SIS Technical Assessment* (Kurt Salmon)<sup>22</sup>

Esta avaliação identificou os principais problemas no funcionamento do SIS e as necessidades que importará suprir no futuro, assinalando prioritariamente as preocupações relativas à maximização da continuidade das operações e à efetiva adaptação da arquitetura global ao aumento das exigências de capacidade.

- *ICT Impact Assessment of Possible Improvements to the SIS II Architecture* (Kurt Salmon)<sup>23</sup>

Este estudo avaliou os custos atuais do funcionamento do SIS ao nível nacional e ponderou dois possíveis cenários técnicos de aperfeiçoamento do sistema. Ambos os

---

<sup>22</sup> Relatório Final da Comissão Europeia — avaliação técnica do SIS II.

<sup>23</sup> Relatório Final da Comissão Europeia — *ICT Impact Assessment of Possible Improvements to the SIS II Architecture* 2016.

cenários abrangem um conjunto de propostas técnicas que incidem em aperfeiçoamentos do sistema central e da arquitetura global.

- «ICT Impact Assessment of the technical improvements to the SIS II architecture – Final Report», 10 de novembro de 2016 (Wavestone)<sup>24</sup>

Este estudo avaliou os impactos, em termos de custos para os Estados-Membros, da implementação de uma cópia nacional, analisando três cenários (um sistema totalmente centralizado, uma implementação normalizada dos N.SIS desenvolvida e proporcionada pela eu-LISA aos Estados-Membros e uma implementação distinta dos N.SIS com normas técnicas comuns).

- **Avaliação de impacto**

A Comissão não efetuou uma avaliação de impacto.

As três avaliações independentes acima mencionadas (na secção «Recolha e utilização de conhecimentos especializados») alicerçaram a ponderação dos impactos das alterações propostas ao sistema numa perspetiva técnica. Além disso, a Comissão finalizou duas revisões do Manual SIRENE desde 2013, ou seja, desde que o SIS II entrou em funcionamento, em 9 de abril de 2013, e desde que a Decisão 2007/533/JAI se tornou aplicável. Inclui-se uma avaliação intercalar, que deu origem ao lançamento de um novo Manual SIRENE<sup>25</sup> em 29 de janeiro de 2015. A Comissão adotou igualmente um inventário de práticas de excelência e recomendações<sup>26</sup>. Além disso, a eu-LISA e os Estados-Membros procedem a melhorias técnicas do sistema de forma periódica e iterativa. Considera-se que estas opções estão agora esgotadas, impondo-se uma alteração mais global da base jurídica. Não é possível, apenas através da melhoria da implementação e execução, obter um quadro claro em domínios como a aplicação de sistemas para os utilizadores finais, nem regras pormenorizadas sobre a supressão das indicações.

Por outro lado, a Comissão realizou uma avaliação exaustiva do SIS, cumprindo o disposto no artigo 24.º, n.º 5, no artigo 43.º, n.º 3, e no artigo 50.º, n.º 5, do Regulamento (CE) n.º 1987/2006, e no artigo 59.º, n.º 3, e no artigo 66.º, n.º 5, da Decisão 2007/533/JAI, tendo publicado um documento de trabalho a acompanhar a avaliação. Os resultados da avaliação exaustiva (o relatório de avaliação e o correspondente documento de trabalho dos serviços da Comissão foram aprovados em 21 de dezembro de 2016) constituíram a base das medidas constantes da presente proposta.

O mecanismo de avaliação de Schengen, definido no Regulamento (UE) n.º 1053/2013<sup>27</sup>, permite examinar periodicamente as vertentes jurídica e operacional do funcionamento do SIS

---

<sup>24</sup> Relatório Final da Comissão Europeia — «ICT Impact Assessment of the technical improvements to the SIS II architecture – Final Report» («Avaliação de Impacto dos Aperfeiçoamentos Técnicos da Arquitetura do SIS II no âmbito das TIC»), 10 de novembro de 2016 (Wavestone).

<sup>25</sup> Decisão de Execução (UE) 2015/219 da Comissão, de 29 de janeiro de 2015, que substitui o anexo da Decisão de Execução 2013/115/UE relativa ao Manual Sirene e outras medidas de execução para o Sistema de Informação de Schengen de segunda geração (SIS II) (JO L 44 de 18.2.2015, p. 75).

<sup>26</sup> Recomendação da Comissão que cria um inventário de recomendações e práticas de excelência para a correta aplicação do Sistema de Informação de Schengen de segunda geração (SIS II) e o intercâmbio de informações suplementares pelas autoridades competentes dos Estados-Membros que aplicam e utilizam o SIS II [C(2015)9169/1].

<sup>27</sup> Regulamento (UE) n.º 1053/2013 do Conselho, de 7 de outubro de 2013, que cria um mecanismo de avaliação e de monitorização para verificar a aplicação do acervo de Schengen e que revoga a Decisão do Comité Executivo, de 16 de setembro de 1998, relativa à criação de uma comissão permanente de avaliação e de aplicação de Schengen (JO L 295 de 6.11.2013, p. 27).

nos Estados-Membros. As avaliações são realizadas conjuntamente pela Comissão e pelos Estados-Membros. Através deste mecanismo, o Conselho formula recomendações aos Estados-Membros individualmente, com base nas avaliações efetuadas no âmbito dos programas anuais e plurianuais. Devido à sua natureza individual, estas recomendações não podem substituir-se às normas juridicamente vinculativas que sejam simultaneamente aplicáveis a todos os Estados-Membros que utilizam o SIS.

O Comité SIS-VIS analisa regularmente questões práticas operacionais e técnicas. Apesar de estas reuniões serem essenciais na cooperação entre a Comissão e os Estados-Membros, os resultados destas análises (alterações legislativas ausentes) não podem solucionar, por exemplo, problemas decorrentes de práticas nacionais divergentes.

As alterações propostas no presente regulamento não apresentam um impacto significativo em termos económicos ou ambientais. Contudo, espera-se que estas alterações produzam um impacto social altamente positivo, já que preveem uma maior segurança ao permitir uma identificação melhorada de pessoas que usam falsas identidades, de autores de crimes cuja identidade permanece desconhecida após terem cometido crimes graves, bem como de menores desaparecidos. O impacto destas alterações sobre os direitos fundamentais e a proteção de dados foi ponderado, sendo descrito de forma mais detalhada na próxima secção («Direitos fundamentais»).

A elaboração da proposta explorou o vasto leque de elementos factuais recolhidos para fundamentar a avaliação global da segunda geração do SIS, que examinou o funcionamento do sistema e os possíveis aspetos a melhorar. Paralelamente, foi realizado um estudo de avaliação dos impactos em termos de custos, a fim de garantir que a arquitetura nacional selecionada seja a mais indicada e proporcionada.

- **Direitos fundamentais e proteção de dados**

A presente proposta desenvolve e reforça um sistema já existente, em vez de se criar um novo e apoia-se, portanto, em garantias efetivas importantes já existentes. No entanto, como o sistema continua a tratar dados pessoais e tratará igualmente novas categorias de dados biométricos sensíveis, existem impactos potenciais sobre os direitos fundamentais das pessoas. Estes eventuais impactos foram minuciosamente considerados, tendo sido instauradas garantias adicionais para limitar a recolha e o subsequente tratamento de dados ao estritamente necessário e aos procedimentos operacionais exigidos, bem como restringir o acesso a esses dados a quem tenha de os tratar para efeitos operacionais. A presente proposta estabelece prazos de conservação de dados bem definidos, incluindo períodos de conservação mais curtos para as indicações relativas a objetos. São explicitamente reconhecidos e previstos os direitos das pessoas a acederem e retificarem os dados que lhes digam respeito, bem como a solicitar o seu apagamento, em conformidade com os seus direitos fundamentais (ver secção «Proteção dos dados e segurança»).

Além disso, a proposta reforça as medidas destinadas a proteger os direitos fundamentais, dado que inscreve na legislação os requisitos aplicáveis à supressão das indicações e introduz uma avaliação da proporcionalidade no caso de uma indicação ser prorrogada. Será possível identificar as pessoas com maior fiabilidade através da utilização de dados biométricos para as pessoas desaparecidas que necessitem de proteção, assegurando que os dados pessoais são exatos e estão devidamente protegidos. A proposta define garantias amplas e sólidas quanto à utilização de identificadores biométricos, a fim de evitar transtornos para pessoas inocentes.

A proposta exige, além disso, a segurança de extremo a extremo do sistema, assegurando uma maior proteção dos dados armazenados no mesmo. Com a instauração de um procedimento claro de gestão de incidentes, bem como uma continuidade melhorada das atividades para o

SIS, a presente proposta cumpre integralmente a Carta dos Direitos Fundamentais da União Europeia<sup>28</sup> no que se refere ao direito à proteção dos dados pessoais. O desenvolvimento e a eficácia contínua do SIS contribuirão para a segurança das pessoas na sociedade.

A proposta prevê alterações significativas quanto aos identificadores biométricos. Além das impressões digitais, também devem ser recolhidas e armazenadas impressões palmares, desde que estejam preenchidos os requisitos legais. Os registos de impressões digitais são apenas as indicações alfanuméricas do SIS, tal como disposto nos artigos 26.º, 32.º, 34.º e 36.º. Será conveniente, no futuro, poder pesquisar estes dados dactilográficos (impressões digitais e impressões palmares) com impressões digitais detetadas no local de um crime, desde que esse crime constitua um crime grave ou um ato terrorista e que se possa afirmar, com elevado grau de probabilidade, que as impressões digitais pertencem ao seu autor. Além disso, a proposta prevê o armazenamento de impressões digitais relativas às chamadas «pessoas desconhecidas procuradas» (as condições aplicáveis estão descritas em pormenor na secção 5, subsecção «Fotografias, imagens faciais, dados dactilográficos e perfis de ADN»). Em caso de incerteza quanto à identidade de uma pessoa de acordo com os seus documentos, as autoridades competentes devem proceder a uma pesquisa de impressões digitais comparativa com as impressões digitais armazenadas na base de dados do SIS.

A proposta exige que sejam recolhidos e armazenados dados adicionais (tais como informações dos documentos de identidades pessoais) que facilitem o trabalho dos agentes no terreno com vista a determinar a identidade de uma pessoa.

Por outro lado, a proposta garante o direito do titular dos dados a um recurso efetivo para contestar qualquer decisão, nas quais deve estar sempre incluído o direito de ação para um órgão jurisdicional, em conformidade com o artigo 47.º da Carta dos Direitos Fundamentais.

#### **4. INCIDÊNCIA ORÇAMENTAL**

O SIS constitui um sistema de informação único. Como tal, as despesas previstas em duas das propostas (a presente proposta e a proposta de regulamento relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen (SIS) no domínio dos controlos das fronteiras) não devem ser tidas em conta como dois montantes distintos, mas antes como um montante único. A incidência orçamental das alterações necessárias para a implementação das duas propostas está incluída numa ficha financeira legislativa.

Devido à natureza complementar da terceira proposta (relativa ao regresso dos nacionais de países terceiros em situação irregular), a incidência orçamental é considerada separadamente, e numa ficha financeira independente que aborda apenas o estabelecimento desta categoria específica de indicações.

Com base numa avaliação dos vários aspetos do trabalho necessário em relação à rede, ao SIS Central por parte da eu-LISA e aos desenvolvimentos ao nível dos Estados-Membros, as duas propostas de regulamento exigirão um montante total de 64,3 milhões de EUR para o período de 2018-2020.

Este valor cobre um aumento da banda larga TESTA-NG, uma vez que, ao abrigo das duas propostas, a rede vai transmitir ficheiros de impressões digitais e imagens faciais, requerendo um débito e uma capacidade acrescidos (9,9 milhões de EUR). Cobre igualmente os custos da eu-LISA respeitantes a despesas com pessoal e operacionais (17,6 milhões de EUR). A eu-LISA informou a Comissão de que está previsto o recrutamento de três novos agentes contratuais para janeiro de 2018, a fim de iniciar a fase de desenvolvimento em tempo útil e

---

<sup>28</sup> Carta dos Direitos Fundamentais da União Europeia (2012/C 326/02).

assegurar a entrada em serviço das funcionalidades atualizadas do SIS em 2020. A presente proposta engloba modificações técnicas do SIS Central destinadas a alargar algumas das categorias de indicações existentes e a fornecer novas funcionalidades. A ficha financeira anexa à presente proposta reflete estas alterações.

Além disso, a Comissão realizou um estudo de avaliação do impacto em termos de custos, no sentido de avaliar os custos dos desenvolvimentos nacionais requeridos pela presente proposta<sup>29</sup>. O custo estimado ascende a 36,8 milhões de EUR, que devem ser distribuídos aos Estados-Membros por meio de montantes fixos. Assim, cada Estado-Membro receberá o montante de 1,2 milhões de EUR para melhorar o seu sistema nacional de acordo com os requisitos definidos na presente proposta, incluindo a criação de uma cópia nacional parcial, nos casos em que ainda não existe, ou de um sistema de salvaguarda.

Está prevista uma reprogramação da parte remanescente da dotação reservada às fronteiras inteligentes no âmbito do Fundo para a Segurança Interna, no intuito de realizar atualizações e implementar as funcionalidades previstas nas duas propostas. O Regulamento relativo ao FSI-Fronteiras<sup>30</sup> é o instrumento financeiro no qual foi incluído o orçamento para a aplicação do pacote sobre as fronteiras inteligentes. O artigo 5.º do regulamento em causa prevê que 791 milhões de EUR devem ser aplicados através de um programa para a criação de sistemas informáticos de apoio à gestão dos fluxos migratórios nas fronteiras externas, nos termos do artigo 15.º. Destes 791 milhões de EUR, 480 milhões de EUR estão reservados ao desenvolvimento do Sistema de Entrada/Saída e 210 milhões de EUR ao desenvolvimento do Sistema Europeu de Informação e Autorização de Viagem (ETIAS). A parte remanescente será parcialmente utilizada para cobrir os custos das alterações previstas nas duas propostas no que toca ao SIS.

## 5. OUTROS ELEMENTOS

### • Planos de execução e mecanismos de acompanhamento, de avaliação e de informação

A Comissão, os Estados-Membros e a eu-LISA avaliarão e acompanharão regularmente a utilização do SIS, a fim de garantir que continua a funcionar com eficácia e eficiência. A Comissão será assistida pelo Comité SIS-VIS na aplicação das medidas técnicas e operacionais, conforme descrito na proposta.

Além disso, a presente proposta de regulamento prevê, no artigo 71.º, n.ºs 7 e 8, um processo de revisão e avaliação formal e periódico.

De dois em dois anos, a eu-LISA deve apresentar ao Parlamento Europeu e ao Conselho um relatório sobre o funcionamento técnico do SIS, incluindo sobre a segurança, a infraestrutura de comunicação que o apoia e o intercâmbio bilateral e multilateral de informações suplementares entre os Estados-Membros.

Além disso, de quatro em quatro anos, a Comissão deve efetuar e partilhar com o Parlamento e o Conselho, uma avaliação global do SIS e do intercâmbio de informações entre os Estados-Membros, com as seguintes finalidades:

- aferir os resultados obtidos relativamente aos objetivos fixados;

<sup>29</sup> Wavestone, *ICT Impact Assessment of the technical improvements to the SIS II architecture – Final Report*, 10 de novembro de 2016; Cenário 3: implementação distinta dos N.SIS II.

<sup>30</sup> 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 (JO L 150 de 20.5.2014, p. 143).

- avaliar se os princípios subjacentes continuam a ser válidos;
- analisar a forma como o regulamento é aplicado ao sistema central;
- avaliar a segurança do sistema central;
- explorar as implicações para o funcionamento do sistema no futuro.

Além disso, a eu-LISA passa a estar encarregada de facultar estatísticas diárias, mensais e anuais sobre a utilização do SIS, assegurando um acompanhamento constante do sistema e do seu funcionamento comparativamente com os seus objetivos.

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

**Disposições comuns à presente proposta e à proposta de regulamento relativo ao estabelecimento, ao funcionamento e à utilização do SIS no domínio dos controlos das fronteiras**

- Disposições gerais (artigos 1.º – 3.º)
- Arquitetura técnica e modo de funcionamento do SIS (artigos 4.º – 14.º)
- Responsabilidades da eu-LISA (artigos 15.º – 18.º)
- Direito ao acesso e conservação das indicações (artigos 43.º, 46.º, 48.º, 50.º e 51.º)
- Regras gerais de tratamento e de proteção de dados (artigos 53.º – 70.º)
- Acompanhamento e estatísticas (artigo 71.º)

**Utilização de extremo a extremo do SIS**

Com mais de 2 milhões de utilizadores finais nas autoridades competentes em toda a Europa, o SIS constitui um instrumento extremamente utilizado e eficaz para o intercâmbio de informações. As presentes propostas incluem regras que abrangem o funcionamento de extremo a extremo do sistema, incluindo a gestão do SIS Central pela eu-LISA, os sistemas nacionais e as aplicações dos utilizadores finais. Referem-se não só aos sistemas central e nacionais, mas também às necessidades técnicas e operacionais dos utilizadores finais.

O artigo 9.º, n.º 2, especifica que os utilizadores finais devem receber os dados necessários para o desempenho das suas funções (nomeadamente todos os dados necessários para a identificação do titular dos dados e para adotar a conduta adequada). Além disso, estabelece um modelo comum de implementação do SIS pelos Estados-Membros, assegurando que todos os sistemas nacionais estejam harmonizados. O artigo 6.º estipula que cada Estado-Membro deve garantir aos utilizadores finais uma disponibilização ininterrupta dos dados do SIS, por forma a maximizar as vantagens operacionais através da redução das possibilidades de períodos de inatividade.

O artigo 10.º, n.º 3, garante que a segurança do tratamento de dados inclui igualmente as atividades de tratamento de dados pelo utilizador final. O artigo 14.º obriga os Estados-Membros a assegurar uma formação regular e contínua do pessoal com acesso ao SIS sobre as normas de segurança de dados e proteção de dados.

Em resultado da inclusão destas medidas, a presente proposta abrange de forma mais completa o funcionamento integral de extremo a extremo do SIS, com regras e obrigações relativas aos milhões de utilizadores finais em toda a Europa. Com vista a potenciar ao máximo a eficácia da utilização do SIS, os Estados-Membros devem assegurar que, sempre que os respetivos utilizadores finais sejam autorizados a consultar uma base de dados nacional da polícia ou dos serviços de imigração, consultem também o SIS em paralelo. Desta forma, o

SIS pode cumprir o seu objetivo enquanto principal medida compensatória no espaço sem controlos nas fronteiras internas, e os Estados-Membros podem melhorar a sua abordagem à dimensão transfronteiriça da criminalidade e à mobilidade dos autores de crimes. Esta consulta paralela deve respeitar o disposto no artigo 4.º da Diretiva (UE) 2016/680<sup>31</sup>.

### **Continuidade das atividades**

As propostas reforçam as disposições em matéria de continuidade das atividades, tanto ao nível nacional como para a eu-LISA (artigos 4.º, 6.º, 7.º e 15.º). Garante-se, deste modo, que o SIS se mantém funcional e acessível para o pessoal no terreno, mesmo no caso de surgirem problemas que afetem o sistema.

### **Qualidade dos dados**

A proposta mantém o princípio de que o Estado-Membro, que é o detentor dos dados, é igualmente responsável pela exatidão dos dados introduzidos no SIS (artigo 56.º). No entanto, é necessário determinar a criação de um mecanismo central gerido pela eu-LISA, que permita aos Estados-Membros rever periodicamente as indicações nas quais os campos de dados obrigatórios sejam suscetíveis de gerar problemas de qualidade. Por conseguinte, o artigo 15.º da proposta habilita a eu-LISA a elaborar, a intervalos regulares, relatórios de qualidade dos dados, destinados aos Estados-Membros. Esta atividade poderá ser facilitada por um repositório de dados para a elaboração de relatórios estatísticos e sobre a qualidade dos dados (artigo 71.º). As melhorias sugeridas refletem as conclusões preliminares do Grupo de Peritos de Alto Nível em matéria de Sistemas de Informação e Interoperabilidade.

### **Fotografias, imagens faciais, dados dactilográficos e perfis de ADN**

A possibilidade de efetuar pesquisas com impressões digitais no sentido de identificar uma pessoa já está prevista no artigo 22.º do Regulamento (CE) n.º 1987/2006 e na Decisão 2007/533/JAI do Conselho. As propostas em apreço tornam esta pesquisa obrigatória caso a identidade da pessoa não possa ser apurada de outro modo. Além do mais, as alterações ao artigo 22.º e os novos artigos 40.º, 41.º e 42.º vão permitir a utilização de imagens faciais, impressões palmares e perfis de ADN para identificar pessoas, juntamente com a utilização de impressões digitais. Atualmente, as imagens faciais apenas podem ser utilizadas para confirmar a identidade da pessoa na sequência de uma pesquisa alfanumérica, e não como base da consulta. A dactiloscopia refere-se ao estudo científico das impressões digitais enquanto método de identificação. Os peritos em dactilografia admitem que as impressões palmares apresentam traços únicos, contendo pontos de referência que possibilitam comparações exatas e conclusivas, à semelhança das impressões digitais. As impressões palmares podem servir para determinar a identidade de uma pessoa da mesma forma que as impressões digitais. A recolha de impressões palmares juntamente com as dez impressões digitais planas e dez impressões digitais roladadas de cada indivíduo tem sido uma prática habitual das polícias há várias décadas. As impressões palmares têm duas aplicações principais:

- i) Fins de identificação quando a pessoa danificou, intencionalmente ou não, as extremidades dos dedos. Este tipo de situação pode ser causado por uma tentativa de a pessoa evitar a sua identificação ou que as suas impressões digitais sejam recolhidas, ou por um acidente ou desgaste devido a trabalho manual pesado. No

---

<sup>31</sup> 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 (JO L 119 de 4.5.2016, p. 89).



decurso dos debates sobre as normas técnicas do AFIS do SIS, Itália deu conta de excelentes resultados na identificação de migrantes em situação irregular que tinham danificado intencionalmente as extremidades dos dedos na tentativa de evitar a sua identificação. A recolha de impressões palmares por parte das autoridades italianas permitiu a subsequente identificação;

- ii) As impressões digitais latentes colhidas no local de um crime. Em muitos casos, o suspeito deixa vestígios no local de um crime, os quais revelam ser provenientes da palma da mão. Só através de uma recolha de rotina de impressões palmares, quando são legalmente recolhidas as impressões digitais de uma pessoa, é possível identificar o suspeito. As impressões palmares também contêm, por norma, informações provenientes da base dos dedos e que estão muitas vezes em falta nas impressões digitais planas e roladas colhidas, uma vez que estas últimas se concentram tendencialmente nas extremidades dos dedos e nas articulações superiores.

O recurso a imagens faciais proporcionará uma maior coerência entre o SIS e os mecanismos propostos do Sistema de Entrada/Saída da UE, das cancelas eletrónicas e dos terminais de self-service. Esta funcionalidade será limitada aos pontos de passagem regular das fronteiras.

Nos casos em que não estão disponíveis impressões digitais ou impressões palmares, o artigo 22.º, n.º 1, permite a utilização de perfis de ADN para as pessoas desaparecidas que precisam de ser colocadas sob proteção, especialmente as crianças. Esta funcionalidade será utilizada unicamente na ausência de impressões digitais e apenas estará acessível aos utilizadores autorizados. Por conseguinte, esta disposição permite o recurso a perfis de ADN por intermédio dos pais ou irmãos da pessoa/criança desaparecida, para que as autoridades nacionais possam identificar e localizar a pessoa em causa. Estas informações já são partilhadas pelos Estados-Membros entre si ao nível operacional, mediante o intercâmbio de informações suplementares. A presente proposta estabelece um quadro regulamentar sobre esta prática, incorporando-a na base legislativa substantiva do funcionamento e utilização do SIS e instituindo procedimentos claros quanto às circunstâncias em que tais perfis poderão ser utilizados.

As alterações propostas vão igualmente permitir a emissão de indicações do SIS para as pessoas desconhecidas procuradas devido a um crime, com base em impressões digitais ou impressões palmares (artigos 40.º-42.º). Estas indicações podem ser criadas, por exemplo, nos casos em que são encontradas impressões digitais ou impressões palmares latentes no local de um crime grave e em que há sérios motivos para suspeitar que as impressões digitais pertencem ao autor desse crime, ou quando são encontradas impressões digitais numa arma usada na prática de um crime ou em qualquer outro objeto usado pelo autor de um crime no momento em que o cometeu. Esta nova categoria de indicações complementa as disposições de Prüm, que permite a interconectividade dos sistemas nacionais de identificação criminal por impressões digitais. Por intermédio do mecanismo Prüm, um Estado-Membro pode apresentar um pedido no sentido de verificar se o autor de um crime cujas impressões digitais foram encontradas é conhecido noutra Estado-Membro (por norma, para fins de investigação). Apenas é possível identificar uma pessoa através do mecanismo Prüm se as suas impressões digitais tiverem sido recolhidas noutra Estado-Membro por motivos penais. Enquanto tal, os infratores sem antecedentes criminais não podem ser identificados. Os desenvolvimentos constantes da presente proposta, designadamente o armazenamento de impressões digitais de pessoas desconhecidas procuradas, permitirão que as impressões digitais do autor desconhecido de um crime sejam descarregadas no SIS, de modo a que possa ser identificado como pessoa procurada se for encontrado noutra Estado-Membro. O recurso a esta funcionalidade pressupõe que os Estados-Membros tenham consultado previamente todas as fontes nacionais e internacionais disponíveis, não tendo logrado apurar a identidade da pessoa

em causa. Estão previstas garantias suficientes na proposta para assegurar que, para esta categoria, o SIS armazene unicamente as impressões digitais das pessoas sobre as quais recaem fortes suspeitas da autoria de um crime grave ou um ato terrorista. Neste sentido, a utilização desta nova categoria de indicações apenas pode ser autorizada nos casos em que o autor desconhecido representa um risco grave para a segurança pública, justificando-se a comparação destas impressões com as impressões digitais dos viajantes, por exemplo para evitar que a pessoa em causa saia do espaço sem controlos nas fronteiras internas.

Esta disposição não permite que os utilizadores finais insiram impressões digitais no âmbito desta categoria quando não é possível estabelecer a relação das mesmas com o autor do crime. Outra condição será a impossibilidade de determinar a identidade da pessoa em causa com recurso a qualquer outra base de dados nacional, europeia ou internacional de armazenamento de impressões digitais. Uma vez armazenadas no SIS, as impressões digitais serão utilizadas para identificar pessoas cuja identidade não possa ser apurada de outro modo. No caso de uma verificação dar origem a uma possível concordância, o Estado-Membro deve realizar verificações adicionais com as impressões digitais, recorrendo eventualmente a peritos em impressões digitais para averiguar se as impressões armazenadas no SIS pertencem à pessoa em causa e apurar a identidade da pessoa. Estes procedimentos estão sujeitos à legislação nacional. Uma identificação correspondente a uma «pessoa desconhecida procurada» no SIS é suscetível de dar lugar a uma detenção.

### **Acesso ao SIS**

A presente subsecção descreve os novos elementos em termos de direitos de acesso ao SIS no que respeita às autoridades nacionais competentes e às agências da UE (utilizadores institucionais).

### **Autoridades nacionais - autoridades de imigração**

Com vista a maximizar a eficácia da utilização do SIS, a proposta faculta o acesso ao SIS às autoridades nacionais responsáveis por examinar as condições e adotar as decisões em matéria de entrada, permanência e regresso de nacionais de países terceiros no território dos Estados-Membros. Este aditamento permite a consulta do SIS respeitante aos migrantes em situação irregular que não tenham sido objeto de verificação nos controlos regulares de fronteira. A presente proposta garante a igualdade de tratamento dos nacionais de países terceiros que atravessam as fronteiras externas nos pontos de passagem regular das fronteiras (sendo, portanto, sujeitos aos controlos aplicáveis aos nacionais de países terceiros) e dos nacionais de países terceiros que chegam irregularmente ao espaço Schengen.

Além disso, ao abrigo da presente proposta, as autoridades responsáveis pela matrícula de veículos (artigo 44.º), embarcações e aeronaves terão um acesso ao sistema limitado ao desempenho das suas funções, desde que sejam serviços da administração pública. Tal contribuirá para evitar que os meios de transporte referidos que tenham sido roubados e sejam procurados noutros Estados-Membros possam ser novamente matriculados. Esta iniciativa não é nova quanto aos serviços de matrícula de veículos, uma vez que o seu acesso ao SIS já estava previsto pelo artigo 102.º-A da Convenção de Schengen e pelo Regulamento (CE) n.º 1986/2006<sup>32</sup>. Segundo a mesma lógica, nos termos desta proposta, as autoridades competentes pelo registo de embarcações e aeronaves podem aceder às indicações do SIS relativas a estes meios de transporte.

---

<sup>32</sup> Regulamento (CE) n.º 1986/2006 do Parlamento Europeu e do Conselho, de 20 de dezembro de 2006, relativo ao acesso ao Sistema de Informação de Schengen de segunda geração (SIS II) dos serviços dos Estados-Membros competentes para a emissão dos certificados de matrícula dos veículos (JO L 381 de 28.12.2006, p. 1).

## **Utilizadores institucionais**

A Europol (artigo 46.º), a Eurojust (artigo 47.º) e a Agência Europeia da Guarda de Fronteiras e Costeira, bem como as respetivas equipas, as equipas envolvidas em operações de regresso e os membros da equipa de apoio à gestão da migração (artigos 48.º e 49.º), têm acesso ao SIS e aos dados do SIS de que necessitam. São estabelecidas garantias adequadas para assegurar que os dados no sistema sejam devidamente protegidos (incluindo também o disposto no artigo 50.º, que determina que os referidos organismos apenas poderão aceder aos dados de que necessitam para o desempenho das suas funções).

Estas alterações alargam o acesso ao SIS por parte da Europol às indicações de recusa de entrada, providenciando-lhe uma melhor utilização do sistema quando exerce as suas funções, e aditam novas disposições que conferem à Agência Europeia da Guarda de Fronteiras e Costeira e às respetivas equipas a possibilidade de aceder ao sistema enquanto executam as diferentes operações no âmbito do seu mandato, apoiando assim os Estados-Membros. No contexto do trabalho desenvolvido pelo Grupo de Peritos de Alto Nível em matéria de Sistemas de Informação e Interoperabilidade, e com vista a reforçar a partilha de informações sobre terrorismo, a Comissão avaliará se a Europol deve receber automaticamente uma notificação do SIS quando é criada uma indicação sobre uma atividade relacionada com o terrorismo.

Além disso, ao abrigo da proposta da Comissão de regulamento do Parlamento Europeu e do Conselho que cria o Sistema Europeu de Informação e Autorização de Viagem (ETIAS)<sup>33</sup>, a unidade central do ETIAS da Agência Europeia da Guarda de Fronteiras e Costeira efetuará pesquisas no SIS, através do ETIAS, a fim de apurar se um nacional de país terceiro que solicite uma autorização de viagem é objeto de uma indicação do SIS. Para o efeito, a unidade central do ETIAS terá igualmente acesso integral ao SIS.

## **Alterações específicas das indicações**

O artigo 26.º dispõe que os Estados-Membros devem suspender temporariamente as indicações para efeitos de detenção (em caso de operação ou investigação policial em curso), tornando-as visíveis apenas aos gabinetes SIRENE, mas não aos agentes no terreno, durante um período limitado. Esta disposição contribui para evitar que uma operação policial confidencial para a detenção de um delinquente fortemente procurado seja prejudicada por um agente da polícia não envolvido no processo.

Os artigos 32.º e 33.º estabelecem disposições aplicáveis às indicações relativas a pessoas desaparecidas. As modificações nesta matéria permitem a emissão de indicações preventivas nos casos em que se considere existir um grande risco de rapto parental, além de ajustarem a categorização das indicações relativas a pessoas desaparecidas. Os raptos parentais ocorrem geralmente em circunstâncias minuciosamente planeadas, com a intenção de abandonar rapidamente o Estado-Membro onde foi fixado o regime de guarda da criança. Estas modificações tratam uma potencial lacuna na legislação em vigor, nos termos da qual as indicações relativas a crianças só podem ser emitidas após o seu desaparecimento. Permitirão às autoridades nos Estados-Membros assinalar as crianças em especial risco. Em virtude destas modificações, nos casos de risco elevado e iminente de rapto parental, os guardas de fronteira e agentes policiais são informados do risco, podendo examinar de forma mais rigorosa as circunstâncias em que uma criança em risco viaja, colocando a criança sob

---

<sup>33</sup> COM(2016) 731 final.

proteção, se tal se afigurar necessário. Serão prestadas, por meio dos Gabinetes SIRENE, informações suplementares, designadamente sobre a decisão da autoridade judiciária competente que solicitou a indicação. O Manual SIRENE será revisto em conformidade com estas disposições. Nestes casos, a indicação exigirá uma decisão correspondente por parte das autoridades judiciárias no sentido de confiar a guarda da criança a apenas um dos progenitores. Outra condição neste cenário prende-se com o risco iminente de rapto. O estado das indicações relativas a crianças desaparecidas será automaticamente atualizado ao atingirem a idade adulta, quando for caso disso.

O artigo 34.º permite que sejam acrescentados à indicação dados sobre veículos se houver indícios claros de que os mesmos estão ligados à pessoa procurada.

O artigo 37.º introduz uma nova forma de verificação, o «controlo de verificação», que visa, em particular, apoiar as medidas de luta contra o terrorismo e os crimes graves. Este tipo de controlo permite que as autoridades intercetem e interroguem a pessoa em causa. É mais aprofundado do que a atual vigilância discreta, mas não envolve uma revista da pessoa nem pode dar lugar à sua detenção. Contudo, poderá gerar informação suficiente para decidir quanto à adoção da conduta adequada. O artigo 36.º também é alterado para refletir este tipo adicional de controlo.

A presente proposta prevê que as indicações do SIS abrangam os documentos oficiais em branco e documentos de identidade emitidos (artigo 36.º), bem como veículos, incluindo embarcações e aeronaves (artigos 32.º, 34.º), sempre que estejam ligados a indicações relativas a pessoas emitidas por força destes artigos. O artigo 37.º é alterado a fim de prever a conduta a adotar com base nestas indicações. O objetivo é meramente de investigação, uma vez que permitirá às autoridades resolver os casos em que várias pessoas utilizam documentos autênticos, embora similares, dos quais não são os legítimos titulares.

O artigo 38.º alarga a lista de objetos para os quais podem ser emitidas indicações, acrescentando os documentos falsificados, os veículos, independentemente do seu sistema de propulsão (ou seja, elétricos ou a gasolina/gasóleo, etc.), as notas de banco falsificadas, os equipamentos informáticos, bem como os componentes identificáveis de veículos e equipamento industrial. Não prevê indicações adicionais relativas aos meios de pagamento, pois a eficácia destas indicações demonstrou ser muito reduzida, não tendo praticamente devolvido acertos.

A fim de clarificar o procedimento a seguir quando é encontrado um objeto indicado, o artigo 39.º alterado determina que os objetos devem ser apreendidos, nos termos do direito nacional, e que deve ser contactada a autoridade que emitiu a indicação.

### **Proteção e segurança dos dados**

A presente proposta especifica as responsabilidades pela prevenção, prestação de informações e resposta a incidentes suscetíveis de afetar a segurança ou a integridade da infraestrutura do SIS, dos dados do SIS ou das informações suplementares (artigos 10.º, 16.º e 57.º).

O artigo 12.º prevê disposições relativas à conservação e à consulta de registos do historial das indicações.

O artigo 12.º inclui igualmente disposições relativas às consultas de varrimento automatizadas das chapas de matrícula de veículos a motor, por meio de sistemas de reconhecimento automático de matrículas, obrigando os Estados-Membros a manter um registo destas pesquisas, em conformidade com a legislação nacional.

O artigo 15.º, n.º 3, mantém o disposto no artigo 15.º, n.º 3, da Decisão 2007/533/JAI do Conselho, assim como a responsabilidade da Comissão pela gestão contratual da

infraestrutura de comunicação, designadamente as atribuições relativas à execução do orçamento e à aquisição e renovação. Estas atribuições serão transferidas para a eu-LISA no âmbito do segundo pacote de propostas respeitantes ao SIS, em junho de 2017.

O artigo 21.º alarga o requisito de verificar se um caso é suficientemente adequado, pertinente e relevante para lhe ser aplicável uma decisão sobre a eventual prorrogação do período de validade de uma indicação. Este artigo impõe igualmente aos Estados-Membros a obrigação nova de criar, em todas as circunstâncias, uma indicação, por força dos artigos 34.º, 36.º e 38.º (consoante o caso), para as pessoas, ou os objetos ligados a estas pessoas, cujos atos sejam abrangidos pelos artigos 1.º, 2.º, 3.º e 4.º da Decisão-Quadro 2002/475/JAI do Conselho relativa à luta contra o terrorismo.

#### Categorias de dados e tratamento de dados

A presente proposta alarga os tipos de informação (artigo 20.º) que podem ser conservados sobre as pessoas indicadas, que passam a incluir também:

- a eventual participação da pessoa em qualquer ato abrangido pelos artigos 1.º, 2.º, 3.º e 4.º da Decisão-Quadro 2002/475/JAI do Conselho;
- outras observações relacionadas com a pessoa; o motivo da indicação;
- informações respeitantes ao número de registo nacional e local de registo da pessoa;
- a categorização do tipo de caso de pessoa desaparecida (somente para as indicações nos termos do artigo 32.º);
- informações inscritas no documento de identidade ou de viagem da pessoa;
- uma cópia a cores do documento de identidade ou de viagem da pessoa;
- perfis de ADN (apenas no caso de não estarem disponíveis impressões digitais adequadas para a identificação).

O artigo 59.º alarga a lista dos dados pessoais que podem ser inseridos e tratados no SIS para evitar usurpações de identidade. Estes dados apenas podem ser introduzidos com o consentimento da vítima de usurpação de identidade. Assim, passam igualmente a ser incluídos os seguintes dados:

- imagens faciais;
- impressões palmares;
- dados dos documentos de identidade;
- o endereço da vítima;
- os nomes dos progenitores da vítima.

O artigo 20.º prevê a inclusão de informações mais pormenorizadas nas indicações. Inclui dados dos documentos de identidade pessoais dos titulares dos dados, e possibilita uma categorização das crianças desaparecidas consoante as circunstâncias do desaparecimento, por exemplo, menores não acompanhados, vítimas de rapto parental, jovens que fugiram de casa, etc. Esta categorização é essencial para que os utilizadores finais adotem sem demora as medidas necessárias à proteção destas crianças. O reforço da abrangência das informações permite melhorar, por um lado, a identificação da pessoa em causa e, por outro, os fundamentos para a decisão a tomar pelos utilizadores finais. Para fins de proteção dos utilizadores finais que efetuam as verificações, o SIS informará igualmente se a pessoa

indicada se insere nas categorias definidas nos artigos 1.º, 2.º, 3.º e 4.º da Decisão-Quadro 2002/475/JAI do Conselho relativa à luta contra o terrorismo<sup>34</sup>.

A proposta estabelece claramente que os Estados-Membros não podem copiar dados inseridos por outro Estado-Membro para os ficheiros de dados nacionais (artigo 53.º).

### Conservação

O período máximo de conservação das indicações relativas a pessoas será aumentado para cinco anos, exceto no caso das indicações para efeitos de vigilância discreta, controlo de verificação ou controlo específico, que manterão um período de conservação de um ano. Os Estados-Membros têm sempre a possibilidade de fixar períodos mais curtos. A prorrogação do prazo máximo segue as práticas nacionais quando uma indicação ainda não cumpriu a sua finalidade devido ao facto de a pessoa em causa continuar a ser procurada. Além disso, era necessário alinhar o SIS pelo período de conservação previsto ao abrigo de outros instrumentos, nomeadamente a Diretiva Regresso e o Eurodac. Por razões de transparência e clareza, é necessário estabelecer o mesmo período de conservação para as indicações relativas a pessoas, com exceção das indicações criadas para efeitos de vigilância discreta, controlo de verificação ou controlo específico. A prorrogação do período de conservação não prejudica os interesses dos titulares dos dados, uma vez que não é possível manter uma indicação por um período mais longo do que o necessário para a sua finalidade. As regras de supressão das indicações são explicitamente descritas no artigo 52.º. O artigo 51.º fixa o calendário relativo à revisão das indicações e, mais particularmente, inclui o período de conservação mais curto para as indicações relativas a objetos. Não sendo necessário, no plano operacional, manter o prazo mais longo relativamente aos objetos, este foi reduzido para cinco anos, a fim de o uniformizar com o período de conservação das indicações relativas a pessoas. Porém, o prazo aplicável aos documentos emitidos e em branco continua a ser de 10 anos, uma vez que o período de validade dos documentos é de 10 anos.

### Supressão

O artigo 52.º descreve as circunstâncias em que as indicações têm de ser suprimidas, proporcionando uma maior harmonização com as práticas nacionais neste domínio. O artigo 51.º estabelece disposições especiais ao abrigo das quais o pessoal dos Gabinetes SIRENE deve suprimir proativamente as indicações que deixem de ser necessárias caso não seja obtida nenhuma resposta da parte das autoridades competentes.

### Direitos dos titulares dos dados em matéria de acesso aos dados, retificação de dados incorretos e apagamento de dados ilegalmente introduzidos

As normas pormenorizadas respeitantes aos direitos dos titulares dos dados mantiveram-se inalteradas, uma vez que as normas existentes já garantem um elevado grau de proteção e são consentâneas com o Regulamento (UE) 2016/679<sup>35</sup> e a Diretiva (UE) 2016/680<sup>36</sup>. Além dessas normas, o artigo 63.º descreve as circunstâncias em que os Estados-Membros podem

<sup>34</sup> Decisão-Quadro 2002/475/JAI do Conselho, de 13 de junho de 2002, relativa à luta contra o terrorismo (JO L 164 de 22.6.2002, p. 3).

<sup>35</sup> 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).

<sup>36</sup> 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 (JO L 119 de 4.5.2016, p. 89).

decidir não comunicar informações aos titulares dos dados. Essa decisão deve ser justificada por um dos motivos referidos neste artigo, devendo tratar-se de uma medida proporcionada e necessária, ao abrigo do direito nacional.

Partilha de dados com a Interpol sobre documentos extraviados, roubados, invalidados ou desviados

O artigo 63.º mantém na íntegra o disposto no artigo 55.º da Decisão 2007/533/JAI do Conselho, dado que a interoperabilidade melhorada entre a secção de documentos do SIS e a base de dados de documentos roubados e perdidos da Interpol será um tema abordado na comunicação do Grupo de Peritos de Alto Nível e no segundo conjunto de propostas relativas ao SIS em junho de 2017.

#### Estatísticas

No sentido de manter uma visão geral do funcionamento, na prática, das vias de recurso, o artigo 66.º prevê um sistema estatístico normalizado que fornece relatórios anuais sobre os números relativos a:

- pedidos de acesso dos titulares dos dados;
- pedidos de retificação de dados incorretos e de apagamento de dados ilegalmente introduzidos;
- processos em tribunal;
- processos em que o tribunal decidiu a favor do requerente; e
- observações sobre os casos de reconhecimento mútuo de decisões definitivas proferidas pelos tribunais ou pelas autoridades de outros Estados-Membros relativamente a indicações criadas pelo Estado autor da indicação.

#### Acompanhamento e estatísticas

O artigo 71.º estipula os mecanismos a pôr em prática para assegurar o acompanhamento adequado do SIS e do seu funcionamento comparativamente aos seus objetivos. Para o efeito, compete à eu-LISA facultar estatísticas diárias, mensais e anuais sobre a forma como o sistema está a ser utilizado.

O artigo 71.º, n.º 5, exige que a eu-LISA transmita aos Estados-Membros, à Comissão, à Europol, à Eurojust e à Agência Europeia da Guarda de Fronteiras e Costeira os relatórios estatísticos por si elaborados e permite que a Comissão solicite relatórios adicionais sobre estatísticas e a qualidade dos dados relacionados com o SIS e a comunicação SIRENE.

O artigo 71.º, n.º 6, prevê a criação e gestão de um repositório central de dados, no âmbito do trabalho desenvolvido pela eu-LISA no acompanhamento do funcionamento do SIS. Torna-se, assim, possível ao pessoal autorizado dos Estados-Membros, da Comissão, da Europol, da Eurojust e da Agência Europeia da Guarda de Fronteiras e Costeira aceder aos dados enumerados no artigo 71.º, n.º 3, a fim de elaborar as estatísticas exigidas.

Proposta de

## **REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO**

**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 o Regulamento (UE) n.º 515/2014 e revoga o Regulamento (CE) n.º 1986/2006, a Decisão 2007/533/JAI do Conselho e a Decisão 2010/261/UE da Comissão**

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), o artigo 85.º, n.º 1, o artigo 87.º, n.º 2, alínea a), e o artigo 88.º, n.º 2, alínea a),

Tendo em conta a proposta da Comissão Europeia,

Após transmissão do projeto de ato legislativo aos parlamentos nacionais,

Deliberando de acordo com o processo legislativo ordinário,

Considerando o seguinte:

- (1) O Sistema de Informação de Schengen (SIS) constitui um instrumento essencial para a aplicação das disposições do acervo de Schengen integrado no âmbito da União Europeia. O SIS constitui uma das principais medidas compensatórias que contribui para manter um elevado nível de segurança no espaço de liberdade, segurança e justiça da União Europeia, apoiando a cooperação operacional entre os guardas de fronteira, as autoridades policiais, aduaneiras e outras autoridades com funções coercivas e as autoridades judiciárias em matéria penal.
- (2) O SIS foi criado nos termos do disposto no título IV da Convenção de 19 de junho de 1990 de Aplicação do Acordo de Schengen, de 14 de junho de 1985, entre os Governos dos Estados da União Económica Benelux, da República Federal da Alemanha e da República Francesa, relativo à supressão gradual dos controlos nas fronteiras comuns<sup>37</sup> (Convenção de Schengen). O desenvolvimento da segunda geração do SIS (SIS II) foi confiado à Comissão nos termos do Regulamento (CE) n.º 2424/2001 da Comissão<sup>38</sup> e da Decisão 2001/886/JAI do Conselho<sup>39</sup>, tendo sido

---

<sup>37</sup> JO L 239 de 22.9.2000, p. 19. Convenção alterada pelo Regulamento (CE) n.º 1160/2005 do Parlamento Europeu e do Conselho (JO L 191 de 22.7.2005, p. 18).

<sup>38</sup> JO L 328 de 13.12.2001, p. 4.

<sup>39</sup> Decisão 2001/886/JAI do Conselho, de 6 de dezembro de 2001, relativa ao desenvolvimento da segunda geração do Sistema de Informação de Schengen (SIS II) (JO L 328 de 13.12.2001, p. 1).



estabelecido pelo Regulamento (CE) n.º 1987/2006<sup>40</sup>, bem como pela Decisão 2007/533/JAI do Conselho<sup>41</sup>. O SIS II substituiu o SIS tal como criado pela Convenção de Schengen.

- (3) Três anos após a entrada em funcionamento do SIS II, a Comissão procedeu à sua avaliação em conformidade com o artigo 24.º, n.º 5, o artigo 43.º, n.º 5, e o artigo 50.º, n.º 5, do Regulamento (CE) n.º 1987/2006, e com o artigo 59.º e o artigo 65.º, n.º 5, da Decisão 2007/533/JAI. O relatório de avaliação, bem como o documento de trabalho correspondente dos serviços da Comissão, foram adotados em 21 de dezembro de 2016<sup>42</sup>. As recomendações formuladas nesses documentos refletem-se, na medida do necessário, no presente regulamento.
- (4) O presente regulamento constitui a base legislativa necessária para regulamentar o SIS no respeitante às matérias que se inscrevem no âmbito do título V, capítulos 4 e 5, do Tratado sobre o Funcionamento da União Europeia. O Regulamento (UE) 2018/... do Parlamento Europeu e do Conselho relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação Schengen no domínio dos controlos das fronteiras<sup>43</sup>, constitui a base legislativa necessária para regulamentar o SIS no que respeita às matérias que se inscrevem no âmbito do título V, capítulo 2, do Tratado sobre o Funcionamento da União Europeia.
- (5) O facto de a base legislativa necessária para regulamentar o SIS consistir em dois instrumentos distintos não afeta o princípio de que o SIS constitui um sistema de informação único e que deverá funcionar como tal. Certas disposições destes instrumentos devem, por esse motivo, ser idênticas.
- (6) É necessário especificar os objetivos do SIS, a sua arquitetura técnica e o seu financiamento, e estabelecer as normas aplicáveis ao seu funcionamento e à sua utilização de extremo a extremo, bem como definir as responsabilidades, as categorias de dados a introduzir no sistema, as finalidades e os critérios que presidem à respetiva introdução, as autoridades autorizadas a aceder aos dados, a utilização de identificadores biométricos e normas complementares relativas ao tratamento dos dados.
- (7) O SIS inclui um sistema central (SIS Central) e sistemas nacionais dotados de uma cópia integral ou parcial da base de dados do SIS. Considerando que o SIS é o mais importante instrumento de intercâmbio de informações na Europa, é necessário assegurar a continuidade do seu funcionamento tanto a nível central como nacional. Por conseguinte, cada Estado-Membro deve estabelecer uma cópia integral ou parcial da base de dados do SIS e criar o seu sistema de salvaguarda.
- (8) É necessário manter um manual com normas pormenorizadas aplicáveis ao intercâmbio de determinadas informações suplementares relativas à conduta a adotar

---

<sup>40</sup> Regulamento (CE) n.º 1987/2006 do Parlamento Europeu e do Conselho, de 20 de dezembro de 2006, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen de segunda geração (SIS II) (JO L 381 de 28.12.2006, p. 4).

<sup>41</sup> 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).

<sup>42</sup> Relatório ao Parlamento Europeu e ao Conselho sobre a avaliação do Sistema de Informação de Schengen de segunda geração (SIS II) em conformidade com o artigo 24.º, n.º 5, o artigo 43.º, n.º 5 e o artigo 50.º, n.º 5, do Regulamento (CE) n.º 1987/2006, e com o artigo 59.º, n.º 3, e o artigo 65.º, n.º 5, da Decisão 2007/533/JAI e o documento de trabalho correspondente dos serviços da Comissão (JO...).

<sup>43</sup> Regulamento (UE) n.º 2018/...

para reagir às indicações. As autoridades nacionais em cada Estado-Membro (Gabinetes SIRENE) devem assegurar o intercâmbio dessas informações.

- (9) A fim de manter a eficácia do intercâmbio de informações suplementares sobre a conduta a adotar especificada nas indicações, é conveniente reforçar o funcionamento dos Gabinetes SIRENE, indicando os requisitos respeitantes aos recursos disponíveis, à formação dos utilizadores e ao tempo de resposta a consultas recebidas de outros Gabinetes SIRENE.
- (10) A gestão operacional das componentes centrais do SIS é exercida pela Agência Europeia para a gestão operacional de sistemas informáticos de grande escala no espaço de liberdade, segurança e justiça<sup>44</sup> («Agência»). A fim de permitir à Agência consagrar os recursos financeiros e humanos necessários para cobrir a totalidade dos aspetos da gestão operacional do SIS Central, o presente regulamento deve estabelecer as suas atribuições em pormenor, principalmente no respeitante aos aspetos técnicos do intercâmbio de informações suplementares.
- (11) Sem prejuízo da responsabilidade dos Estados-Membros em relação à exatidão dos dados introduzidos no SIS, a Agência deve tornar-se responsável pelo reforço da qualidade dos dados através da introdução de uma ferramenta central de monitorização da qualidade dos dados, bem como pela apresentação de relatórios periódicos aos Estados-Membros.
- (12) A fim de permitir um melhor acompanhamento da utilização do SIS para analisar as tendências da criminalidade, a Agência deve ter condições para desenvolver uma ferramenta moderna para comunicar dados estatísticos aos Estados-Membros, à Comissão, à Europol e à Agência Europeia da Guarda de Fronteiras e Costeira sem comprometer a integridade dos dados. Por conseguinte, deve ser criado um repositório central de estatísticas. As estatísticas elaboradas nunca devem conter dados pessoais.
- (13) O SIS deve incluir novas categorias de dados para que os utilizadores finais tomem rapidamente decisões informadas com base numa indicação. Por conseguinte, a fim de facilitar a identificação de pessoas e a deteção de identidades múltiplas, as categorias de dados relativas a uma pessoa devem incluir uma referência ao documento de identidade ou ao número de identidade pessoal e uma cópia desse documento, se disponível.
- (14) O SIS não deve armazenar quaisquer dados utilizados para consultas, excetuando para fins de manutenção dos registos para permitir verificar a legalidade da consulta e a legalidade do tratamento de dados, proceder ao autocontrolo e assegurar o correto funcionamento do N.SIS, bem como a integridade e a segurança dos dados.
- (15) O SIS deve permitir o tratamento de dados biométricos, a fim de contribuir para a identificação fiável das pessoas em causa. Na mesma perspetiva, o SIS deve permitir igualmente o tratamento de dados sobre pessoas cuja identidade tenha sido usurpada (para evitar os inconvenientes causados por erros de identificação), sob reserva das garantias adequadas, nomeadamente o consentimento das pessoas em causa e uma limitação estrita das finalidades para as quais esses dados podem ser legalmente tratados.

---

<sup>44</sup> Estabelecida pelo Regulamento (UE) n.º 1077/2011 do Parlamento Europeu e do Conselho, de 25 de outubro de 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 286 de 1.11.2011, p. 1).

- (16) Os Estados-Membros devem tomar as medidas técnicas necessárias para que cada vez que os utilizadores finais são autorizados a consultar uma base de dados nacional dos serviços policiais ou de imigração possam igualmente consultar o SIS em paralelo, em conformidade com o artigo 4.º da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho<sup>45</sup>. Tal deve assegurar que o SIS funciona como a principal medida de compensação no espaço sem controlos das fronteiras internas e trata com maior eficácia a dimensão transnacional da criminalidade e a mobilidade dos criminosos.
- (17) O presente regulamento deve estabelecer as condições respeitantes à utilização de dados dactilográficos e imagens faciais para efeitos de identificação. A utilização de imagens faciais para efeitos de identificação no SIS contribui também para garantir a coerência dos procedimentos de controlo nas fronteiras quando se exige a identificação e a verificação da identidade através da utilização de impressões digitais e imagens faciais. É conveniente que a consulta de dados dactilográficos seja obrigatória em caso de dúvida sobre a identidade de uma pessoa. A imagem facial para efeitos de identificação só deve ser utilizada no contexto de controlos regulares nas fronteiras em terminais de *self-service* e cancelas eletrónicas.
- (18) A introdução de um serviço automatizado de identificação por impressões digitais no SIS completa o atual mecanismo de Prüm sobre o acesso transfronteiras em linha a determinadas bases de dados nacionais de perfis de ADN e sistemas nacionais automatizados de identificação por impressões digitais<sup>46</sup>. O mecanismo de Prüm permite a interconexão dos sistemas nacionais automatizados de identificação por impressões digitais através do qual um Estado-Membro pode lançar um pedido para verificar se o autor de um crime, cujas impressões digitais foram detetadas, é conhecido noutro Estado-Membro. Contudo, este mecanismo verifica apenas se o titular das impressões digitais é conhecido num determinado momento, de modo que se o infrator só mais tarde for detetado em algum dos outros Estados-Membro poderá não ser capturado. A pesquisa de impressões digitais no SIS permite uma procura ativa do autor de um crime. Deve ser possível, portanto, carregar no SIS as impressões digitais de um infrator desconhecido, desde que o seu titular possa ser identificado com elevado grau de probabilidade como o autor de um crime grave ou de um ato de terrorismo. Tal é nomeadamente o caso se as impressões digitais forem detetadas na arma ou em qualquer objeto utilizado para a prática do crime. A mera presença de impressões digitais na cena do crime não deve ser considerada, porém, como indicando com elevado grau de probabilidade que as impressões digitais pertencem ao autor do crime. Outra condição prévia para a criação de tal indicação deve ser a impossibilidade de estabelecer a identidade do infrator através de qualquer outra base de dados nacional, europeia ou internacional. Se a consulta das impressões digitais resultar numa correspondência potencial, o Estado-Membro deve proceder a

---

<sup>45</sup> 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, (JO L 119 de 4.5.2016, p. 89).

<sup>46</sup> Decisão 2008/615/JAI do Conselho, de 23 de junho de 2008, relativa ao aprofundamento da cooperação transfronteiras, em particular no domínio da luta contra o terrorismo e a criminalidade transfronteiras (JO L 210 de 6.8.2008, p. 1); e Decisão 2008/616/JAI do Conselho, de 23 de junho de 2008, referente à execução da Decisão 2008/615/JAI, relativa ao aprofundamento da cooperação transfronteiras, em particular no domínio da luta contra o terrorismo e da criminalidade transfronteiras (JO L 210 de 6.8.2008, p. 12).

verificações complementares, eventualmente com a ajuda de peritos na matéria, para determinar se as impressões digitais armazenadas no SIS pertencem à pessoa em causa, devendo estabelecer a identidade desta última. Os procedimentos devem ser regidos pelo direito nacional. O facto de se identificar uma «pessoa desconhecida procurada» no SIS pode contribuir substancialmente para fazer progredir a investigação e conduzir à detenção, desde que todas as condições para esta última estejam preenchidas.

- (19) As impressões digitais encontradas no local de um crime devem poder ser comparadas com as impressões digitais armazenadas no SIS, caso se possa determinar com um elevado grau de probabilidade que pertencem ao autor de um crime grave ou de um crime de terrorismo. Um «crime grave» corresponde às infrações penais enunciadas na Decisão-Quadro 2002/584/JAI do Conselho<sup>47</sup>, e o «crime de terrorismo» corresponde às infrações penais tal como definidas no direito nacional a que se refere a Decisão-Quadro 2002/475/JAI do Conselho<sup>48</sup>.
- (20) Deve ser permitido acrescentar um perfil de ADN nos casos em que não existam dados dactilográficos, o qual só será acessível aos utilizadores autorizados. Os perfis de ADN podem facilitar a identificação de pessoas desaparecidas que necessitam de proteção e, em especial, crianças desaparecidas, nomeadamente se for autorizada a utilização de perfis de ADN dos pais ou irmãos para permitir a identificação. Os dados de ADN não devem fazer menção à origem racial.
- (21) O SIS deve conter indicações relativas a pessoas procuradas para detenção para efeitos de entrega e procuradas para detenção para efeitos de extradição. Além das indicações, convém prever o intercâmbio de informações suplementares, necessário para os processos de entrega e de extradição. Devem ser tratados no SIS, em especial, os dados referidos no artigo 8.º da 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<sup>49</sup>. Por razões operacionais, é conveniente que o Estado-Membro autor da indicação, com autorização das autoridades judiciais, torne temporariamente indisponível a consulta de uma indicação existente para efeitos de detenção quando a pessoa objeto do mandado de detenção europeu for ativamente procurada e os utilizadores finais não envolvidos nas operações de busca possam prejudicar o êxito dessa diligência. A indisponibilidade temporária dessas indicações não deve exceder 48 horas.
- (22) É conveniente prever a possibilidade de aditar ao SIS uma tradução dos dados suplementares introduzidos para efeitos de entrega, ao abrigo do mandado de detenção europeu, e de extradição.
- (23) O SIS deve conter indicações relativas a pessoas desaparecidas para assegurar a sua proteção ou prevenir ameaças contra a segurança pública. A possibilidade de inserir uma indicação no SIS relativa a crianças que correm risco de rapto (ou seja, para prevenir um futuro dano que ainda não ocorreu, como é o caso do risco de rapto parental) deve ser limitada, pelo que é conveniente prever garantias rigorosas e

---

<sup>47</sup> 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).

<sup>48</sup> Decisão-Quadro 2002/475/JAI do Conselho, de 13 de junho de 2002, relativa à luta contra o terrorismo (JO L 164 de 22.6.2002, p. 3).

<sup>49</sup> 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).

adequadas. No caso de crianças, essas indicações e os procedimentos correspondentes devem servir o seu interesse superior, tendo em conta o artigo 24.º da Carta dos Direitos Fundamentais da União Europeia e a Convenção das Nações Unidas sobre os Direitos da Criança de 20 de novembro de 1989.

- (24) Deve ser prevista uma nova conduta a adotar nos casos de suspeita de terrorismo e de crime grave que permita intercepar e interrogar a pessoa suspeita de ter cometido um crime grave ou quando houver motivos para considerar que irá cometer tal crime, a fim de comunicar informações o mais pormenorizadas possível ao Estado-Membro autor da indicação. Esta nova conduta a adotar não deve implicar a revista ou a detenção da pessoa em causa, devendo, no entanto, permitir obter informações suficientes para decidir das medidas a tomar. Os crimes graves devem corresponder às infrações penais enunciadas na Decisão-Quadro 2002/584/JAI do Conselho.
- (25) O SIS deve conter novas categorias de objetos de valor elevado, como os equipamentos eletrónicos e técnicos, que podem ser identificados e consultados com um número único.
- (26) É conveniente prever a possibilidade de um Estado-Membro aditar uma menção a uma indicação, conhecida por «referência», a fim de que a conduta a adotar com base na indicação não seja executada no seu território. Quando são inseridas indicações para detenção para efeitos de entrega, nada no presente regulamento deve ser interpretado de forma a derrogar ou impedir a aplicação do disposto na Decisão-Quadro 2002/584/JAI. A decisão de aposição de uma referência numa indicação deverá basear-se exclusivamente nos motivos de não admissão previstos nessa decisão-quadro.
- (27) Quando é aposta uma referência e se torna conhecido o paradeiro da pessoa procurada para detenção para efeitos de entrega, esse paradeiro deve ser sempre comunicado à autoridade judicial de emissão, que pode decidir transmitir um mandado de detenção europeu à autoridade judicial competente, em conformidade com o disposto na Decisão-Quadro 2002/584/JAI.
- (28) Os Estados-Membros devem poder estabelecer ligações entre indicações constantes do SIS. O estabelecimento de ligações por um Estado-Membro entre duas ou mais indicações não deve ter efeitos a nível da conduta a adotar, do período de conservação ou dos direitos de acesso às indicações.
- (29) As indicações não devem ser conservadas no SIS por mais tempo do que o necessário à realização das finalidades para as quais foram inseridas. A fim de reduzir a carga administrativa que recai sobre as diferentes autoridades que intervêm no tratamento de dados das pessoas singulares para diversas finalidades, é conveniente alinhar os prazos de conservação das indicações relativas a pessoas com os prazos de conservação previstos para efeitos de regresso e de permanência irregular. Além disso, os Estados-Membros devem prorrogar regularmente a data de validade de indicações relativas a pessoas se a conduta a adotar não puder ser executada dentro do prazo inicial. Por conseguinte, o prazo máximo de conservação das indicações relativas a pessoas deve ser de cinco anos. Como princípio geral, as indicações relativas a pessoas devem ser automaticamente suprimidas do SIS após cinco anos, exceto aquelas inseridas para efeitos de vigilância discreta, de controlo específico e de controlo de verificação. Tais indicações devem ser suprimidas após um ano. As indicações relativas a objetos inseridas para efeitos de vigilância discreta, de controlo de verificação ou de controlo específico devem ser automaticamente suprimidas do SIS após um ano, uma vez que estão sempre ligadas a pessoas. As indicações relativas a objetos, para efeitos de

apreensão ou de utilização como prova em processos penais, devem ser automaticamente suprimidas do SIS após cinco anos, uma vez que no termo deste prazo a probabilidade de os encontrar é muito reduzida e o seu valor económico diminui consideravelmente. As indicações relativas a documentos de identidade emitidos ou em branco devem ser conservadas durante 10 anos, uma vez que o período de validade dos documentos é de 10 anos no momento da emissão. As decisões de manter as indicações relativas a pessoas devem ser baseadas numa avaliação individual circunstanciada. Os Estados-Membros devem proceder à apreciação das indicações relativas a pessoas no prazo definido e manter estatísticas sobre o número de indicações relativas a pessoas cujo prazo de conservação foi prorrogado.

- (30) A inserção e a prorrogação do prazo de validade de indicações no SIS devem ser sujeitas ao necessário requisito da proporcionalidade, examinando se o caso concreto é adequado, pertinente e suficientemente importante para merecer a inserção da indicação no SIS. As infrações enunciadas nos artigos 1.º, 2.º, 3.º e 4.º da Decisão-Quadro 2002/475/JAI do Conselho relativa à luta contra o terrorismo<sup>50</sup>, constituem ameaças graves contra a segurança pública e integridade das pessoas e contra a sociedade, sendo extremamente difícil a sua prevenção, deteção e investigação num espaço sem controlos nas fronteiras internas no qual os potenciais criminosos circulam livremente. Se uma pessoa ou objeto for procurado em relação a esses crimes, é sempre necessário criar a indicação correspondente no SIS sobre pessoas procuradas para efeitos de um processo judicial penal, sobre pessoas ou objetos sujeitos a vigilância discreta, a controlo de verificação e a controlo específico, bem como sobre objetos para efeitos de apreensão, pois nenhum outro meio será tão eficaz para essa finalidade.
- (31) É necessário assegurar a clareza no que diz respeito à supressão das indicações. A indicação só deve ser conservada no SIS pelo período de tempo necessário à realização da finalidade para a qual foi inserida. Tendo em conta as práticas divergentes dos Estados-Membros no que respeita à definição do momento em que a indicação atingiu o seu objetivo, é conveniente estabelecer critérios pormenorizados para cada categoria de indicação, a fim de determinar o momento em que deve ser suprimida do SIS.
- (32) A integridade dos dados do SIS tem uma importância crucial. Por conseguinte, devem ser previstas as garantias adequadas para o tratamento de dados no SIS a nível central e nacional, a fim de assegurar a segurança dos dados de extremo a extremo. As autoridades envolvidas no tratamento de dados devem cumprir os requisitos de segurança do presente regulamento e respeitar um procedimento uniforme de comunicação de incidentes.
- (33) Os dados tratados no SIS por força do presente regulamento não devem ser transferidos para países terceiros ou organizações internacionais nem colocados à sua disposição. No entanto, é conveniente reforçar a cooperação entre a União Europeia e a Interpol, promovendo um intercâmbio eficaz de dados dos passaportes. Sempre que sejam transferidos dados pessoais do SIS para a Interpol, esses dados devem ser objeto de um nível adequado de proteção, garantido por acordo que preveja garantias e condições estritas.
- (34) Deve ser concedido acesso ao SIS às autoridades responsáveis pelo registo de veículos, embarcações e aeronaves, a fim de lhes permitir verificar se o meio de

---

<sup>50</sup> Decisão-Quadro 2002/475/JAI do Conselho, de 13 de junho de 2002, relativa à luta contra o terrorismo (JO L 164 de 22.6.2002, p. 3).

transporte em causa já é procurado noutro Estado-Membro para efeitos de apreensão ou controlo. Deve ser previsto o acesso direto às autoridades que são serviços públicos. Este acesso deve limitar-se a indicações respeitantes aos meios de transporte em causa e respetivos documentos de registo ou número de matrícula. Por conseguinte, as disposições do Regulamento (CE) n.º 1986/2006 do Parlamento Europeu e do Conselho<sup>51</sup> devem ser incluídas no presente regulamento e o referido regulamento deve ser revogado.

- (35) No que diz respeito ao tratamento de dados pelas autoridades nacionais competentes para efeitos de prevenção, investigação, deteção de crimes graves ou crimes de terrorismo, ou repressão de infrações penais e execução de sanções penais, incluindo a prevenção de ameaças contra a segurança pública, aplicam-se as disposições nacionais de transposição da Diretiva (UE) 2016/680. As disposições do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho<sup>52</sup> e da Diretiva (UE) 2016/680 devem ser aprofundadas no presente regulamento, sempre que necessário.
- (36) O Regulamento (UE) 2016/679 deve aplicar-se ao tratamento de dados pessoais, por força do presente regulamento, pelas autoridades nacionais quando não se aplica a Diretiva (UE) 2016/680. O Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho<sup>53</sup> deve aplicar-se ao tratamento de dados pessoais pelas instituições e organismos da União no exercício das responsabilidades que lhes incumbem por força do presente regulamento.
- (37) As disposições da Diretiva (UE) 2016/680, do Regulamento (UE) 2016/679 e do Regulamento (CE) n.º 45/2001 devem ser aprofundadas no presente regulamento, sempre que necessário. No que diz respeito ao tratamento dos dados pessoais pela Europol, aplica-se o Regulamento (UE) 2016/794 que cria a Agência da União Europeia para a Cooperação Policial<sup>54</sup> (Regulamento Europol).
- (38) As disposições em matéria de proteção de dados da Decisão 2002/187/JAI, de 28 de fevereiro de 2002<sup>55</sup>, relativa à criação da Eurojust a fim de reforçar a luta contra as formas graves de criminalidade, aplicam-se ao tratamento de dados do SIS pela Eurojust, incluindo as disposições relativas aos poderes da instância comum de controlo, criada pela referida decisão, no que respeita à supervisão das atividades da Eurojust e à sua responsabilidade decorrente do tratamento ilegal de dados pessoais. Atualmente, quando as consultas realizadas pela Eurojust no SIS revelam a existência de indicações emitidas por um Estado-Membro, a Eurojust não pode adotar a conduta

---

<sup>51</sup> Regulamento (CE) n.º 1986/2006 do Parlamento Europeu e do Conselho, de 20 de dezembro de 2006, relativo ao acesso ao Sistema de Informação de Schengen de segunda geração (SIS II) dos serviços dos Estados-Membros competentes para a emissão dos certificados de matrícula dos veículos (JO L 381 de 28.12.2006, p. 1).

<sup>52</sup> 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).

<sup>53</sup> 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).

<sup>54</sup> 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 25.5.2016, p. 53).

<sup>55</sup> Decisão 2002/187/JAI do Conselho, de 28 de fevereiro de 2002, relativa à criação da Eurojust a fim de reforçar a luta contra as formas graves de criminalidade (JO L 63 de 6.3.2002, p. 1).

adequada. Deve, portanto, informar o Estado-Membro em causa para que este possa dar seguimento ao caso.

- (39) No que respeita à confidencialidade, as disposições pertinentes do Estatuto dos Funcionários da União Europeia e do Regime Aplicável aos Outros Agentes da União são aplicáveis aos funcionários e outros agentes empregados e a trabalhar em ligação com o SIS.
- (40) Tanto os Estados-Membros como a Agência devem manter planos de segurança para facilitar a aplicação das obrigações de segurança e devem cooperar entre si para tratar as questões de segurança numa perspetiva comum.
- (41) As autoridades nacionais de controlo independentes devem verificar a legalidade do tratamento dos dados pessoais pelos Estados-Membros no quadro do presente regulamento. É oportuno estabelecer os direitos dos titulares dos dados em matéria de acesso, retificação e apagamento dos seus dados pessoais conservados no SIS e as eventuais vias de recurso para os tribunais nacionais, bem como o reconhecimento mútuo das decisões judiciais. É conveniente, portanto, exigir que os Estados-Membros comuniquem estatísticas anuais nesta matéria.
- (42) As autoridades de controlo devem assegurar que é efetuada, no mínimo de quatro em quatro anos, uma auditoria das operações de tratamento de dados no N.SIS de acordo com as normas internacionais de auditoria. Essa auditoria deve ser efetuada pelas próprias autoridades de controlo ou ser por estas encomendada diretamente a um auditor independente em matéria de proteção de dados. O auditor independente fica sob a supervisão e a responsabilidade da ou das autoridades nacionais de controlo, que devem, portanto, ordenar a auditoria propriamente dita e estabelecer com rigor a finalidade, o âmbito e a metodologia da auditoria, bem como a orientação e a supervisão em relação à auditoria e aos seus resultados finais.
- (43) O Regulamento (UE) 2016/794 (Regulamento Europol) estabelece que a Europol apoia e reforça a ação das autoridades competentes dos Estados-Membros e a sua cooperação mútua em matéria de combate ao terrorismo e formas graves de criminalidade, e que apresenta análises e avaliações de ameaças. O alargamento do direito de acesso da Europol às indicações do SIS sobre pessoas desaparecidas deve contribuir para reforçar a sua capacidade de fornecer às autoridades nacionais com funções coercivas apoio operacional e analítico completo em matéria de tráfico de seres humanos e de exploração sexual de crianças, incluindo em linha. A Europol contribuirá, portanto, para uma melhor prevenção desses crimes, para a proteção das vítimas potenciais, bem como para as investigações sobre os autores dos crimes. Este novo direito de acesso da Europol às indicações do SIS sobre pessoas desaparecidas beneficiará igualmente o seu Centro Europeu da Cibercriminalidade, nomeadamente nos casos de turismo sexual e de abuso sexual de crianças através da Internet, em que os infratores alegam muitas vezes ter acesso ou poder ter acesso a crianças que são suscetíveis de ter sido registadas como pessoas desaparecidas. Além disso, dado que o Centro Europeu contra a Introdução Clandestina de Migrantes da Europol desempenha um importante papel estratégico de combate contra a facilitação da migração irregular, deve ter acesso às indicações relativas a pessoas a quem for recusada a entrada e a permanência no território de um Estado-Membro por motivos criminais ou por incumprimento das condições relativas ao visto ou à permanência.
- (44) A fim de colmatar as lacunas no intercâmbio de informações sobre terrorismo, em especial a respeito dos combatentes terroristas estrangeiros cujos movimentos é essencial acompanhar, os Estados-Membros devem partilhar com a Europol



informações sobre atividades ligadas ao terrorismo em paralelo com a inserção de uma indicação no SIS, bem como acertos e informações conexas. Tal permitirá ao Centro Europeu de Luta contra o Terrorismo da Europol verificar se existe alguma informação contextual adicional disponível em bases de dados da Europol e realizar análises de elevada qualidade que contribuam para o desmantelamento de redes terroristas e, se possível, a prevenção de atentados.

- (45) É igualmente necessário estabelecer normas claras aplicáveis à Europol sobre o tratamento e o descarregamento de dados do SIS, a fim de permitir uma utilização mais ampla do SIS, desde que sejam respeitadas as normas de proteção dos dados, tal como previsto no presente regulamento e no Regulamento (UE) 2016/794. Atualmente, quando as consultas realizadas pela Europol no SIS revelam a existência de uma indicação emitida por um Estado-Membro, a Europol não pode adotar a conduta adequada. Deve, portanto, informar o Estado-Membro em causa para que este possa dar seguimento ao caso.
- (46) O Regulamento (UE) 2016/1624 do Parlamento Europeu e do Conselho<sup>56</sup> prevê, para efeitos do presente regulamento, que o Estado-Membro de acolhimento autorize os membros das equipas da Guarda Europeia de Fronteiras e Costeira ou os membros das equipas envolvidas em operações de regresso, destacados pela Agência Europeia de Guarda de Fronteiras e Costeira, a consultarem as bases de dados europeias sempre que seja necessário para a realização dos objetivos operacionais especificados no plano operacional relativo aos controlos e vigilância das fronteiras e aos regressos. Outras agências competentes da União, nomeadamente o Gabinete Europeu de Apoio em matéria de Asilo e a Europol, podem também destacar peritos no quadro de equipas de apoio à gestão da migração que não sejam membros do pessoal das agências da União. O destacamento das equipas da Guarda Europeia de Fronteiras e Costeira, dos membros das equipas envolvidas em operações de regresso e da equipa de apoio à gestão da migração tem por objetivo fornecer um reforço técnico e operacional aos Estados-Membros que o solicitem, especialmente os que enfrentam desafios migratórios desproporcionados. Para cumprirem as missões que lhes são atribuídas, essas diferentes equipas necessitam de ter acesso ao SIS através de uma interface técnica da Agência Europeia de Guarda de Fronteiras e Costeira com ligação ao SIS Central. Quando resulta de uma consulta no SIS realizada pela ou pelas equipas de pessoal que existe uma indicação emitida por um Estado-Membro, os membros da equipa ou o agente não podem adotar a conduta adequada, exceto se autorizados pelo Estado-Membro de acolhimento. Devem, portanto, informar os Estados-Membros em causa para que estes possam dar seguimento ao caso.
- (47) Em conformidade com a proposta da Comissão de regulamento do Parlamento Europeu e do Conselho que cria o Sistema Europeu de Informação e Autorização de Viagem (ETIAS)<sup>57</sup>, a unidade central da Agência Europeia da Guarda de Fronteiras e Costeira procederá a verificações no SIS através do ETIAS tendo em vista avaliar pedidos de autorização de viagem para saber, designadamente, se um nacional de país terceiro que solicita uma autorização de viagem é objeto de uma indicação no SIS.

---

<sup>56</sup> 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).

<sup>57</sup> COM(2016) 731 final.

Para esse efeito, a unidade central do ETIAS a nível da Agência Europeia da Guarda de Fronteiras e Costeira deve ter igualmente acesso ao SIS, na medida necessária ao desempenho da sua missão, ou seja, a todas as categorias de indicações relativas a pessoas e a documentos pessoais de identidade em branco e emitidos.

- (48) Devido à sua natureza técnica, ao nível de pormenor e à necessidade de atualização regular, determinados aspetos do SIS não podem ser regulados exaustivamente pelas disposições do presente regulamento. Entre estes aspetos incluem-se, por exemplo, as regras técnicas para a introdução de dados, a atualização, supressão e consulta de dados, a qualidade dos dados e as regras de consulta relacionadas com identificadores biométricos, as regras de compatibilidade e de prioridade das indicações, a aposição de referências, as ligações entre indicações, a indicação de novas categorias de objetos na categoria de equipamentos técnicos e eletrónicos, a fixação de um prazo máximo de expiração das indicações e o intercâmbio de informações suplementares. Por conseguinte, devem conferir-se competências de execução à Comissão nestas matérias. As regras técnicas para a consulta de indicações devem ter em conta o funcionamento regular das aplicações nacionais.
- (49) Devem ser atribuídas competências de execução à Comissão, a fim de assegurar condições uniformes para a aplicação do presente regulamento. Essas competências devem ser exercidas em conformidade com o Regulamento (UE) n.º 182/2011<sup>58</sup>. A adoção das medidas de execução por força do presente regulamento e do Regulamento (UE) 2018/xxx (controles das fronteiras) deve estar subordinada ao mesmo procedimento.
- (50) A fim de assegurar a transparência, a Agência deve apresentar, de dois em dois anos, um relatório sobre o funcionamento técnico do SIS Central e da infraestrutura de comunicação, incluindo a sua segurança, bem como sobre o intercâmbio de informações suplementares. A Comissão deve proceder a uma avaliação global de quatro em quatro anos.
- (51) Atendendo a que os objetivos do presente regulamento, a saber, o estabelecimento e a regulação de um sistema de informação conjunto e o intercâmbio de informações suplementares não podem ser suficientemente alcançados pelos Estados-Membros e podem, pois, ser mais bem alcançados ao nível da União, a União pode adotar medidas em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do Tratado da União Europeia. Em conformidade com o princípio da proporcionalidade, consagrado no mesmo artigo, o presente regulamento não excede o necessário para alcançar esses objetivos.
- (52) O presente regulamento respeita os direitos fundamentais e observa os princípios reconhecidos, nomeadamente, na Carta dos Direitos Fundamentais da União Europeia. Em particular, o presente regulamento visa garantir um ambiente seguro para todas as pessoas que residam no território da União Europeia e uma proteção especial das crianças que correm o risco de ser vítimas do tráfico de seres humanos ou de rapto parental, respeitando plenamente a proteção de dados pessoais.
- (53) Nos termos dos artigos 1.º e 2.º do Protocolo n.º 22 relativo à posição da Dinamarca, anexo ao Tratado da União Europeia e ao Tratado sobre o Funcionamento da União

---

<sup>58</sup> 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).

Europeia, a Dinamarca não participa na adoção do presente regulamento, não ficando por ele vinculada nem sujeita à sua aplicação. Uma vez que o presente regulamento desenvolve o acervo de Schengen, a Dinamarca deve decidir, nos termos do artigo 4.º do Protocolo acima referido e no prazo de seis meses a contar da decisão do Conselho relativa ao presente regulamento, se procede à sua transposição para o direito interno.

- (54) O Reino Unido participa no presente regulamento, nos termos do artigo 5.º do Protocolo que integra o acervo de Schengen no âmbito da União Europeia, anexo ao Tratado da União Europeia e ao Tratado sobre o Funcionamento da União Europeia, e do artigo 8.º, n.º 2, da Decisão 2000/365/CE do Conselho, de 29 de maio de 2000, sobre o pedido do Reino Unido da Grã-Bretanha e Irlanda do Norte para participar em algumas das disposições do acervo de Schengen<sup>59</sup>.
- (55) A Irlanda participa no presente regulamento, nos termos do artigo 5.º do Protocolo que integra o acervo de Schengen no âmbito da União Europeia, anexo ao Tratado da União Europeia e ao Tratado sobre o Funcionamento da União Europeia, e do artigo 6.º, n.º 2, da 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<sup>60</sup>.
- (56) 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 Estados à execução, à aplicação e ao desenvolvimento do acervo de Schengen<sup>61</sup>, que se inserem no domínio a que se refere o artigo 1.º, ponto G, da Decisão 1999/437/CE do Conselho<sup>62</sup>, relativo a determinadas regras de aplicação desse acordo.
- (57) Em relação à Suíça, o presente regulamento constitui 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, que se inserem no domínio a que se refere o artigo 1.º, ponto G, da Decisão 1999/437/CE, conjugado com o artigo 4.º, n.º 1, das Decisões 2004/849/CE<sup>63</sup> e 2004/860/CE<sup>64</sup>.
- (58) Em relação ao Liechtenstein, o presente regulamento constitui um desenvolvimento das disposições do acervo de Schengen, na aceção do Protocolo entre a União Europeia, a Comunidade Europeia, a Confederação Suíça e o Principado do Liechtenstein relativo à adesão do Principado do Liechtenstein ao Acordo entre a União Europeia, a Comunidade Europeia e a Confederação Suíça relativo à associação da Confederação Suíça à execução, à aplicação e ao desenvolvimento do acervo de

---

<sup>59</sup> JO L 131 de 1.6.2000, p. 43.

<sup>60</sup> JO L 64 de 7.3.2002, p. 20.

<sup>61</sup> JO L 176 de 10.7.1999, p. 36.

<sup>62</sup> JO L 176 de 10.7.1999, p. 31.

<sup>63</sup> Decisão 2004/849/CE do Conselho, de 25 de Outubro de 2004, respeitante à assinatura, em nome da União Europeia, e à aplicação provisória de certas disposições 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 368 de 15.12.2004, p. 26).

<sup>64</sup> Decisão 2004/860/CE do Conselho, de 25 de Outubro de 2004, respeitante à assinatura, em nome da Comunidade Europeia, e à aplicação provisória de certas disposições 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 370 de 17.12.2004, p. 78).

Schengen<sup>65</sup>, que se inserem no domínio a que se refere no artigo 1.º, ponto G, da Decisão 1999/437/CE, em conjugação com o artigo 3.º da Decisão 2011/350/UE do Conselho<sup>66</sup> e o artigo 3.º da Decisão 2011/350/UE do Conselho<sup>67</sup>.

- (59) Em relação à Bulgária e à Roménia, o presente regulamento constitui um ato baseado no acervo de Schengen ou de algum modo com ele relacionado, na aceção do artigo 4.º, n.º 2, do Ato de Adesão de 2005, e deve ser lido em conjugação com a Decisão 2010/365/UE do Conselho relativa à aplicação das disposições do acervo de Schengen respeitantes ao Sistema de Informação Schengen na República da Bulgária e na Roménia<sup>68</sup>.
- (60) Em relação a Chipre e à Croácia, o presente regulamento constitui um ato baseado no acervo de Schengen ou de algum modo com ele relacionado, na aceção, respetivamente, do artigo 3.º, n.º 2, do Ato de Adesão de 2003 e do artigo 4.º, n.º 2, do Ato de Adesão de 2011.
- (61) O presente regulamento deve aplicar-se à Irlanda em datas fixadas segundo os procedimentos estabelecidos nos instrumentos pertinentes relativos à aplicação do acervo de Schengen a esse Estado.
- (62) Os custos estimados da atualização dos sistemas nacionais do SIS e da aplicação das novas funcionalidades, previstas no presente regulamento, são inferiores ao montante remanescente da rubrica orçamental para as fronteiras inteligentes referido no Regulamento (UE) n.º 515/2014 do Parlamento Europeu e do Conselho<sup>69</sup>. Por conseguinte, o presente regulamento deve reafetar o montante atribuído para o desenvolvimento dos sistemas informáticos de apoio à gestão dos fluxos migratórios nas fronteiras externas, em conformidade com o artigo 5.º, n.º 5, alínea b), do Regulamento (UE) n.º 515/2014.
- (63) A Decisão 2007/533/JAI do Conselho e a Decisão 2010/261/UE da Comissão<sup>70</sup> devem, portanto, ser revogadas.
- (64) A Autoridade Europeia para a Proteção de Dados foi consultada nos termos do artigo 28.º, n.º 2, do Regulamento (CE) n.º 45/2001 e emitiu parecer em ...,

---

<sup>65</sup> JO L 160 de 18.6.2011, p. 21.

<sup>66</sup> Decisão 2011/349/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 Liechtenstein relativo à adesão do Principado do Liechtenstein ao Acordo entre a União Europeia, a Comunidade Europeia e a Confederação Suíça relativo à associação da Confederação Suíça à execução, à aplicação e ao desenvolvimento do acervo de Schengen, no que respeita em especial à cooperação judiciária em matéria penal e à cooperação policial (JO L 160 de 18.6.2011, p. 1).

<sup>67</sup> 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 Liechtenstein relativo à adesão do Principado do Liechtenstein ao Acordo entre a União Europeia, a Comunidade Europeia e a Confederação Suíça relativo à associação da Confederação Suíça à execução, à aplicação e ao desenvolvimento do acervo de Schengen, no que respeita à supressão dos controlos das fronteiras internas e à circulação das pessoas (JO L 160 de 18.6.2011, p. 19).

<sup>68</sup> JO L 166 de 1.7.2010, p. 17.

<sup>69</sup> 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 (JO L 150 de 20.5.2014, p. 143).

<sup>70</sup> Decisão 2010/261/UE da Comissão, de 4 de maio de 2010, relativa ao plano de segurança para o SIS II Central e a infraestrutura de comunicação (JO L 112 de 5.5.2010, p. 31).

ADOTARAM O PRESENTE REGULAMENTO:

## CAPÍTULO I

### DISPOSIÇÕES GERAIS

#### *Artigo 1.º*

#### *Objetivo geral do SIS*

O SIS tem por objetivo assegurar um elevado nível de segurança no espaço de liberdade, segurança e justiça da União, incluindo a manutenção da segurança pública e da ordem pública e a salvaguarda da segurança no território dos Estados-Membros, bem como aplicar as disposições do título V, parte III, capítulos 4 e 5, do Tratado sobre o Funcionamento da União Europeia relativas à circulação das pessoas nos seus territórios, com base nas informações transmitidas por este sistema.

#### *Artigo 2.º*

#### *Âmbito de aplicação*

1. O presente regulamento estabelece as condições e os procedimentos a aplicar à introdução e ao tratamento no SIS de indicações relativas a pessoas e objetos, bem como ao intercâmbio de informações suplementares e de dados suplementares para efeitos da cooperação policial e judiciária em matéria penal.
2. O presente regulamento também inclui disposições sobre a arquitetura técnica do SIS, as responsabilidades dos Estados-Membros e da Agência europeia para a gestão operacional de sistemas informáticos de grande escala no espaço de liberdade, segurança e justiça, as normas gerais de tratamento de dados, os direitos das pessoas em causa, bem como em matéria de responsabilidade.

#### *Artigo 3.º*

#### *Definições*

1. Para efeitos do presente regulamento, entende-se por:
  - (a) «Indicação», um conjunto de dados, incluindo identificadores biométricos como referido nos artigos 22.º e 40.º, introduzidos no SIS para permitir que as autoridades competentes procedam à identificação de pessoas ou objetos com vista à tomada de medidas específicas;
  - (b) «Informações suplementares», as informações não incluídas na indicação armazenada no SIS, mas ligadas a indicações inseridas no SIS, cujo intercâmbio é efetuado:
    - (1) Para permitir que os Estados-Membros se consultem ou informem mutuamente quando é inserida uma indicação;
    - (2) Na sequência de um acerto a fim de adotar a conduta adequada;
    - (3) Quando não for possível adotar a conduta adequada;
    - (4) Para efeitos da qualidade dos dados do SIS;
    - (5) Para efeitos da compatibilidade e prioridade das indicações;
    - (6) Para efeitos do exercício dos direitos de acesso;

- (c) «Dados suplementares», os dados armazenados no SIS e ligados a indicações inseridas no SIS que devem estar imediatamente à disposição das autoridades competentes quando, em resultado da consulta deste sistema, sejam localizadas pessoas relativamente às quais tinham sido introduzidos dados no SIS;
- (d) «Dados pessoais», qualquer informação relativa a uma pessoa singular identificada ou identificável («titular de dados»);
- (e) «Pessoa singular identificável», qualquer pessoa suscetível de ser identificada, direta ou indiretamente, nomeadamente através de elementos identificadores como um nome, um número de identidade, dados de localização, um identificador em linha ou um ou mais elementos específicos da identidade física, fisiológica, genética, psíquica, económica, cultural ou social dessa pessoa singular;
- (f) «Tratamento de dados pessoais», uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição;
- (g) Obter um «acerto» no SIS significa que:
  - (1) É efetuada uma consulta por um utilizador;
  - (2) A consulta deteta uma indicação inserida por outro Estado-Membro no SIS;
  - (3) Os dados relativos à indicação no SIS correspondem aos dados procurados; e
  - (4) É solicitada a adoção de uma conduta;
- h) «Referência», a suspensão de validade de uma indicação a nível nacional, que pode ser aditada às indicações para efeitos de detenção, às indicações relativas a pessoas desaparecidas e às indicações para efeitos de vigilância discreta, controlo específico ou controlo de verificação quando um Estado-Membro considera que dar execução a essa indicação não é compatível com a legislação nacional, as suas obrigações internacionais ou interesses nacionais essenciais. Sempre que uma referência é aposta numa indicação, a conduta a adotar com base nessa indicação não pode ser executada no território deste Estado-Membro.
- i) «Estado-Membro autor da indicação», o Estado-Membro que inseriu a indicação no SIS;
- j) «Estado-Membro de execução», o Estado-Membro que adota ou adotou a conduta adequada na sequência de um acerto;
- k) «Utilizadores finais», as autoridades competentes que consultam diretamente o CS-SIS, o N.SIS ou uma cópia técnica destes sistemas;
- l) «Dados dactilográficos», os dados das impressões digitais e das impressões palmares que, devido ao carácter único e aos pontos de referência que contêm permitem comparações rigorosas e fiáveis sobre a identidade das pessoas;

- m) «Crimes graves», as infrações enumeradas no artigo 2.º, n.ºs 1 e 2 da Decisão-Quadro 2002/584/JAI de 13 de junho de 2002<sup>71</sup>;
- n) «Crimes de terrorismo», as infrações previstas pelo direito nacional a que se referem os artigos 1.º a 4.º da Decisão-Quadro 2002/475/JAI de 13 de junho de 2002<sup>72</sup>.

#### *Artigo 4.º*

##### *Arquitetura técnica e modo de funcionamento do SIS*

1. O SIS é composto por:
  - (a) Um sistema central (SIS Central) constituído por:
    - uma função de apoio técnico (CS-SIS) que contém uma base de dados (base de dados SIS),
    - uma interface nacional uniforme (NI-SIS);
  - (b) Um sistema nacional (N.SIS) em cada Estado-Membro, constituído pelos sistemas de dados nacionais que comunicam com o SIS Central. Cada N.SIS deve conter um ficheiro de dados (cópia nacional) que constitui a cópia integral ou parcial da base de dados do SIS, bem como uma cópia de salvaguarda do N.SIS. O N.SIS e a sua cópia de salvaguarda podem ser utilizados simultaneamente para assegurar disponibilidade ininterrupta aos utilizadores finais;
  - (c) Uma infraestrutura de comunicação entre o CS-SIS 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.
2. Os dados do SIS são introduzidos, atualizados, suprimidos e consultados através dos vários N.SIS. É disponibilizada uma cópia nacional, parcial ou integral, destinada às consultas automatizadas no território de cada um dos Estados-Membros que utilizem tal cópia. A cópia nacional parcial deve incluir, pelo menos, os dados a que se refere o artigo 20.º, n.º 2, relativos a objetos e os dados a que se refere o artigo 20.º, n.º 3, alíneas a) a v), do presente regulamento respeitantes a indicações relativas a pessoas. Não é possível consultar os ficheiros de dados dos N. SIS dos outros Estados-Membros.
3. O CS-SIS assegura a supervisão técnica e funções de administração e deve dispor de um CS-SIS de salvaguarda capaz de assegurar todas as funcionalidades do CS-SIS principal em caso de falha deste sistema. O CS-SIS e a sua cópia de salvaguarda são instalados nas duas localizações técnicas da Agência Europeia para a gestão operacional de sistemas informáticos de grande escala no espaço de liberdade, segurança e justiça, criada pelo Regulamento (UE) n.º 1077/2011<sup>73</sup> («Agência»). O

---

<sup>71</sup> 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 18.07.2002, p. 1).

<sup>72</sup> Decisão-Quadro 2002/475/JAI do Conselho, de 13 de junho de 2002, relativa à luta contra o terrorismo (JO L 164 de 22.6.2002, p. 3).

<sup>73</sup> Estabelecida pelo Regulamento (UE) n.º 1077/2011 do Parlamento Europeu e do Conselho, de 25 de outubro de 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 286 de 1.11.2011, p. 1).

CS-SIS, ou o CS-SIS de salvaguarda, podem conter uma cópia adicional da base de dados do SIS e podem ser utilizados simultaneamente em funcionamento ativo desde que cada um deles tenha capacidade para tratar todas as operações relacionadas com as indicações do SIS.

4. O CS-SIS presta os serviços necessários para a introdução e o tratamento de dados no SIS, incluindo a consulta da base de dados do SIS. O CS-SIS assegura:
  - a) A atualização em linha das cópias nacionais;
  - b) A sincronização e a coerência entre as cópias nacionais e a base de dados do SIS;
  - c) As operações de inicialização e restauro das cópias nacionais;
  - d) A disponibilidade ininterrupta.

#### *Artigo 5.º*

##### *Custos*

1. Os custos de funcionamento, manutenção e desenvolvimento ulterior do SIS Central e da infraestrutura de comunicação são suportados pelo orçamento geral da União Europeia.
2. Os referidos custos incluem os trabalhos efetuados em relação ao CS-SIS para assegurar os serviços referidos no artigo 4.º, n.º 4.
3. Os custos de instalação, funcionamento, manutenção e desenvolvimento ulterior de cada N.SIS são suportados pelo Estado-Membro em causa.

## **CAPÍTULO II**

### **RESPONSABILIDADES DOS ESTADOS-MEMBROS**

#### *Artigo 6.º*

##### *Sistemas nacionais*

Cada Estado-Membro é responsável pela instalação, funcionamento, manutenção e desenvolvimento ulterior do respetivo N.SIS e pela conexão do seu N.SIS à NI-SIS.

Cada Estado-Membro é responsável por assegurar a continuidade do funcionamento do N.SIS, a sua conexão à NI-SIS e a disponibilidade ininterrupta dos dados do SIS aos utilizadores finais.

#### *Artigo 7.º*

##### *Serviço N.SIS e Gabinete SIRENE*

1. Cada Estado-Membro deve designar uma autoridade (Serviço N.SIS) que assume a responsabilidade central pelo seu N.SIS.

A referida autoridade é responsável pelo correto funcionamento e segurança do N.SIS, assegura o acesso das autoridades competentes ao SIS e adota as medidas necessárias para assegurar o cumprimento das disposições do presente regulamento. Incumbe-lhe a responsabilidade de assegurar que todas as funcionalidades do SIS são devidamente disponibilizadas aos utilizadores finais.



Cada Estado-Membro deve transmitir as suas indicações por intermédio do respetivo Serviço N.SIS.

2. Cada Estado-Membro deve designar a autoridade que assegura o intercâmbio e a disponibilidade de todas as informações suplementares (Gabinete SIRENE) em conformidade com as disposições do Manual SIRENE, como referido no artigo 8.º.

Estes gabinetes devem coordenar igualmente a verificação da qualidade das informações introduzidas no SIS. Para esse efeito, devem ter acesso aos dados tratados no SIS.

3. Cada Estado-Membro deve comunicar à Agência os nomes do seu Serviço N.SIS e do seu Gabinete SIRENE. A Agência deve publicar a lista dessas entidades juntamente com a lista a que se refere o artigo 53.º, n.º 8.

#### *Artigo 8.º*

##### *Intercâmbio de informações suplementares*

1. O intercâmbio de informações suplementares deve ser conforme com as disposições do Manual SIRENE e realizado através da infraestrutura de comunicação. Os Estados-Membros devem fornecer os recursos técnicos e humanos necessários para garantir a disponibilidade contínua e o intercâmbio de informações suplementares. Em caso de indisponibilidade da infraestrutura de comunicação, os Estados-Membros podem utilizar outros meios técnicos dotados da segurança adequada ao intercâmbio de informações suplementares.
2. As informações suplementares devem ser utilizadas exclusivamente para as finalidades para que foram transmitidas em conformidade com o artigo 61.º, a menos que seja obtido o consentimento prévio do Estado-Membro autor da indicação.
3. Os Gabinetes SIRENE devem desempenhar as suas funções de forma rápida e eficiente, em especial respondendo a um pedido o mais rapidamente possível e, o mais tardar, 12 horas após a receção do mesmo.
4. Devem ser adotadas normas pormenorizadas para o intercâmbio de informações suplementares mediante atos de execução em conformidade com o procedimento de exame a que se refere o artigo 72.º, n.º 2, sob a forma de um manual denominado «Manual SIRENE».

#### *Artigo 9.º*

##### *Adequação técnica e funcional*

1. Ao criar o seu N.SIS, cada Estado-Membro deve proceder em conformidade com normas, protocolos e processos técnicos comuns estabelecidos para assegurar a compatibilidade do seu N.SIS com o CS-SIS tendo em vista uma transmissão de dados rápida e efetiva. Essas normas, protocolos e procedimentos técnicos comuns devem ser adotados através de medidas de execução em conformidade com o procedimento de exame a que se refere o artigo 72.º, n.º 2.
2. Os Estados-Membros devem assegurar, através dos serviços prestados pelo CS-SIS, que os dados armazenados na cópia nacional são idênticos e coerentes com a base de dados do SIS, mediante as atualizações automáticas referidas no artigo 4.º, n.º 4, bem como que a consulta na sua cópia nacional produz um resultado equivalente ao de uma consulta na base de dados do SIS. Os utilizadores finais devem receber os dados

necessários ao desempenho das suas funções, em especial todos os dados necessários para identificar o titular dos dados e para adotar a conduta adequada.

### *Artigo 10.º*

#### *Segurança - Estados-Membros*

1. Cada Estado-Membro deve adotar, relativamente ao seu N.SIS, as medidas necessárias, incluindo um plano de segurança, um plano de continuidade operacional e um plano de recuperação em caso de incidente, a fim de:
  - (a) Proteger fisicamente os dados, nomeadamente através da elaboração de planos de emergência para a proteção das infraestruturas críticas;
  - (b) Impedir o acesso de pessoas não autorizadas às instalações utilizadas para o tratamento de dados pessoais (controlo da entrada nas instalações);
  - (c) Impedir que os suportes de dados sejam lidos, copiados, alterados ou retirados sem autorização (controlo dos suportes de dados);
  - (d) Impedir a introdução não autorizada de dados, bem como qualquer inspeção, alteração ou supressão não autorizadas de dados pessoais conservados (controlo de conservação);
  - (e) Impedir que sistemas automatizados de tratamento de dados possam ser utilizados por pessoas não autorizadas por meio de equipamento de transmissão de dados (controlo da utilização);
  - (f) Garantir que as pessoas autorizadas a utilizar um sistema automatizado de tratamento de dados só tenham acesso aos dados abrangidos pela sua autorização de acesso através de identidades de utilizador pessoais e únicas e de modos de acesso confidenciais (controlo do acesso aos dados);
  - (g) Garantir que todas as autoridades com direito de acesso ao SIS ou às instalações de tratamento de dados criam perfis que descrevam as funções e responsabilidades das pessoas autorizadas a ter acesso, introduzir, atualizar, suprimir e consultar os dados, e colocam esses perfis à disposição das autoridades nacionais de controlo a que se refere o artigo 66.º, sem demora e a pedido destas (perfis do pessoal);
  - (h) Garantir a possibilidade de verificar e determinar a que entidades podem ser transmitidos os dados pessoais por meio de equipamentos de transmissão de dados (controlo da transmissão);
  - (i) Garantir que se possa verificar e determinar posteriormente quais foram os dados pessoais introduzidos nos sistemas automatizados de tratamento de dados, quando, por quem e com que finalidade (controlo da introdução);
  - (j) Impedir, designadamente por meio de técnicas de cifragem adequadas, que os dados possam ser lidos, copiados, alterados ou suprimidos sem autorização durante a transmissão de dados pessoais ou o transporte dos suportes de dados (controlo do transporte);
  - (k) Fiscalizar a eficácia das medidas de segurança referidas no presente número e adotar as medidas organizativas necessárias relacionadas com o controlo interno (autocontrolo).

2. Os Estados-Membros devem adotar medidas equivalentes às referidas no n.º 1 no que respeita à segurança do tratamento e do intercâmbio de informações suplementares, incluindo a segurança das instalações do Gabinete SIRENE.
3. Os Estados-Membros devem adotar medidas equivalentes às referidas no n.º 1 no que respeita à segurança do tratamento dos dados do SIS pelas autoridades a que se refere o artigo 43.º.

#### *Artigo 11.º*

#### *Confidencialidade – Estados-Membros*

Cada Estado-Membro deve aplicar as suas regras de sigilo profissional ou outros deveres de confidencialidade equivalentes a todas as pessoas e entidades que tenham de trabalhar com dados do SIS e informações suplementares, nos termos do seu direito nacional. A referida obrigação mantém-se igualmente depois de essas pessoas cessarem funções ou deixarem o emprego, ou após a cessação das suas atividades.

#### *Artigo 12.º*

#### *Manutenção de registos a nível nacional*

1. Os Estados-Membros devem assegurar que cada acesso e todos os intercâmbios de dados pessoais a nível do CS-SIS são registados nos respetivos N.SIS a fim de verificar a legalidade da consulta e a legalidade do tratamento de dados, proceder ao autocontrolo e assegurar o correto funcionamento do N.SIS, bem como a integridade e a segurança dos dados.
2. Os registos indicam, em especial, o historial da indicação, a data e a hora da operação de tratamento dos dados, os dados utilizados para efetuar uma consulta, a referência aos dados transmitidos e os nomes da autoridade competente e da pessoa responsável pelo tratamento dos dados.
3. Se a consulta for realizada a partir de dados dactilográficos ou de uma imagem facial em conformidade com os artigos 40.º, 41.º e 42.º, os registos indicam, em especial, o tipo de dados utilizados para proceder a uma consulta, a referência ao tipo de dados transmitidos e o nome da autoridade competente e da pessoa responsável pelo tratamento dos dados.
4. Os registos só podem ser utilizados para os fins referidos no n.º 1, sendo suprimidos no prazo mínimo de um ano e máximo de três anos após a sua criação.
5. Os registos podem ser conservados por um período mais longo, se forem necessários para procedimentos de controlo já em curso.
6. As autoridades nacionais competentes encarregadas de controlar a legalidade da consulta, verificar a legalidade do tratamento de dados, proceder ao autocontrolo e assegurar o correto funcionamento do N.SIS e a integridade e segurança dos dados têm acesso a estes registos, nos limites da sua competência e a seu pedido, para efeitos de assegurar o cumprimento das suas funções.
7. Sempre que os Estados-Membros realizarem consultas automatizadas por *scan* de chapas de matrícula dos veículos a motor através de sistemas de reconhecimento automático de matrículas, devem manter um registo da consulta, nos termos do direito nacional. O conteúdo deste registo deve ser estabelecido através de medidas de execução, em conformidade com o procedimento de exame a que se refere o

artigo 72.º, n.º 2. Sempre que se obtiver uma correspondência consultando os dados armazenados no SIS ou numa cópia nacional ou técnica de dados dos SIS, deve ser efetuada uma consulta completa neste último para verificar se existe efetivamente tal correspondência. O disposto nos n.ºs 1 a 6 do presente artigo aplicam-se a essa consulta completa.

*Artigo 13.º*  
*Autocontrolo*

Os Estados-Membros devem assegurar que cada autoridade com direito de acesso aos dados do SIS toma as medidas necessárias para cumprir o disposto no presente regulamento e coopera, se necessário, com a autoridade nacional de controlo.

*Artigo 14.º*  
*Formação do pessoal*

Antes de ser autorizado a proceder ao tratamento dos dados armazenados no SIS, e periodicamente depois de o acesso aos dados do SIS ter sido concedido, o pessoal das autoridades com direito de acesso ao SIS deve receber formação adequada sobre as regras aplicáveis à segurança, à proteção de dados e aos procedimentos de tratamento dos dados referidas no Manual SIRENE. O pessoal deve ser informado de todas as infrações e sanções penais pertinentes.

## **CAPÍTULO III**

### **RESPONSABILIDADES DA AGÊNCIA**

*Artigo 15.º*  
*Gestão operacional*

1. A gestão operacional do SIS Central é da responsabilidade da Agência. A Agência deve, em cooperação com os Estados-Membros, assegurar que o SIS Central utiliza permanentemente a melhor tecnologia disponível com base numa análise custo-benefício.
2. A Agência é igualmente responsável pelo desempenho das seguintes atribuições relacionadas com a infraestrutura de comunicação:
  - (a) Supervisão;
  - (b) Segurança;
  - (c) Coordenação das relações entre os Estados-Membros e o fornecedor.
3. A Comissão é responsável por todas as outras funções relacionadas com a infraestrutura de comunicação, em especial:
  - (a) As relativas à execução do orçamento;
  - (b) Aquisição e renovação;
  - (c) Questões contratuais.

4. A Agência é responsável pelo desempenho das seguintes atribuições relacionadas com os Gabinetes SIRENE e a comunicação entre estes gabinetes:
  - (a) A coordenação e gestão de testes;
  - (b) A manutenção e atualização das especificações técnicas relativas ao intercâmbio de informações suplementares entre os Gabinetes SIRENE e a infraestrutura de comunicação, bem como a gestão do impacto das alterações técnicas quando afetam simultaneamente o SIS e o intercâmbio de informações suplementares entre os Gabinetes SIRENE.
5. A Agência deve desenvolver e manter um mecanismo e procedimentos para a realização de controlos de qualidade dos dados do CS-SIS e apresentar relatórios periódicos aos Estados-Membros. A Agência deve apresentar regularmente um relatório à Comissão sobre os problemas encontrados e os Estados-Membros em causa. O mecanismo, os procedimentos e a interpretação relativa à qualidade conforme dos dados são estabelecidos através de medidas de execução em conformidade com o procedimento de exame a que se refere o artigo 72.º, n.º 2.
6. A gestão operacional do SIS Central engloba todas as funções necessárias para assegurar o funcionamento do SIS Central, 24 horas por dia e sete dias por semana, em especial os trabalhos de manutenção e as adaptações técnicas indispensáveis ao correto funcionamento do sistema. Tais funções incluem igualmente as atividades de teste para assegurar que o SIS Central e os sistemas nacionais funcionam de acordo com os requisitos técnicos e funcionais, em conformidade com o artigo 9.º do presente regulamento.

*Artigo 16.º*  
*Segurança*

1. A Agência deve adotar as medidas necessárias, incluindo um plano de segurança, um plano de continuidade operacional e um plano de recuperação em caso de incidente para o SIS Central e a infraestrutura de comunicação, a fim de:
  - (a) Proteger fisicamente os dados, nomeadamente através da elaboração de planos de emergência para a proteção das infraestruturas críticas;
  - (b) Impedir o acesso de pessoas não autorizadas às instalações utilizadas para o tratamento de dados pessoais (controlo da entrada nas instalações);
  - (c) Impedir que os suportes de dados sejam lidos, copiados, alterados ou retirados sem autorização (controlo dos suportes de dados);
  - (d) Impedir a introdução não autorizada de dados, bem como qualquer inspeção, alteração ou supressão não autorizadas de dados pessoais conservados (controlo de conservação);
  - (e) Impedir que sistemas automatizados de tratamento de dados possam ser utilizados por pessoas não autorizadas por meio de equipamento de transmissão de dados (controlo da utilização);
  - (f) Garantir que as pessoas autorizadas a utilizar um sistema automatizado de tratamento de dados só tenham acesso aos dados abrangidos pela sua autorização de acesso através de identidades de utilizador pessoais e únicas e de modos de acesso confidenciais (controlo do acesso aos dados);

- (g) Criar perfis que descrevam as funções e responsabilidades das pessoas autorizadas a ter acesso aos dados ou às instalações de tratamento de dados e colocar esses perfis à disposição da Autoridade Europeia para a Proteção de Dados a que se refere o artigo 64.º, sem demora e a pedido desta (perfis do pessoal);
  - (h) Garantir a possibilidade de verificar e determinar a que entidades podem ser transmitidos os dados pessoais por meio de equipamentos de transmissão de dados (controlo da transmissão);
  - (i) Garantir que se possa verificar e determinar posteriormente quais os dados pessoais introduzidos nos sistemas automatizados de tratamento de dados, quando e por quem (controlo da introdução);
  - (j) Impedir, designadamente por meio de técnicas de cifragem adequadas, que os dados possam ser lidos, copiados, alterados ou suprimidos sem autorização durante a transferência de dados pessoais ou o transporte dos suportes de dados (controlo do transporte);
  - (k) Fiscalizar a eficácia das medidas de segurança referidas no presente número e adotar organizativas necessárias relacionadas com o controlo interno de forma a assegurar a conformidade com o presente regulamento (autocontrolo).
2. A Agência deve adotar medidas equivalentes às referidas no n.º 1 no que respeita à segurança do tratamento e do intercâmbio de informações suplementares através da infraestrutura de comunicação.

#### *Artigo 17.º*

##### *Confidencialidade – Agência*

1. Sem prejuízo do artigo 17.º do Estatuto dos Funcionários da União Europeia e do Regime Aplicável aos Outros Agentes da União, a Agência deve aplicar regras de sigilo profissional adequadas ou outros deveres de confidencialidade equivalentes a todo o seu pessoal que tenha de trabalhar com dados do SIS, segundo padrões comparáveis aos previstos no artigo 11.º do presente regulamento. A referida obrigação mantém-se depois de essas pessoas cessarem funções ou deixarem o emprego, ou após a cessação das suas atividades.
2. A Agência deve adotar medidas equivalentes às referidas no n.º 1 no que respeita à confidencialidade do intercâmbio de informações suplementares através da infraestrutura de comunicação.

#### *Artigo 18.º*

##### *Manutenção de registos a nível central*

1. A Agência deve assegurar que cada acesso e todos os intercâmbios de dados pessoais a nível do CS-SIS são registados para os efeitos previstos no artigo 12.º, n.º 1.
2. Os registos devem conter, em especial, o historial das indicações, a data e a hora da transmissão dos dados, o tipo de dados utilizados para proceder a uma consulta, a referência ao tipo de dados transmitidos e o nome da autoridade competente responsável pelo tratamento dos dados.
3. Se a consulta for realizada a partir de dados dactilográficos ou de uma imagem facial em conformidade com os artigos 40.º, 41.º e 42.º, os registos indicam, em especial, o tipo de dados utilizados para proceder a uma consulta, a referência ao tipo de dados

transmitidos e o nome da autoridade competente e da pessoa responsável pelo tratamento dos dados.

4. Os registos só podem ser utilizados para os fins previstos no n.º 1, sendo suprimidos no prazo mínimo de um ano e máximo de três anos depois da sua criação. Os registos que incluam o historial de indicações devem ser apagados entre um a três anos após a supressão das indicações.
5. Os registos podem ser mantidos por um período mais longo se forem necessários para procedimentos de controlo já em curso.
6. As autoridades nacionais competentes encarregadas de controlar a legalidade da consulta, verificar a legalidade do tratamento de dados, proceder ao autocontrolo e assegurar o correto funcionamento do CS.SIS, a integridade e segurança dos dados têm acesso a estes registos, nos limites da sua competência e a seu pedido, para efeitos de assegurar o cumprimento das suas funções.

## **CAPÍTULO IV**

### **INFORMAÇÃO DO PÚBLICO**

#### *Artigo 19.º*

#### *Campanhas de informação do SIS*

A Comissão deve, em cooperação com as autoridades nacionais de controlo e com a Autoridade Europeia para a Proteção de Dados, realizar campanhas de informação dirigidas ao público sobre os objetivos do SIS, os dados conservados, as autoridades com acesso ao SIS e os direitos dos titulares de dados. Os Estados-Membros devem, em cooperação com as respetivas autoridades nacionais de controlo, elaborar e aplicar as políticas necessárias para informar os seus cidadãos sobre o SIS em geral.

## **CAPÍTULO V**

### **CATEGORIAS DE DADOS E APOSIÇÃO DE REFERÊNCIAS**

#### *Artigo 20.º*

#### *Categorias de dados*

1. Sem prejuízo do disposto no artigo 8.º, n.º 1, ou das disposições do presente regulamento que preveem a conservação de dados suplementares, o SIS deve incluir exclusivamente as categorias de dados transmitidos por cada um dos Estados-Membros e necessários para os fins previstos nos artigos 26.º, 32.º, 34.º, 36.º e 38.º.
2. As categorias de dados são as seguintes:
  - (a) Informações sobre pessoas objeto de indicações;
  - (b) Informações sobre objetos a que se referem os artigos 32.º, 36.º e 38.º.
3. As informações sobre pessoas objeto de uma indicação devem incluir exclusivamente os seguintes dados:

- (a) Apelido(s);
  - (b) Nome(s);
  - (c) Nome(s) à nascença;
  - (d) Apelidos utilizados anteriormente e pseudónimos;
  - (e) Características físicas particulares, objetivas e permanentes;
  - (f) Local de nascimento;
  - (g) Data de nascimento;
  - (h) Sexo;
  - (i) Nacionalidade(s);
  - (j) Se a pessoa em causa está armada, é violenta ou fugiu, ou está implicada numa atividade a que se referem os artigos 1.º, 2.º, 3.º e 4.º da Decisão-Quadro 2002/475/JAI do Conselho relativa à luta contra o terrorismo;
  - (k) Motivo da indicação;
  - (l) Autoridade que insere a indicação;
  - (m) Referência à decisão que originou a indicação;
  - (n) Conduta a adotar;
  - (o) Ligação(ões) a outras indicações inseridas no SIS nos termos do artigo 53.º;
  - (p) Tipo de crime que justificou a inserção da indicação;
  - (q) Número de inscrição da pessoa num registo nacional;
  - (r) Categoria de pessoa desaparecida (unicamente para as indicações a que se refere o artigo 32.º);
  - (s) Categoria de documento de identidade da pessoa;
  - (t) País de emissão do documento de identidade da pessoa;
  - (u) Número do documento de identidade da pessoa;
  - (v) Data de emissão do documento de identidade da pessoa;
  - (w) Fotografias e imagens faciais;
  - (x) Perfis de ADN em causa, sob reserva do disposto no artigo 22.º, n.º 1, alínea b), do presente regulamento;
  - (y) Dados dactilográficos;
  - (z) Cópia a cores do documento de identidade.
4. As regras técnicas necessárias para a introdução, atualização, supressão e consulta dos dados referidos nos n.ºs 2 e 3, devem ser estabelecidas e desenvolvidas através de medidas de execução em conformidade com o procedimento de exame a que se refere o artigo 72.º, n.º 2.
5. As regras técnicas necessárias para a consulta dos dados referidos no n.º 3, devem ser estabelecidas e desenvolvidas em conformidade com o procedimento de exame a que se refere o artigo 72.º, n.º 2. Essas regras técnicas devem ser similares às utilizadas para as consultas no CS-SIS, bem como nas cópias nacionais e nas cópias técnicas,



tal como referido no artigo 53.º, n.º 2, devendo basear-se em normas comuns estabelecidas e desenvolvidas através de medidas de execução em conformidade com o procedimento de exame a que se refere o artigo 72.º, n.º 2.

*Artigo 21.º*  
*Proporcionalidade*

1. Antes de emitir uma indicação e quando o seu prazo de validade é prorrogado, os Estados-Membros devem determinar se o caso é adequado, pertinente e suficientemente importante para justificar a sua inserção no SIS.
2. Sempre que um Estado-Membro procura uma pessoa ou um objeto em relação com um crime abrangido pelos artigos 1.º a 4.º da Decisão-Quadro 2002/475/JAI do Conselho relativa à luta contra o terrorismo, deve criar, em todas as circunstâncias, a indicação correspondente em conformidade com os artigos 34.º, 36.º ou 38.º, consoante o caso.

*Artigo 22.º*  
*Regras aplicáveis à inserção de fotografias, imagens faciais, dados dactilográficos e perfis de ADN*

1. A introdução no SIS dos dados mencionados no artigo de 20.º, n.º 3, alíneas w), x) e y), está subordinada às seguintes disposições:
  - (a) As fotografias, as imagens faciais, os dados dactilográficos e os perfis de ADN apenas são introduzidos depois de terem sido sujeitos a um controlo de qualidade visando garantir o respeito de normas mínimas em matéria de qualidade dos dados;
  - (b) O perfil de ADN apenas pode ser aditado às indicações previstas no artigo 32.º, n.º 2, alíneas a) e c), quando as fotografias, as imagens faciais ou os dados dactilográficos que permitam a identificação não se encontrem disponíveis. Os perfis de ADN de pessoas que são ascendentes ou descendentes diretos ou irmãos ou irmãs da pessoa objeto da indicação podem ser acrescentados à indicação, desde que as pessoas em causa deem o seu consentimento explícito. A origem racial da pessoa não deve ser incluída no perfil de ADN.
2. Devem ser estabelecidas normas de qualidade para o armazenamento dos dados referidos no n.º 1, alínea a), do presente artigo e no artigo 40.º. As especificações dessas normas devem ser estabelecidas através de medidas de execução e atualizadas em conformidade com o procedimento de exame a que se refere o artigo 72.º, n.º 2.

*Artigo 23.º*  
*Requisito para a inserção de indicações*

1. Não podem ser inseridas indicações sem os dados referidos no artigo 20.º, n.º 3, alíneas a), g), k), m) e n), e, quando aplicável, p), exceto nas situações referidas no artigo 40.º.
2. Sempre que estejam disponíveis, devem ser introduzidos todos os outros dados enumerados no artigo 20.º, n.º 3.

#### *Artigo 24.º*

##### *Disposições gerais sobre a aposição de referências*

1. Sempre que um Estado-Membro considerar que dar execução a uma indicação inserida nos termos dos artigos 26.º, 32.º e 36.º não é compatível com o seu direito nacional, as suas obrigações internacionais ou interesses nacionais essenciais, pode solicitar posteriormente que seja aposta nessa indicação uma referência assinalando que a conduta a adotar com base na indicação não será executada no seu território. Essa referência será aposta pelo Gabinete SIRENE do Estado-Membro autor da indicação.
2. Para permitir aos Estados-Membros solicitar a aposição de referências em indicações emitidas de acordo com o artigo 26.º, todos os Estados-Membros são informados automaticamente, através do intercâmbio de informações suplementares, da inserção de qualquer nova indicação dessa categoria.
3. Se, em casos especialmente urgentes e graves, o Estado-Membro autor da indicação solicitar a execução da medida, o Estado-Membro de execução examina se pode autorizar a retirada da referência aposta a seu pedido. Se o Estado-Membro de execução puder retirá-la, deve fazer o necessário para que a conduta a adotar possa ser imediatamente executada.

#### *Artigo 25.º*

##### *Aposição de referências nas indicações para detenção para efeitos de entrega*

1. Sempre que se aplique a Decisão-Quadro 2002/584/JAI, a referência visando impedir a detenção só deve ser aposta nas indicações de detenção para entrega se a autoridade judiciária competente, por força do direito nacional, tendo em vista a execução de um mandado de detenção europeu, tiver recusado o seu cumprimento invocando um motivo de não execução e a aposição da referência tiver sido solicitada.
2. Todavia, a pedido de uma autoridade judiciária competente por força do direito nacional, quer com base numa instrução geral quer num caso específico, pode também ser solicitada a aposição de uma referência a uma indicação de detenção para entrega se for evidente que a execução do mandado de detenção europeu terá de ser recusada.

## **CAPÍTULO VI**

### **INDICAÇÕES RELATIVAS A PESSOAS PROCURADAS PARA DETENÇÃO PARA EFEITOS DE ENTREGA OU DE EXTRADIÇÃO**

#### *Artigo 26.º*

##### *Objetivos e condições para a emissão de indicações*

1. Os dados relativos a pessoas procuradas para detenção para efeitos de entrega, com base num mandado de detenção europeu, ou procuradas para detenção para efeitos de extradição, são introduzidos a pedido da autoridade judiciária do Estado-Membro autor da indicação.
2. Os dados relativos a pessoas procuradas para detenção para efeitos de entrega também devem ser introduzidos com base em mandados de detenção emitidos ao abrigo de acordos celebrados entre a União e países terceiros, com base no

artigo 37.º do Tratado da União Europeia, para efeitos de entrega de pessoas com base num mandado de detenção, que prevejam a transmissão desse mandado através do SIS.

3. Qualquer referência no presente regulamento às disposições da Decisão-Quadro 2002/584/JAI deve ser interpretada de modo a incluir as disposições correspondentes dos acordos celebrados entre a União Europeia e países terceiros, com base no artigo 37.º do Tratado da União Europeia, para efeitos de entrega de pessoas com base num mandado de detenção, que prevejam a transmissão desse mandado através do SIS.
4. O Estado-Membro autor da indicação pode, no caso de operações de consulta em curso e após ter obtido autorização da sua autoridade judiciária competente, tornar temporariamente indisponível para consulta a indicação para detenção emitida por força do artigo 26.º do presente regulamento, para que o utilizador final não possa consultar essa indicação e que esta só fique acessível aos Gabinetes SIRENE. Esta funcionalidade deve ser utilizada durante um período não superior a 48 horas. Caso seja necessário a nível operacional, a sua utilização pode, contudo, ser prorrogada por períodos adicionais de 48 horas. Os Estados-Membros devem manter estatísticas sobre o número de indicações relativamente às quais esta funcionalidade foi utilizada.

#### *Artigo 27.º*

##### *Dados suplementares relativos a pessoas procuradas para detenção para efeitos de entrega*

1. No caso de pessoas procuradas para detenção para efeitos de entrega com base em mandados de detenção europeus, o Estado-Membro autor da indicação deve inserir no SIS uma cópia do original dos mandados.
2. O Estado-Membro autor da indicação pode inserir cópia da tradução do mandado de detenção europeu, numa ou mais línguas oficiais das instituições da União Europeia.

#### *Artigo 28.º*

##### *Informações suplementares relativas a pessoas procuradas para detenção para efeitos de entrega*

O Estado-Membro que inseriu a indicação no SIS para detenção para efeitos de entrega deve comunicar a informação a que se refere o artigo 8.º, n.º 1, da Decisão-Quadro 2002/584/JAI a todos os Estados-Membros mediante o intercâmbio de informações suplementares.

#### *Artigo 29.º*

##### *Informações suplementares relativas a pessoas procuradas para detenção para efeitos de extradição*

1. O Estado-Membro que inseriu a indicação no SIS para efeitos de extradição deve comunicar os seguintes dados a todos os outros Estados-Membros através do intercâmbio de informações suplementares:
  - (a) A autoridade que emitiu o pedido de detenção;
  - (b) A existência de mandado de detenção ou documento com o mesmo efeito jurídico, ou de decisão executória;
  - (c) A natureza e a classificação jurídica do crime;

- (d) A descrição das circunstâncias em que foi cometido o crime, incluindo a hora, o local e o grau de participação da pessoa a respeito da qual foi inserida a indicação;
  - (e) Se possível, as consequências do crime;
  - (f) Qualquer outra informação útil ou necessária para a execução da conduta a adotar solicitada na indicação.
2. Os dados referidos no n.º 1 não são comunicados quando os dados a que se referem os artigos 27.º ou 28.º já tiverem sido transmitidos e sejam considerados suficientes para a execução da conduta a adotar solicitada na indicação pelo Estado-Membro em causa.

#### *Artigo 30.º*

#### *Conversão das indicações de pessoas procuradas para detenção para efeitos de entrega ou de extradição*

Se não for possível proceder à detenção quer devido à recusa do Estado-Membro requerido, em conformidade com os procedimentos sobre a aposição de referências previstos nos artigos 24.º ou 25.º, quer porque no caso de indicação para detenção para efeitos de extradição a investigação ainda não foi concluída, o Estado-Membro requerido deve tratar a indicação como sendo para efeitos de comunicação do paradeiro da pessoa em causa.

#### *Artigo 31.º*

#### *Execução da conduta a adotar baseada nas indicações sobre pessoas procuradas para detenção para efeitos de entrega ou de extradição*

1. A indicação inserida no SIS em conformidade com o artigo 26.º, associada aos dados suplementares referidos no artigo 27.º, constitui e produz os mesmos efeitos do mandado de detenção europeu emitido em conformidade com a Decisão-Quadro 2002/584/JAI, caso esta última se aplique.
2. Sempre que não se aplique a Decisão-Quadro 2002/584/JAI, a indicação inserida no SIS em conformidade com os artigos 26.º e 29.º produz os mesmos efeitos do pedido de detenção provisória na aceção do artigo 16.º da Convenção Europeia de Extradição, de 13 de dezembro de 1957, ou do artigo 15.º do Tratado Benelux de Extradição e de Auxílio Judiciário Mútuo em Matéria Penal, de 27 de junho de 1962.

## **CAPÍTULO VII**

### **INDICAÇÕES RELATIVAS A PESSOAS DESAPARECIDAS**

#### *Artigo 32.º*

#### *Objetivos e condições para a emissão de indicações*

1. São inseridos no SIS os dados relativos a pessoas desaparecidas ou outras pessoas que necessitam de ser colocadas sob proteção e cujo paradeiro tem de ser determinado a pedido da autoridade competente do Estado-Membro autor da indicação.
2. Podem ser inseridas as seguintes categorias de pessoas desaparecidas:
  - (a) Pessoas desaparecidas que devem ser colocadas sob proteção:

- para sua própria proteção;
- para prevenir ameaças;
- (b) Pessoas desaparecidas que não precisam de ser colocadas sob proteção.
- (c) Crianças que correm risco de rapto, em conformidade com o n.º 4.
3. O n.º 2, alínea a), aplica-se apenas às crianças e às pessoas que devem ficar retidas após decisão da autoridade competente.
4. A indicação relativa a uma criança a que se refere o n.º 2, alínea c), é inserida a pedido da autoridade judiciária competente de um Estado-Membro que tenha competência em matéria de responsabilidade parental, em conformidade com o Regulamento (CE) n.º 2201/2003<sup>74</sup>, quando exista um risco concreto e manifesto de que a criança seja deslocada, de forma ilegal e iminente, para fora do Estado-Membro onde se encontra essa autoridade judiciária competente. Nos Estados-Membros que são Partes na Convenção da Haia, de 19 de outubro de 1996, relativa à Competência, à Lei Aplicável, ao Reconhecimento, à Execução e à Cooperação em matéria de Responsabilidade Parental e Medidas de Proteção das Crianças e sempre que não se aplique o Regulamento (CE) n.º 2201/2003, são aplicáveis as disposições da Convenção da Haia.
5. Os Estados-Membros devem assegurar que os dados introduzidos no SIS indicam em que categoria referida no n.º 2 se insere a pessoa desaparecida. Além disso, os Estados-Membros devem assegurar que os dados introduzidos no SIS indicam se o tipo de caso se refere a pessoas desaparecidas ou pessoas vulneráveis. As regras sobre a categorização dos tipos de casos e a introdução desses dados devem ser estabelecidas e desenvolvidas através de medidas de execução adotadas em conformidade com o procedimento de exame a que se refere o artigo 72.º, n.º 2.
6. Quatro meses antes de a criança, objeto de indicação por força do presente artigo, atingir a maioridade, o CS-SIS notifica automaticamente o Estado-Membro autor da indicação de que o motivo do pedido e a conduta a adotar devem ser atualizados ou a indicação tem de ser suprimida.
7. Sempre que existam indícios manifestos de uma ligação entre veículos, embarcações ou aeronaves a uma pessoa que é objeto de uma indicação por força do n.º 2, podem ser inseridas indicações relativas a esses veículos, embarcações e aeronaves a fim de localizar a pessoa. Nestes casos, a indicação sobre a pessoa desaparecida e a indicação sobre o objeto devem ser associadas, em conformidade com o artigo 60.º. As regras técnicas necessárias para a introdução, atualização, supressão e consulta dos dados referidos no presente número, devem ser estabelecidas e desenvolvidas através de medidas de execução adotadas em conformidade com o procedimento de exame a que se refere o artigo 72.º, n.º 2.

### *Artigo 33.º*

#### *Execução da conduta solicitada na indicação*

1. Sempre que a pessoa a que se refere o artigo 32.º for localizada, as autoridades competentes devem comunicar o seu paradeiro ao Estado-Membro autor da

---

<sup>74</sup> Regulamento (CE) n.º 2201/2003 do Conselho de 27 de novembro de 2003, relativo à competência, ao reconhecimento e à execução de decisões em matéria matrimonial e em matéria de responsabilidade parental e que revoga o Regulamento (CE) n.º 1347/2000 (JO L 338 de 23.12.2003, p. 1).

indicação, sob reserva do disposto no n.º 2. No caso de crianças desaparecidas ou que devem ser colocadas sob proteção, o Estado-Membro de execução consulta imediatamente o Estado-Membro autor da indicação, a fim de decidir sem demora as medidas a tomar para preservar o interesse superior da criança. As autoridades competentes podem, nos casos referidos no artigo 32.º, n.º 2, alíneas a) e c), colocar as pessoas em causa em segurança, a fim de as impedir de prosseguir viagem, se o direito nacional o autorizar.

2. A comunicação de dados, diferente daquela efetuada entre as autoridades competentes, sobre a pessoa maior desaparecida que foi localizada, está subordinada ao consentimento dessa pessoa. As autoridades competentes podem, contudo, informar a pessoa que assinalou o desaparecimento de que a indicação foi apagada devido ao facto de pessoa desaparecida ter sido localizada.

## **CAPÍTULO VIII**

### **INDICAÇÕES RELATIVAS A PESSOAS PROCURADAS NO ÂMBITO DE PROCESSOS JUDICIAIS**

#### *Artigo 34.º*

#### *Objetivos e condições para a emissão de indicações*

1. Para efeitos da comunicação do local de residência ou do domicílio de pessoas, os Estados-Membros devem introduzir no SIS, a pedido das autoridades judiciais competentes, os dados relativos a:
  - (a) Testemunhas;
  - (b) Pessoas notificadas ou procuradas para serem notificadas a comparecer perante as autoridades judiciais, no âmbito de um processo penal, a fim de responder por factos que lhes são imputados;
  - (c) Pessoas que devam ser notificadas de uma sentença penal ou de outros documentos, no âmbito de um processo penal, a fim de responder por factos que lhes são imputados;
  - (d) Pessoas que devam ser citadas ou notificadas para se apresentar, a fim de cumprir uma pena privativa de liberdade.
2. Sempre que existam indícios manifestos de uma ligação entre veículos, embarcações ou aeronaves a uma pessoa objeto de uma indicação por força do n.º 1, podem ser inseridas indicações relativas a esses veículos, embarcações e aeronaves a fim de localizar a pessoa. Nestes casos, a indicação relativa à pessoa e a indicação relativa ao objeto devem ser associadas, em conformidade com o artigo 60.º. As regras técnicas necessárias para a introdução, atualização, supressão e consulta dos dados referidos no presente número, devem ser estabelecidas e desenvolvidas através de medidas de execução adotadas em conformidade com o procedimento de exame a que se refere o artigo 72.º, n.º 2.

*Artigo 35.º*  
*Execução da conduta solicitada na indicação*

As informações solicitadas são comunicadas ao Estado-Membro requerente através do intercâmbio de informações suplementares.

## CAPÍTULO IX

### INDICAÇÕES RELATIVAS A PESSOAS E OBJETOS PARA EFEITOS DE VIGILÂNCIA DISCRETA, CONTROLO DE VERIFICAÇÃO OU DE CONTROLO ESPECÍFICO

*Artigo 36.º*  
*Objetivos e condições para a emissão de indicações*

1. Os dados sobre pessoas ou veículos, embarcações, aeronaves e contentores devem ser introduzidos nos termos do direito nacional do Estado-Membro autor da indicação para efeitos de vigilância discreta, controlo de verificação ou de controlo específico, em conformidade com o artigo 37.º, n.º 4.
2. A indicação pode ser inserida para efeitos de ação penal contra crimes, de execução de uma condenação penal ou de prevenção de ameaças contra a segurança pública:
  - (a) Sempre que existam indícios concretos de que a pessoa tem a intenção de cometer ou está a cometer um crime grave, em especial os correspondentes às infrações a que se refere o artigo 2.º, n.º 2, da Decisão-Quadro 2002/584/JAI;
  - (b) Sempre que as informações referidas no artigo 37.º, n.º 1, sejam necessárias para a execução de uma condenação penal da pessoa reconhecida culpada de um crime grave, em especial os correspondentes às infrações a que se refere o artigo 2.º, n.º 2, da Decisão-Quadro 2002/584/JAI; ou
  - (c) Sempre que a apreciação global da pessoa, em especial com base em crimes já cometidos, permita supor que poderá igualmente cometer no futuro um crime grave, em especial os correspondentes às infrações a que se refere o artigo 2.º, n.º 2, da Decisão-Quadro 2002/584/JAI.
3. Além disso, pode ser inserida uma indicação nos termos do direito nacional, a pedido das entidades responsáveis pela segurança nacional, sempre que indícios concretos permitam supor que as informações a que se refere o artigo 37.º, n.º 1, são necessárias para a prevenção de uma ameaça grave colocada pela pessoa em causa ou de outras ameaças graves contra a segurança nacional interna e externa. O Estado-Membro autor da indicação por força do presente número informa desse facto os outros Estados-Membros. Cada Estado-Membro determina as autoridades às quais esta informação deve ser transmitida.
4. Sempre que exista indício manifesto de que veículos, embarcações, aeronaves e contentores estão relacionados com os crimes graves referidos no n.º 2, ou com as ameaças graves referidas no n.º 3, podem ser inseridas indicações relativas a esses veículos, embarcações, aeronaves e contentores.
5. Sempre que exista indício manifesto de que documentos oficiais em branco ou documentos de identidade já emitidos estão relacionados com os crimes graves referidos no n.º 2, ou com as ameaças graves referidas no n.º 3, podem ser inseridas

indicações relativas a esses documentos, independentemente da identidade do eventual titular inicial do documento de identidade. As regras técnicas necessárias para a introdução, atualização, supressão e consulta dos dados referidos no presente número, devem ser estabelecidas e desenvolvidas através de medidas de execução adotadas em conformidade com o procedimento de exame a que se refere o artigo 72.º, n.º 2.

### *Artigo 37.º*

#### *Execução da conduta solicitada na indicação*

1. Para efeitos de vigilância discreta, de controlo de verificação ou de controlo específico, as informações seguintes podem, no todo ou em parte, ser recolhidas e transmitidas à autoridade autora da indicação, quando forem efetuados controlos nas fronteiras, controlos policiais e aduaneiros ou outras atividades repressivas no interior de um Estado-Membro:
  - (a) O facto de a pessoa ou o veículo, embarcação, aeronave, contentor, documento oficial em branco ou documento de identidade emitido objeto da indicação ter sido localizado;
  - (b) Local, hora e motivo do controlo;
  - (c) Itinerário e destino da viagem;
  - (d) As pessoas que acompanham o interessado ou os ocupantes do veículo, embarcação ou aeronave, ou as pessoas que acompanham o titular do documento oficial em branco ou do documento de identidade emitido, relativamente às quais se pode razoavelmente presumir estarem associadas ao interessado;
  - (e) A identidade revelada e a descrição da pessoa que utiliza o documento oficial em branco ou o documento de identidade emitido objeto da indicação;
  - (f) O veículo, embarcação, aeronave ou contentor utilizado;
  - (g) Os objetos transportados, incluindo documentos de viagem;
  - (h) As circunstâncias em que a pessoa ou o veículo, embarcação, aeronave, contentor, documento oficial em branco ou documento de identidade emitido foi localizado.
2. As informações mencionadas no n.º 1 devem ser comunicadas através do intercâmbio de informações suplementares.
3. Em função das condições operacionais e no respeito do direito nacional, a vigilância discreta deve incluir o controlo de rotina da pessoa ou do objeto, no intuito de recolher o máximo de informações descritas no n.º 1, sem prejudicar o carácter discreto da vigilância.
4. Em função das condições operacionais e no respeito do direito nacional, o controlo de verificação deve incluir o controlo mais aprofundado e um interrogatório da pessoa. Sempre que o controlo de verificação não seja autorizado pelo direito de um Estado-Membro deve ser substituído pela vigilância discreta nesse Estado-Membro.
5. Durante os controlos específicos, as pessoas, veículos, embarcações, aeronaves, contentores e objetos transportados podem ser revistados, nos termos do direito nacional, para os fins previstos no artigo 36.º. As revistas devem ser realizadas nos termos do direito nacional. Sempre que os controlos específicos não sejam



autorizados pelo direito de um Estado-Membro devem ser substituído por controlos de verificação nesse Estado-Membro.

## **CAPÍTULO X**

### **INDICAÇÕES RELATIVAS A OBJETOS PARA EFEITOS DE APREENSÃO OU DE UTILIZAÇÃO COMO PROVA EM PROCESSOS PENAIS**

#### *Artigo 38.º*

##### *Objetivos e condições para a emissão de indicações*

1. Os dados sobre objetos procurados para efeitos de apreensão ou de prova em processo penal devem ser introduzidos no SIS.
2. São introduzidas as seguintes categorias de objetos facilmente identificáveis:
  - (a) Veículos automóveis, tal como definidos no direito nacional, independentemente do seu sistema de propulsão;
  - (b) Reboques de peso superior a 750 kg, sem carga;
  - (c) Caravanas;
  - (d) Equipamento industrial;
  - (e) Embarcações;
  - (f) Motores de embarcações;
  - (g) Contentores;
  - (h) Aeronaves;
  - (i) Armas de fogo;
  - (j) Documentos oficiais em branco que tenham sido roubados, desviados ou extraviados;
  - (k) Documentos de identidade emitidos, tais como passaportes, cartões de identidade, cartas de condução, títulos de residência e documentos de viagem que tenham sido roubados, desviados, extraviados, invalidados ou falsificados;
  - (l) Certificados de matrícula dos veículos e chapas de matrícula que tenham sido roubados, desviados, extraviados, invalidados ou falsificados;
  - (m) Notas de banco (notas registadas) e notas de banco falsificadas;
  - (n) Equipamentos técnicos, produtos informáticos e outros objetos facilmente identificáveis de grande valor;
  - (o) Componentes identificáveis de veículos a motor;
  - (p) Componentes identificáveis de material industrial.
3. A definição de novas subcategorias de objetos, tal como mencionados no n.º 2, alínea n), e as regras técnicas necessárias para a introdução, atualização, supressão e consulta dos dados referidos no n.º 2, devem ser estabelecidas e desenvolvidas através de medidas de execução em conformidade com o procedimento de exame a que se refere o artigo 72.º, n.º 2.

*Artigo 39.º*

*Execução da conduta solicitada na indicação*

1. Sempre que a consulta revele que há uma indicação relativa a um objeto já localizado, a autoridade que estabeleceu a correspondência entre os dois dados procede à apreensão do objeto nos termos do direito nacional e entra em contacto com a autoridade autora da indicação a fim de decidirem das medidas a tomar. Para esse efeito, os dados pessoais podem ser igualmente transmitidos em conformidade com o presente regulamento.
2. As informações mencionadas no n.º 1 devem ser comunicadas através do intercâmbio de informações suplementares.
3. O Estado-Membro que localizou o objeto toma as medidas em conformidade com o seu direito nacional.

## **CAPÍTULO XI**

### **INDICAÇÕES RELATIVAS A PESSOAS PROCURADAS DESCONHECIDAS PARA EFEITOS DE IDENTIFICAÇÃO NOS TERMOS DO DIREITO NACIONAL E CONSULTA COM RECURSO A DADOS BIOMÉTRICOS**

*Artigo 40.º*

*Indicações relativas a pessoas procuradas desconhecidas para efeitos de detenção nos termos do direito nacional*

Podem ser introduzidos no SIS dados dactilográficos não associados a pessoas objeto de indicações. Estes dados dactilográficos devem consistir em conjuntos completos ou incompletos de impressões digitais ou palmares detetadas em locais de crimes sob investigação, de crimes graves ou de crimes de terrorismo, e em que seja possível determinar, com elevado grau de probabilidade, que pertencem ao autor do crime. Os dados dactilográficos incluídos nesta categoria são armazenados com a menção «pessoa ou suspeito procurado desconhecido», desde que as autoridades competentes não possam determinar a identidade da pessoa recorrendo a qualquer outra base dados nacional, europeia ou internacional.

*Artigo 41.º*

*Execução da conduta solicitada na indicação*

Em caso de acerto ou eventual correspondência com os dados armazenados por força do artigo 40.º, a identidade da pessoa é determinada nos termos do direito nacional, sendo verificado simultaneamente se os dados dactilográficos armazenados no SIS lhe pertencem. Os Estados-Membros devem comunicar entre si através do intercâmbio de informações suplementares para facilitar a investigação atempada do caso.

*Artigo 42.º*

*Regras aplicáveis à verificação ou consulta com recurso a fotografias, imagens faciais, dados dactilográficos e perfis de ADN*

1. As fotografias, impressões digitais, dados dactilográficos e perfis de ADN devem ser extraídos do SIS para verificar a identidade da pessoa localizada em resultado de consulta alfanumérica efetuada no SIS.
2. Os dados dactilográficos podem ser igualmente utilizados para identificar pessoas. Os dados dactilográficos armazenados no SIS devem ser consultados para fins de identificação se a identidade da pessoa não puder ser determinada por outros meios.
3. Os dados dactilográficos armazenados no SIS relativos a indicações inseridas por força dos artigos 26.º, 34.º, n.º 1, alínea b), e 36.º, também podem ser consultados utilizando conjuntos completos ou incompletos de impressões digitais ou impressões palmares detetadas em locais de crimes sob investigação e quando seja possível apurar, com elevado grau de probabilidade, que pertencem ao autor do crime, desde que as autoridades competentes não possam determinar a identidade da pessoa recorrendo a qualquer outra base de dados nacional, europeia ou internacional.
4. Logo que seja tecnicamente possível, e assegurando simultaneamente um elevado grau de fiabilidade da identificação, as fotografias e imagens faciais podem ser utilizadas para identificar pessoas. A identificação baseada em fotografias ou imagens faciais deve ser utilizada unicamente nos pontos de passagem regular das fronteiras onde são utilizados sistemas de *self-service* e sistemas automatizados de controlo das fronteiras.

## **CAPÍTULO XII**

### **DIREITO DE ACESSO E DE CONSERVAÇÃO DAS INDICAÇÕES**

*Artigo 43.º*

*Autoridades com direito de acesso às indicações*

1. O acesso aos dados inseridos no SIS, bem como o direito de os consultar diretamente ou por meio de uma cópia de dados do SIS, são reservados às autoridades competentes para efeitos de:
  - (a) Controlo das fronteiras, em conformidade com o Regulamento (UE) 2016/399 do Parlamento Europeu e do Conselho, de 19 de março de 2016, que estabelece o Código da União relativo ao regime de passagem de pessoas nas fronteiras (Código das Fronteiras Schengen);
  - (b) Verificações policiais e aduaneiras efetuadas no interior do Estado-Membro em causa, bem como a respetiva coordenação pelas autoridades designadas;
  - (c) Outras atividades de aplicação coerciva da lei para efeitos de prevenção, deteção e investigação de crimes no Estado-Membro em causa;
  - (d) Análise das condições e tomada de decisões relativas à entrada e permanência de nacionais de países terceiros no território dos Estados-Membros, incluindo sobre autorizações de residência e vistos de longa duração, bem como sobre o regresso de nacionais de países terceiros.
2. O direito de acesso aos dados introduzidos no SIS, bem como o direito de os consultar diretamente, podem também ser exercidos pelas autoridades judiciais

nacionais, nomeadamente as autoridades responsáveis pela instauração de ações penais e inquéritos judiciais antes de deduzida a acusação, no exercício das suas funções, nos termos previstos no direito nacional, bem como pelas respetivas autoridades de coordenação.

3. O direito de acesso aos dados introduzidos no SIS e de os consultar diretamente pode ser exercido pelas autoridades competentes para realizar as atividades referidas no n.º 1, alínea c), no exercício dessas atribuições. O acesso das referidas autoridades rege-se pelo direito nacional de cada Estado-Membro.
4. As autoridades referidas no presente artigo são incluídas na lista referida no artigo 53.º, n.º 8.

#### *Artigo 44.º*

##### *Autoridades responsáveis pela matrícula de veículos*

1. Os serviços responsáveis, nos Estados-Membros, pela emissão de certificados de matrícula dos veículos, como referido na Diretiva 1999/37/CE do Conselho<sup>75</sup>, devem ter acesso aos seguintes dados introduzidos no SIS em conformidade com o artigo 38.º, n.º 2, alíneas a), b), c) e l), do presente regulamento, tendo exclusivamente em vista verificar se os veículos que lhes são apresentados para matrícula foram roubados, desviados ou extraviados, ou se são procurados como meio de prova em processos penais:
  - (a) Dados sobre veículos a motor, tal como definidos no direito nacional, independentemente do seu sistema de propulsão;
  - (b) Dados sobre reboques de peso superior a 750 kg, sem carga, e sobre caravanas;
  - (c) Dados sobre certificados de matrícula de veículos e chapas de matrícula de veículos que tenham sido roubados, desviados, extraviados ou cancelados.

O acesso a esses dados por parte dos serviços responsáveis pela emissão dos certificados de matrícula de veículos rege-se pelo direito nacional de cada Estado-Membro.
2. Os serviços referidos no n.º 1 que sejam serviços públicos têm o direito de aceder diretamente aos dados introduzidos no SIS.
3. Os serviços referidos no n.º 1 que não sejam serviços públicos apenas têm acesso aos dados introduzidos no SIS por intermédio de uma das autoridades referidas no artigo 43.º do presente regulamento. Essa autoridade tem o direito de aceder diretamente aos dados e de os transmitir ao serviço em questão. O Estado-Membro em causa deve assegurar que esse serviço e o seu pessoal respeitam eventuais limitações de utilização dos dados comunicados pela referida autoridade.
4. O artigo 39.º do presente regulamento não se aplica ao acesso obtido em conformidade com o presente artigo. A comunicação às autoridades policiais ou judiciais, por parte dos serviços referidos no n.º 1, de informações que indiciem a suspeita de prática de um crime, obtidas através do acesso ao SIS, rege-se pelo direito nacional.

---

<sup>75</sup> Diretiva 1999/37/CE do Conselho, de 29 de abril de 1999, relativa aos documentos de matrícula dos veículos (JO L 138 de 1.6.1999, p. 57).

#### *Artigo 45.º*

##### *Autoridades responsáveis pelo registo de embarcações e aeronaves*

1. Os serviços responsáveis, nos Estados-Membros, pela emissão de certificados de registo ou por assegurar a gestão do tráfego de embarcações, incluindo motores de embarcações e de aeronaves, devem ter acesso aos seguintes dados introduzidos no SIS em conformidade com o artigo 38.º, n.º 2, do presente regulamento, tendo exclusivamente em vista verificar se as embarcações, incluindo motores de embarcações, as aeronaves ou os contentores que lhes são apresentados para registo ou no âmbito da gestão do tráfego, foram roubados, desviados ou extraviados, ou se são procurados como meio de prova em processos penais;
  - (a) Dados sobre embarcações;
  - (b) Dados sobre motores de embarcações;
  - (c) Dados sobre aeronaves.

Sob reserva do n.º 2, o acesso desses serviços a estes dados rege-se pelo direito de cada Estado-Membro. O acesso aos dados referidos nas alíneas a) a c) deve ser limitado à competência específica dos serviços em causa.

2. Os serviços referidos no n.º 1 que sejam serviços públicos têm o direito de aceder diretamente aos dados introduzidos no SIS.
3. Os serviços referidos no n.º 1 que não sejam serviços públicos apenas têm acesso aos dados introduzidos no SIS por intermédio de uma das autoridades referidas no artigo 43.º do presente regulamento. Essa autoridade tem o direito de aceder diretamente aos dados e de os transmitir ao serviço em questão. O Estado-Membro em causa deve assegurar que esse serviço e o seu pessoal respeitam eventuais limitações de utilização dos dados comunicados pela referida autoridade.
4. O artigo 39.º do presente regulamento não se aplica ao acesso obtido em conformidade com o presente artigo. A comunicação às autoridades policiais ou judiciárias, por parte dos serviços referidos no n.º 1, de informações que indiciem a suspeita de prática de um crime, obtidas através do acesso ao SIS, rege-se pelo direito nacional.

#### *Artigo 46.º*

##### *Acesso da Europol aos dados do SIS*

1. A Agência da União Europeia para a Cooperação Policial (Europol) deve ter, no âmbito do seu mandato, o direito de acesso e de consulta dos dados introduzidos no SIS.
2. Sempre que uma consulta efetuada pela Europol revele a existência de uma indicação no SIS, a Europol deve informar o Estado-Membro autor da indicação através dos canais definidos pelo Regulamento (UE) 2016/794.
3. A utilização das informações obtidas através de uma consulta no SIS está sujeita ao consentimento do Estado-Membro em causa. Se este último autorizar a utilização de tais informações, o seu tratamento deve reger-se pelo disposto no Regulamento (UE) 2016/794. A Europol só pode comunicar essas informações a países e organismos terceiros com o consentimento do Estado-Membro em causa.

4. A Europol pode solicitar informações adicionais ao Estado-Membro em causa, em conformidade como disposto no Regulamento (UE) 2016/794.
5. A Europol deve:
  - (a) Sem prejuízo dos n.ºs 3, 4 e 6, abster-se de ligar as partes do SIS a que aceda, bem como transferir os dados nelas contidos, para outro sistema informático de recolha e tratamento de dados gerido pela Europol, ou que funcione nas suas instalações, e descarregar ou copiar por outros meios qualquer parte do SIS;
  - (b) Limitar o acesso aos dados inseridos no SIS a membros do pessoal da Europol especificamente autorizados;
  - (c) Adotar e aplicar as medidas previstas nos artigos 10.º e 11.º;
  - (d) Permitir que a Autoridade Europeia para a Proteção de Dados supervisione as atividades da Europol no exercício do seu direito de aceder e consultar os dados introduzidos no SIS.
6. Os dados só podem ser copiados para fins técnicos desde que tal cópia seja necessária para uma consulta direta pelo pessoal devidamente autorizado da Europol. O disposto no presente regulamento é igualmente aplicável às referidas cópias. A cópia técnica deve ser utilizada para fins de armazenamento de dados do SIS enquanto esses dados estão a ser consultados. Depois dessa consulta, os dados devem ser suprimidos. As referidas utilizações não devem ser interpretadas como descargas ou cópias ilegais dos dados do SIS. A Europol não deve copiar dados das indicações nem dados adicionais introduzidos pelos Estados-Membros nem dados do CS-SIS para outros sistemas da Europol.
7. As cópias referidas no n.º 6, que deem origem a bases de dados fora de linha, podem ser conservadas por um período máximo de 48 horas. Este período pode ser prorrogado numa situação de emergência até que a mesma cessa. A Europol deve comunicar as eventuais prorrogações à Autoridade Europeia para a Proteção de Dados.
8. A Europol pode receber e tratar informações suplementares sobre as indicações correspondentes inseridas no SIS, desde que as normas de tratamento de dados referidas nos n.ºs 2 a 7 sejam aplicadas, se for caso disso.
9. Para efeitos de verificar a legalidade do tratamento de dados, o autocontrolo e a adequada integridade e segurança dos dados, a Europol deve conservar um registo de cada acesso e consulta no SIS. Esses registos e documentação não devem ser considerados descargas ou cópias ilegais de qualquer parte do SIS.

#### *Artigo 47.º*

##### *Acesso da Eurojust aos dados do SIS*

1. Os membros nacionais da Eurojust e os seus assistentes têm o direito, no âmbito do seu mandato, de acesso e de consulta dos dados do SIS introduzidos em conformidade com os artigos 26.º, 32.º, 34.º, 38.º e 40.º.
2. Sempre que a consulta do sistema efetuada por um membro nacional da Eurojust revele a existência de uma indicação no SIS, esse membro nacional deve informar do facto o Estado-Membro autor da indicação.
3. O presente artigo em nada afeta as disposições da Decisão 2002/187/JAI relativa à proteção de dados e à responsabilidade por qualquer tratamento não autorizado ou

incorreto dos dados por parte dos membros nacionais da Eurojust ou dos seus assistentes, nem os poderes da Instância Comum de Controlo, criada pela referida decisão.

4. Todos os acessos e consultas efetuados por membros nacionais da Eurojust ou seus assistentes devem ser registados nos termos do artigo 12.º, bem como qualquer utilização que façam dos dados a que acederam.
5. Nenhuma parte do SIS deve ser ligada a outro sistema informático de recolha e tratamento de dados gerido pela Eurojust, ou que funcione nas suas instalações, nem nenhum dos dados contidos no SIS aos quais os membros nacionais ou os seus assistentes tenham acesso deve ser transferido para esse sistema informático. Nenhuma parte do SIS deve ser descarregada. O registo dos acessos e das consultas não deve ser considerado como descarga ou cópia ilegal dos dados do SIS.
6. O acesso aos dados introduzidos no SIS é limitado aos membros nacionais e aos seus assistentes e não é extensivo ao pessoal da Eurojust.
7. Devem ser adotadas e aplicadas medidas para assegurar a segurança e a confidencialidade previstas nos artigos 10.º e 11.º.

#### *Artigo 48.º*

*Acesso aos dados do SIS pelas equipas da Guarda Europeia de Fronteiras e Costeira, pelas equipas envolvidas em operações de regresso e pelos membros da equipa de apoio à gestão da migração*

1. Em conformidade com o artigo 40.º, n.º 8, do Regulamento (UE) 2016/1624, os membros das equipas da Guarda Europeia de Fronteiras e Costeira ou das equipas envolvidas em operações de regresso, bem como dos membros das equipas de apoio à gestão da migração devem, no âmbito do seu mandato, ter o direito de aceder e consultar os dados introduzidos no SIS.
2. Os membros das equipas da Guarda Europeia de Fronteiras e Costeira ou das equipas envolvidas em operações de regresso, bem como das equipas de apoio à gestão da migração, devem poder aceder e consultar os dados introduzidos no SIS em conformidade com o n.º 1 através da interface técnica criada e gerida pela Agência Europeia da Guarda de Fronteiras e Costeira, como previsto no artigo 49.º, n.º 1.
3. Sempre que uma consulta efetuada por um membro das equipas da Guarda Europeia de Fronteiras e Costeira ou das equipas envolvidas em operações de regresso ou da equipa de apoio à gestão da migração revele a existência de uma indicação no SIS, o Estado-Membro autor da indicação deve ser informado deste facto. Em conformidade com o artigo 40.º do Regulamento (UE) 2016/1624, os membros das equipas só podem atuar em resposta a uma indicação no SIS sob instruções e, regra geral, na presença dos guardas de fronteira ou do pessoal que participa em missões relacionadas com o regresso do Estado-Membro de acolhimento em que operem. O Estado-Membro de acolhimento pode autorizar os membros das equipas a agir em seu nome.
4. Cada acesso e cada consulta que efetue um membro das equipas da Guarda Europeia de Fronteiras e Costeira ou das equipas envolvidas em operações de regresso ou da equipa de apoio à gestão da migração devem ser registados, em conformidade com o disposto no artigo 12.º, bem como cada utilização que façam dos dados a que acederam.

5. O acesso aos dados introduzidos no SIS deve ser limitado a um membro das equipas da Guarda Europeia de Fronteiras e Costeira ou das equipas envolvidas em operações de regresso ou da equipa de apoio à gestão da migração, e não deve ser alargado a nenhum outro membro das equipas.
6. Devem ser adotadas e aplicadas medidas para garantir a segurança e a confidencialidade a que se referem os artigos 10.º e 11.º.

#### *Artigo 49.º*

##### *Acesso aos dados do SIS pela Agência Europeia da Guarda de Fronteiras e Costeira*

1. Para efeitos do artigo 48.º, n.ºs 1 e 2 do presente artigo, a Agência Europeia da Guarda de Fronteiras e Costeira deve criar e gerir uma interface técnica que permita a ligação direta ao SIS Central.
2. A Agência Europeia da Guarda de Fronteiras e Costeira deve, para efeitos do exercício das atribuições que lhe foram conferidas pelo Regulamento que cria o Sistema Europeu de Informação e Autorização de Viagem (ETIAS), ter o direito de aceder e consultar os dados introduzidos no SIS, em conformidade com os artigos 26.º, 32.º, 34.º, 36.º e 38.º, n.º 2, alíneas j) e k).
3. Sempre que uma verificação pela Agência Europeia da Guarda de Fronteiras e Costeira revele a existência de uma indicação no SIS, aplica-se o procedimento previsto no artigo 22.º do Regulamento que cria o Sistema Europeu de Informação e Autorização de Viagem (ETIAS).
4. Nenhuma disposição do presente artigo deve ser interpretada no sentido de afetar o disposto no Regulamento (UE) 2016/1624 no que diz respeito à proteção de dados e à responsabilidade pelo tratamento não autorizado ou incorreto desses dados pela Agência Europeia da Guarda de Fronteiras e Costeira.
5. Cada acesso e consulta efetuados pela Agência Europeia da Guarda de Fronteiras e Costeira devem ser registados, em conformidade com o artigo 12.º, bem como cada utilização que faça dos dados a que acedeu.
6. Exceto quando necessário ao exercício das atribuições previstas para efeitos do Regulamento que cria o Sistema Europeu de Informação e Autorização de Viagem (ETIAS), nenhuma parte do SIS deve ser ligada a outro sistema informático de recolha e tratamento de dados gerido pela Agência Europeia da Guarda de Fronteiras e Costeira, ou que funcione nas suas instalações, nem os dados do SIS aos quais a Agência tenha acedido devem ser transferidos para esse sistema. Nenhuma parte do SIS deve ser descarregada. O registo dos acessos e consultas não deve ser considerado como descarga ou cópia dos dados do SIS.
7. Devem ser adotadas e aplicadas pela Agência Europeia da Guarda de Fronteiras e Costeira medidas para garantir a segurança e a confidencialidade a que se referem os artigos 10.º e 11.º.

#### *Artigo 50.º*

##### *Âmbito do direito de acesso*

Os utilizadores finais, incluindo a Europol, os membros nacionais da Eurojust e os seus assistentes, bem como a Agência Europeia da Guarda de Fronteiras e Costeira, só podem ter acesso aos dados que sejam necessários para o exercício das suas atribuições.



## *Artigo 51.º*

### *Período de conservação das indicações*

1. As indicações inseridas no SIS nos termos do presente regulamento devem ser conservadas apenas durante o período necessário à realização das finalidades para as quais foram inseridas.
2. No prazo de cinco anos a contar da inserção de uma indicação no SIS, o Estado-Membro autor da indicação deve rever a necessidade da sua conservação. As indicações inseridas para efeitos do artigo 36.º do presente regulamento são conservadas pelo período máximo de um ano.
3. As indicações relativas a documentos oficiais em branco e documentos de identidade emitidos, inseridas em conformidade com o artigo 38.º, são conservadas pelo período máximo de 10 anos. Podem ser fixados períodos de conservação mais curtos para categorias de indicações de objetos através de medidas de execução adotadas em conformidade com o procedimento de exame a que se refere o artigo 72.º, n.º 2.
4. Cada Estado-Membro estabelece, se for caso disso, prazos de revisão mais curtos, em conformidade com o seu direito nacional.
5. Nos casos em que resulte evidente para o pessoal do Gabinete SIRENE, responsável pela coordenação e controlo da qualidade dos dados, que a indicação relativa a uma pessoa alcançou o seu objetivo e deve ser suprimida do SIS, notifica deste facto a autoridade autora da indicação. A referida autoridade dispõe de um prazo de 30 dias a contar da receção dessa notificação para comunicar que a indicação foi ou será suprimida, ou para apresentar os motivos para conservar a indicação. Se o prazo de 30 dias expirar sem uma resposta, o pessoal do Gabinete SIRENE suprime a indicação. Os Gabinetes SIRENE devem comunicar quaisquer problemas recorrentes neste domínio às respetivas autoridades nacionais de controlo.
6. O Estado-Membro autor da indicação pode decidir, durante o período de revisão, e na sequência de uma avaliação individual exaustiva que deve ser registada, manter a indicação por um período mais longo, se tal se revelar necessário à realização das finalidades para as quais foi inserida. Neste caso, o n.º 2 também se aplica à prorrogação. Qualquer prorrogação de uma indicação deve ser comunicada ao CS-SIS.
7. As indicações são automaticamente apagadas uma vez expirado o período de revisão a que se refere o n.º 2, exceto no caso de o Estado-Membro autor da indicação ter informado o CS-SIS da prorrogação da indicação por força do n.º 6. O CS-SIS informa automaticamente os Estados-Membros da supressão programada dos dados do sistema, mediante um pré-aviso de quatro meses.
8. Os Estados-Membros devem manter estatísticas sobre o número de indicações cujo período de conservação tenha sido prorrogado em conformidade com o n.º 6.

## CAPÍTULO XIII

### SUPRESSÃO DE INDICAÇÕES

#### *Artigo 52.º*

#### *Supressão de indicações*

1. São suprimidas as indicações inseridas por força do artigo 26.º, tendo em vista a detenção para efeitos de entrega ou extradição, quando a pessoa for entregue às autoridades competentes do Estado-Membro autor da indicação ou extraditada para este Estado. Podem ser igualmente suprimidas quando a decisão judicial em que se baseou a indicação for revogada pela autoridade judiciária competente nos termos do direito nacional.
2. A supressão das indicações relativas a pessoas desaparecidas deve respeitar as seguintes regras:
  - (a) Em relação a crianças desaparecidas, por força do artigo 32.º, a indicação é suprimida:
    - Desde a resolução do caso, por exemplo quando a criança for repatriada ou quando as autoridades competentes do Estado-Membro de execução tomarem uma decisão sobre a guarda da criança;
    - Desde o termo de validade da indicação, em conformidade com o artigo 51.º;
    - Desde a tomada de uma decisão pela autoridade competente do Estado-Membro autor da indicação; ou
    - Desde a localização da criança.
  - b) Em relação a adultos desaparecidos, por força do artigo 32.º, quando não for solicitada qualquer medida de proteção, a indicação é suprimida:
    - Desde a execução da conduta solicitada (paradeiro confirmado pelo Estado-Membro de execução);
    - Desde o termo de validade da indicação, em conformidade com o artigo 51.º; ou
    - Desde a tomada de uma decisão pela autoridade competente do Estado-Membro autor da indicação.
  - c) Em relação a adultos desaparecidos, por força do artigo 32.º, quando forem solicitadas medidas de proteção, a indicação é suprimida:
    - Desde a execução da conduta solicitada (pessoa colocada sob proteção);
    - Desde o termo de validade da indicação, em conformidade com o artigo 51.º; ou
    - Desde a tomada de uma decisão pela autoridade competente do Estado-Membro autor da indicação.

Sob reserva das disposições do direito nacional, quando a pessoa for retida por decisão da autoridade competente, a indicação pode ser mantida até ao repatriamento dessa pessoa.

3. A supressão de indicações relativas a pessoas procuradas no âmbito de processos judiciais deve respeitar as seguintes regras:

Em relação a indicações relativas a pessoas procuradas no âmbito de processos judiciais, por força do artigo 34.º, a indicação é suprimida:

- (a) Desde que o paradeiro da pessoa for comunicado à autoridade competente do Estado-Membro autor da indicação. Sempre que não possa ser dado seguimento às informações comunicadas, o Gabinete SIRENE do Estado-Membro autor da indicação deve informar o Gabinete SIRENE do Estado-Membro de execução para que o problema seja resolvido;
- (b) Desde o termo de validade da indicação, em conformidade com o artigo 51.º; ou
- (c) Desde a tomada de uma decisão pela autoridade competente do Estado-Membro autor da indicação.

Sempre que se obtiver um acerto num Estado-Membro e os dados do endereço forem transmitidos ao Estado-Membro autor da indicação e, posteriormente, outro acerto obtido nesse Estado-Membro revelar o mesmo endereço, este acerto é registado no Estado-Membro de execução mas nem o endereço nem as informações suplementares devem ser reenviados ao Estado-Membro autor da indicação. Nestes casos, o Estado-Membro de execução informa o Estado-Membro autor da indicação sobre esses acertos repetidos, e este último deve avaliar a necessidade de manter a indicação.

4. A supressão de indicações relativas a vigilâncias discretas, controlos de verificação e controlos específicos, deve respeitar as seguintes regras:

Em relação a indicações relativas a vigilâncias discretas, controlos de verificação e controlos específicos, por força do artigo 36.º, a indicação é suprimida:

- (a) Desde o termo de validade da indicação, em conformidade com o artigo 51.º;
- (b) Desde a tomada de uma decisão de supressão pela autoridade competente do Estado-Membro autor da indicação.

5. A supressão de indicações relativas a objetos para efeitos de apreensão ou de utilização como prova, deve respeitar as seguintes regras:

Em relação a indicações relativas a objetos para efeitos de apreensão ou de utilização como prova em processos penais, por força do artigo 38.º, a indicação é suprimida:

- (a) Desde a apreensão do objeto ou medida equivalente, sempre que o necessário intercâmbio consecutivo de informações suplementares tiver lugar entre os Gabinetes SIRENE ou esse objeto for visado por outro procedimento judicial ou administrativo;
- (b) Desde o termo de validade da indicação; ou
- (c) Desde a tomada de uma decisão de supressão pela autoridade competente do Estado-Membro autor da indicação.

6. A supressão das indicações relativas a pessoas procuradas desconhecidas, por força do artigo 40.º, deve respeitar as seguintes regras:

7. a) Desde a identificação da pessoa; ou
8. b) Desde o termo de validade da indicação.

## **CAPÍTULO XIV**

### **REGRAS GERAIS APLICÁVEIS AO TRATAMENTO DE DADOS**

#### *Artigo 53.º*

#### *Tratamento dos dados do SIS*

1. Os Estados-Membros apenas podem tratar os dados referidos no artigo 20.º para os efeitos previstos para cada uma das categoria de indicações referidas nos artigos 26.º, 32.º, 34.º, 36.º, 38.º e 40.º.
2. Os dados só podem ser copiados para fins técnicos desde que essa cópia seja necessária para uma consulta direta pelas autoridades referidas no artigo 43.º. O disposto no presente regulamento é igualmente aplicável às referidas cópias. Um Estado-Membro não pode copiar os dados sobre indicações nem dados adicionais introduzidos por outro Estado-Membro a partir do seu N.SIS ou do CS-SIS para outros ficheiros de dados nacionais.
3. As cópias técnicas referidas no n.º 2, que deem origem a bases de dados fora de linha, podem ser conservadas por um período máximo de 48 horas. Este período pode ser prorrogado numa situação de emergência até que a mesma cesse.
4. Os Estados-Membros devem manter um inventário atualizado dessas cópias, torná-lo acessível às autoridades nacionais de controlo, e assegurar a aplicação a essas cópias das disposições do presente regulamento, em particular o disposto no artigo 10.º.
5. O acesso aos dados do SIS só é autorizado dentro dos limites de competência das autoridades nacionais a que se refere o artigo 43.º, e ao pessoal devidamente autorizado.
6. No que respeita às indicações previstas nos artigos 26.º, 32.º, 34.º, 36.º e 38.º do presente regulamento, qualquer tratamento das informações nelas contidas para finalidades diferentes daquelas para que foram inseridas no SIS tem de estar ligado a um caso específico e justificado pela necessidade de prevenir uma ameaça grave iminente para a ordem e a segurança públicas, por motivos graves de segurança nacional e para efeitos de prevenir um crime grave. Para este efeito, deve ser obtida a autorização prévia do Estado-Membro autor da indicação.
7. Qualquer utilização de dados não conforme com os n.ºs 1 a 6 é considerada indevida ao abrigo do direito nacional de cada Estado-Membro.
8. Os Estados-Membros devem comunicar à Agência a lista das respetivas autoridades competentes autorizadas a consultar diretamente os dados introduzidos no SIS, nos termos do presente regulamento, e as alterações da referida lista. A lista deve especificar, para cada autoridade, os dados que estão autorizadas a consultar e para que finalidades. A Agência assegura a publicação anual da lista no *Jornal Oficial da União Europeia*.
9. Na medida em que o direito da União não preveja disposições específicas, aplica-se o direito de cada Estado-Membro aos dados introduzidos no respetivo N.SIS.

*Artigo 54.º*

*Dados do SIS e ficheiros nacionais*

1. O artigo 53.º, n.º 2, não prejudica o direito de um Estado-Membro conservar, nos seus ficheiros nacionais, os dados do SIS relacionados com medidas tomadas no seu território. Esses dados são mantidos em ficheiros nacionais por um período máximo de três anos, exceto se disposições específicas do direito nacional estabelecerem um período de conservação mais longo.
2. O artigo 53.º, n.º 2, não prejudica o direito de um Estado-Membro manter, em ficheiros nacionais, dados constantes de uma determinada indicação que eles próprios tiverem inserido no SIS.

*Artigo 55.º*

*Informação em caso de não execução de uma indicação*

Se a ação solicitada não puder ser executada, o Estado-Membro requerido informa imediatamente desse facto o Estado-Membro autor da indicação.

*Artigo 56.º*

*Qualidade dos dados tratados no SIS*

1. O Estado-Membro autor de uma indicação é responsável pela exatidão e atualidade dos dados, bem como pela legalidade da introdução no SIS.
2. Apenas o Estado-Membro autor de uma indicação está autorizado a alterar, completar, retificar, atualizar ou suprimir os dados que introduziu.
3. Sempre que um Estado-Membro diferente do Estado autor da indicação dispuser de indícios que o levem a presumir que um dado é factualmente incorreto ou foi ilegalmente introduzido, deve informar deste facto, mediante o intercâmbio de informações suplementares, o Estado-Membro autor da indicação com a maior brevidade possível e, em qualquer caso, no prazo máximo de 10 dias após ter tido conhecimento desses indícios. O Estado-Membro autor da indicação deve verificar tal comunicação e, se necessário, corrigir ou suprimir sem demora o dado em questão.
4. Sempre que os Estados-Membros não conseguirem chegar a acordo no prazo de dois meses a contar da data em que tiveram conhecimento desses indícios pela primeira vez, tal como descrito no n.º 3, o Estado-Membro que não inseriu a indicação submete o caso à apreciação das autoridades nacionais de controlo competentes para que adotem uma decisão.
5. Os Estados-Membros devem proceder ao intercâmbio de informações suplementares sempre que uma pessoa alegue não ser a pessoa procurada através de uma indicação. Se, em resultado dessa verificação, se comprovar que existem efetivamente duas pessoas diferentes, o queixoso deve ser informado das medidas previstas no artigo 59.º.
6. Se uma pessoa já tiver sido objeto de uma indicação no SIS, o Estado-Membro que inserir uma nova indicação deve chegar a acordo sobre a mesma com o Estado-Membro autor da primeira indicação. O acordo deve ser obtido com base no intercâmbio de informações suplementares.

### *Artigo 57.º*

#### *Incidentes de segurança*

1. Qualquer acontecimento que tenha ou possa ter impacto na segurança do SIS e que possa causar-lhe danos ou perdas é considerado um incidente de segurança, especialmente quando possa ter havido acesso 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 de forma a assegurar uma resolução rápida, eficaz e adequada.
3. Os Estados-Membros devem notificar a Comissão, a Agência e a autoridade nacional de controlo dos incidentes de segurança. A Agência deve notificar a Comissão e a Autoridade Europeia para a Proteção de Dados dos incidentes de segurança.
4. As informações relativas a um incidente de segurança que tenham ou possam ter impacto no funcionamento do SIS num Estado-Membro ou na Agência ou na disponibilidade, integridade e confidencialidade dos dados introduzidos ou transmitidos por outros Estados-Membros, são disponibilizadas aos Estados-Membros e comunicadas em conformidade com o plano de gestão de incidentes fornecido pela Agência.

### *Artigo 58.º*

#### *Distinção entre pessoas com características similares*

Sempre que, durante a inserção de uma nova indicação, se verificar que já existe no SIS uma pessoa com os mesmos elementos de descrição da identidade, deve ser adotado o seguinte procedimento:

- (a) O Gabinete SIRENE entra em contacto com a autoridade requerente para esclarecer se se trata da mesma pessoa;
- (b) Sempre que resultar dessa verificação que a pessoa objeto da nova indicação e a pessoa já indicada no SIS é efetivamente a mesma pessoa, o Gabinete SIRENE aplica o procedimento relativo à inserção de indicações múltiplas a que se refere o artigo 56.º, n.º 6. Sempre que resultar da verificação que se trata efetivamente de duas pessoas diferentes, o Gabinete SIRENE valida o pedido de inserção da segunda indicação, acrescentando os elementos necessários para evitar qualquer erro de identificação.

### *Artigo 59.º*

#### *Dados suplementares para tratar os casos de usurpação de identidade*

1. Sempre que seja possível confundir a pessoa efetivamente visada pela indicação e uma pessoa cuja identidade tenha sido usurpada, o Estado-Membro autor da indicação acrescenta na indicação, com o consentimento expresso da pessoa cuja identidade foi usurpada, os dados a ela relativos, a fim de evitar as consequências negativas de um erro de identificação.
2. Os dados relativos a uma pessoa cuja identidade tenha sido usurpada são utilizados exclusivamente para:

- (a) Permitir que a autoridade competente distinga entre a pessoa cuja identidade foi usurpada e a pessoa que é efetivamente visada pela indicação;
  - (b) Permitir que a pessoa cuja identidade foi usurpada comprove a sua identidade e confirme que esta foi usurpada.
3. Para efeitos do presente artigo, só podem ser introduzidos e tratados ulteriormente no SIS os seguintes dados pessoais:
- (a) Apelido(s);
  - (b) Nome(s);
  - (c) Nome(s) à nascença;
  - (d) Apelidos utilizados anteriormente e eventuais pseudónimos possivelmente registados em separado;
  - (e) Características físicas particulares, objetivas e permanentes;
  - (f) Local de nascimento;
  - (g) Data de nascimento;
  - (h) Sexo;
  - (i) Fotografias e imagens faciais;
  - (j) Impressões digitais;
  - (k) Nacionalidade(s);
  - (l) Categoria de documento de identidade da pessoa;
  - (m) País de emissão do documento de identidade da pessoa;
  - (n) Número(s) do documento de identidade da pessoa;
  - (o) Data de emissão do documento de identidade da pessoa;
  - (p) Endereço da vítima;
  - (q) Nome do pai da vítima;
  - (r) Nome da mãe da vítima.
4. As regras técnicas necessárias para a introdução e o tratamento ulterior dos dados referidos no n.º 3, devem ser previstas através de medidas de execução estabelecidas e desenvolvidas em conformidade com o procedimento de exame a que se refere o artigo 72.º, n.º 2.
5. Os dados referidos no n.º 3 devem ser suprimidos ao mesmo tempo que a indicação correspondente, ou antes se a pessoa o solicitar.
6. Os dados referidos no n.º 3 só podem ser consultados pelas autoridades com direito de acesso à indicação correspondente, as quais poderão fazê-lo unicamente para evitar erros de identificação.

*Artigo 60.º*

*Ligações entre indicações*

1. Os Estados-Membros podem criar ligações entre as indicações que inserem no SIS. Essas ligações têm por efeito estabelecer uma relação entre duas ou mais indicações.

2. A criação de uma ligação não afeta a conduta específica a adotar com base em cada indicação que é objeto de ligação, nem o período de conservação de cada uma dessas indicações ligadas.
3. A criação de uma ligação não afeta os direitos de acesso previstos no presente regulamento. As autoridades que não tenham direito de acesso a certas categorias de indicações não podem ver a ligação a uma indicação a que não tenham acesso.
4. Os Estados-Membros devem criar ligações entre indicações quando tal corresponda a uma necessidade operacional.
5. Sempre que um Estado-Membro considerar que a criação por outro Estado-Membro de uma ligação entre indicações é incompatível com o seu direito nacional ou as suas obrigações internacionais, pode tomar as medidas necessárias para impedir o acesso a essa ligação a partir do seu território ou pelas suas autoridades estabelecidas fora do seu território.
6. As regras técnicas necessárias para a ligação de indicações devem ser estabelecidas e desenvolvidas em conformidade com o procedimento de exame a que se refere o artigo 72.º, n.º 2.

#### *Artigo 61.º*

##### *Finalidade e período de conservação das informações suplementares*

1. Os Estados-Membros devem conservar no Gabinete SIRENE uma referência às decisões que originaram a indicação, a fim de apoiar o intercâmbio de informações suplementares.
2. Os dados pessoais guardados em ficheiros pelo Gabinete SIRENE em resultado do intercâmbio de informações são conservados apenas durante o período necessário à realização das finalidades para as quais foram fornecidos. Devem, em qualquer caso, ser suprimidos no prazo máximo de um ano após ter sido suprimida do SIS a indicação correspondente.
3. O disposto no n.º 2 não prejudica o direito de os Estados-Membros manterem em ficheiros nacionais os dados relativos a indicações especiais por si inseridas ou a indicações relativamente às quais tenham sido tomadas medidas no seu território. O prazo durante o qual tais dados podem ser conservados nesses ficheiros é determinado pelo direito nacional.

#### *Artigo 62.º*

##### *Transferência de dados pessoais para terceiros*

Os dados tratados no SIS e as informações suplementares correspondentes na aceção do presente regulamento não podem ser transferidos para países terceiros ou organizações internacionais nem colocados à sua disposição.

#### *Artigo 63.º*

##### *Intercâmbio de dados com a Interpol sobre passaportes roubados, desviados, extraviados ou invalidados*

1. Em derrogação do artigo 62.º, os dados introduzidos no SIS referentes ao número de passaporte, país de emissão e tipo de passaportes roubados, desviados, extraviados ou invalidados podem ser objeto de intercâmbio com membros da Interpol, mediante



o estabelecimento de uma ligação entre o SIS e a base de dados da Interpol relativa a documentos de viagem roubados ou extraviados, desde que seja celebrado um acordo entre a Interpol e a União Europeia. Esse acordo deve prever que a transmissão de dados introduzidos por um Estado-Membro deve ser subordinada ao consentimento desse Estado-Membro.

2. O acordo a que se refere o n.º 1 deve prever que os dados partilhados só são acessíveis a membros da Interpol provenientes de países que assegurem um nível adequado de proteção dos dados pessoais. Antes de celebrar esse acordo, o Conselho deve solicitar à Comissão que se pronuncie sobre a adequação do nível de proteção dos dados pessoais e do respeito pelos direitos e liberdades fundamentais no que se refere ao tratamento dos dados pessoais pela Interpol e pelos países que destacaram membros para a Interpol.
3. O acordo a que se refere o n.º 1 pode igualmente prever que os Estados-Membros tenham acesso, através do SIS, a dados da base de dados da Interpol relativa a documentos de viagem roubados ou extraviados, em conformidade com as disposições do presente regulamento que regem as indicações inseridas no SIS sobre passaportes roubados, desviados, extraviados e invalidados.

## **CAPÍTULO XV**

### **PROTEÇÃO DE DADOS**

#### *Artigo 64.º*

#### *Legislação aplicável*

1. O Regulamento (CE) n.º 45/2001 aplica-se ao tratamento de dados pessoais pela Agência ao abrigo do presente regulamento.
2. O Regulamento (UE) 2016/679 aplica-se ao tratamento de dados pessoais desde que não se apliquem as disposições nacionais de transposição da Diretiva (UE) 2016/680.
3. No que diz respeito ao tratamento de dados pelas autoridades nacionais competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais e execução de sanções penais, incluindo a prevenção de ameaças contra a segurança pública, aplicam-se as disposições nacionais de transposição da Diretiva (UE) 2016/680.

#### *Artigo 65.º*

#### *Direito de acesso, retificação de dados inexatos e supressão de dados ilegalmente armazenados*

1. O direito de os titulares de dados terem acesso aos seus dados introduzidos no SIS e a que tais dados sejam retificados ou apagados, deve ser exercido nos termos do direito do Estado-Membro no qual tal direito seja invocado.
2. Se o direito nacional assim o estabelecer, compete à autoridade nacional de controlo decidir se as informações podem ser comunicadas e em que condições.
3. Um Estado-Membro diferente daquele que emitiu uma indicação só pode comunicar informações sobre tais dados se previamente tiver dado oportunidade a este último

Estado-Membro de tomar posição através do intercâmbio de informações suplementares.

4. Os Estados-Membros devem adotar a decisão de não comunicar informações ao titular dos dados, no todo ou em parte, nos termos do direito nacional, na medida e sempre que tal limitação, parcial ou total, constitua uma medida necessária e proporcionada numa sociedade democrática, tendo devidamente em conta os direitos fundamentais e os interesses legítimos da pessoa interessada, a fim de:
  - (a) Evitar prejudicar os inquéritos, as investigações ou os procedimentos oficiais ou judiciais;
  - (b) Evitar prejudicar a prevenção, deteção, investigação ou repressão de infrações penais ou a execução de sanções penais;
  - (c) Proteger a segurança pública;
  - (d) Proteger a segurança nacional;
  - (e) Proteger os direitos e as liberdades de terceiros.
5. Todas as pessoas têm direito a que sejam retificados os dados factualmente inexatos que lhes digam respeito ou apagados os dados ilegalmente armazenados que lhes digam respeito.
6. A pessoa interessada deve ser informada o mais rapidamente possível e, em todo o caso, no prazo máximo de 60 dias a contar da data em que solicitou o acesso, ou num prazo mais curto se o direito nacional assim o estabelecer.
7. A pessoa interessada deve ser informada do seguimento dado ao exercício dos seus direitos de retificação e de supressão o mais rapidamente possível e, em todo o caso, no prazo máximo de três meses a contar da data em que solicitou a retificação ou a supressão, ou num prazo mais curto se o direito nacional assim o estabelecer.

*Artigo 66.º*  
*Recursos*

1. Qualquer pessoa pode instaurar perante os tribunais ou a autoridade competente, nos termos do direito nacional de qualquer Estado-Membro, uma ação que tenha por objeto aceder, retificar, apagar ou obter informações ou uma indemnização relacionada com uma indicação que lhe diga respeito.
2. Os Estados-Membros comprometem-se mutuamente a executar as decisões definitivas proferidas por tribunais ou autoridades a que se refere o n.º 1 deste artigo, sem prejuízo do disposto no artigo 70.º.
3. A fim de dispor de uma visão geral coerente do funcionamento das vias de recurso, as autoridades nacionais devem desenvolver um sistema estatístico uniforme para a apresentação de relatórios anuais sobre:
  - (a) O número de pedidos de acesso apresentados ao responsável pelo tratamento dos dados, bem como o número de casos em que foi concedido acesso aos dados;
  - (b) O número de pedidos de acesso apresentados à autoridade nacional de controlo, bem como o número de casos em que foi concedido acesso aos dados;

- (c) O número de pedidos de retificação de dados inexatos e de apagamento de dados ilegalmente armazenados ao responsável pelo tratamento de dados, bem como o número de casos em que os dados foram retificados ou apagados;
- (d) O número de pedidos de retificação de dados inexatos e de apagamento de dados ilegalmente armazenados apresentados à autoridade nacional de controlo;
- (e) O número de casos submetidos à apreciação dos tribunais;
- (f) O número de casos em que um tribunal decidiu a favor do requerente em qualquer aspeto do processo;
- (g) Observações respeitantes a casos de reconhecimento mútuo de decisões definitivas proferidas por tribunais ou autoridades de outros Estados-Membros sobre indicações criadas pelo Estado-Membro autor da indicação.

Os relatórios das autoridades nacionais de controlo devem ser reenviados através do mecanismo de cooperação previsto no artigo 69.º.

*Artigo 67.º*  
*Supervisão do N.SIS*

1. Os Estados-Membros devem assegurar que a ou as respetivas autoridades nacionais de controlo designadas e investidas dos poderes a que se refere o capítulo VI da Diretiva (UE) 2016/680, ou o capítulo VI do Regulamento (UE) 2016/679, fiscalizam de forma independente a legalidade do tratamento dos dados pessoais do SIS no seu território, a sua transmissão a partir do seu território e o intercâmbio e o tratamento ulterior de informações suplementares.
2. A autoridade nacional de controlo deve assegurar que é efetuada, no mínimo de quatro em quatro anos, uma auditoria das operações de tratamento de dados no N.SIS de acordo com as normas internacionais de auditoria. Essa auditoria deve ser efetuada pela ou pelas próprias autoridades de controlo ou ser por estas encomendada diretamente a um auditor independente em matéria de proteção de dados. A autoridade nacional de controlo deve, em todos os casos, manter o controlo e assumir as responsabilidades do auditor independente.
3. Os Estados-Membros devem assegurar que a autoridade nacional de controlo dispõe dos meios necessários para desempenhar as funções que lhe são conferidas pelo presente regulamento.

*Artigo 68.º*  
*Supervisão da Agência*

1. A Autoridade Europeia para a Proteção de Dados deve assegurar que as atividades de tratamento de dados pessoais efetuadas pela Agência são realizadas em conformidade com o presente regulamento. Por conseguinte, aplicam-se as disposições sobre as funções e competências previstas pelos artigos 46.º e 47.º do Regulamento (CE) n.º 45/2001.
2. A Autoridade Europeia para a Proteção de Dados deve assegurar que é efetuada, no mínimo de quatro em quatro anos, uma auditoria das atividades de tratamento de dados pessoais da Agência, em conformidade com as normas internacionais de auditoria. O relatório da referida auditoria é enviado ao Parlamento Europeu, ao

Conselho, à Agência, à Comissão e às autoridades nacionais de controlo. A Agência deve ter a possibilidade de apresentar observações antes da adoção do relatório.

*Artigo 69.º*

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

1. As autoridades nacionais de controlo e a Autoridade Europeia para a Proteção de Dados, agindo no âmbito das respetivas competências, devem cooperar ativamente no quadro das suas responsabilidades e assegurar a supervisão coordenada do SIS.
2. Agindo no âmbito das respetivas competências, estas autoridades devem trocar informações relevantes, assistir-se mutuamente na realização de auditorias e inspeções, analisar as dificuldades de interpretação ou aplicação do presente regulamento e de outros atos jurídicos aplicáveis da União, examinar os problemas detetados aquando do exercício de controlo independente ou por ocasião do exercício dos direitos dos titulares dos dados, elaborar propostas harmonizadas tendo em vista encontrar soluções comuns para os eventuais problemas e promover o conhecimento dos direitos em matéria de proteção de dados, na medida necessária.
3. Para efeitos do disposto no n.º 2, as autoridades nacionais de controlo e a Autoridade Europeia para a Proteção de Dados devem reunir-se pelo menos duas vezes por ano, no âmbito do Comité Europeu para a Proteção de Dados instituído pelo Regulamento (UE) 2016/679. Os custos e a assistência associados a essas reuniões são suportados pelo Comité instituído pelo Regulamento (UE) 2016/679. O regulamento interno deve ser aprovado na primeira reunião. Devem ser definidos conjuntamente novos métodos de trabalho em função das necessidades.
4. O Comité instituído pelo Regulamento (UE) 2016/679 transmite ao Parlamento Europeu, ao Conselho e à Comissão, de dois em dois anos, um relatório conjunto de atividades no que respeita à supervisão coordenada.

## **CAPÍTULO XVI**

### **RESPONSABILIDADE**

*Artigo 70.º*

*Responsabilidade*

1. Os Estados-Membros são responsáveis pelos danos eventualmente causados às pessoas em consequência da utilização do N.SIS. O mesmo se verifica quando os danos forem causados pelo Estado-Membro autor da indicação, se este tiver introduzido dados factualmente incorretos ou armazenado dados ilegalmente.
2. Sempre que o Estado-Membro contra o qual uma ação é instaurada não for o Estado-Membro autor da indicação, este último é obrigado a reembolsar, mediante pedido, os montantes pagos a título de indemnização, a menos que a utilização dos dados pelo Estado-Membro que requer o reembolso viole o presente regulamento.
3. Sempre que o incumprimento por um Estado-Membro das obrigações que lhe incumbem por força do presente regulamento causar danos ao SIS, esse Estado-Membro é considerado responsável, a menos que a Agência ou outros Estados-

Membros que participam no SIS não tenham tomado medidas razoáveis para prevenir os danos ou minimizar os seus efeitos.

## **CAPÍTULO XVII**

### **DISPOSIÇÕES FINAIS**

#### *Artigo 71.º*

#### *Acompanhamento e estatísticas*

1. A Agência deve assegurar que estão criados os procedimentos para o controlo do funcionamento do SIS em relação aos objetivos fixados em termos de resultados, relação custo-eficácia, segurança e qualidade do serviço.
2. Para efeitos de manutenção técnica, elaboração de relatórios e estatísticas, a Agência deve ter acesso às informações necessárias relacionadas com as operações de tratamento que se realizam no SIS Central.
3. A Agência deve elaborar estatísticas diárias, mensais e anuais que apresentem o número de registos por categoria de indicação, o número de acertos por categoria de indicação, o número de vezes que o SIS foi consultado e o número de vezes em que se acedeu ao SIS para efeitos de inserção, atualização ou supressão de uma indicação, no total e por Estado-Membro. As estatísticas elaboradas não podem incluir dados pessoais. O relatório estatístico anual deve ser publicado. A Agência deve transmitir igualmente estatísticas anuais sobre a utilização da funcionalidade que permite tornar temporariamente indisponível a consulta de indicações inseridas por força do artigo 26.º do presente regulamento, no total e por Estado-Membro, incluindo eventuais prorrogações do período de indisponibilidade de 48 horas.
4. Os Estados-Membros, bem como a Europol, a Eurojust e a Agência Europeia da Guarda de Fronteiras e Costeira, devem transmitir à Agência e à Comissão as informações necessárias à elaboração dos relatórios referidos nos n.ºs 3, 7 e 8. Estas informações incluem estatísticas separadas sobre o número de consultas efetuadas por ou em nome dos serviços dos Estados-Membros competentes para a emissão dos certificados de matrícula dos veículos e dos serviços dos Estados-Membros competentes para a emissão dos certificados de registo ou a gestão do tráfego de embarcações, incluindo motores de embarcações, aeronaves e contentores. As estatísticas devem também indicar o número de acertos obtidos por categoria de indicações.
5. A Agência deve transmitir aos Estados-Membros, à Comissão, à Europol, à Eurojust e à Agência Europeia da Guarda de Fronteiras e Costeira os relatórios estatísticos que elabora. A fim de controlar a aplicação dos atos jurídicos da União, a Comissão deve poder solicitar à Agência a transmissão de outros relatórios estatísticos específicos, de forma periódica ou pontualmente, sobre o funcionamento ou a utilização do SIS e sobre a comunicação SIRENE.
6. Para efeitos dos n.ºs 3, 4 e 5 deste artigo e do artigo 15.º, n.º 5, a Agência deve criar, implementar e alojar um repositório central nas suas instalações técnicas que contenha os dados referidos no n.º 3 deste artigo e no artigo 15.º, n.º 5, que impossibilite a identificação de pessoas, mas permita que a Comissão e as agências

referidas no n.º 5 obtenham os referidos relatórios e estatísticas. A Agência deve conceder o acesso ao repositório central aos Estados-Membros, à Comissão, à Europol, à Eurojust e à Agência Europeia da Guarda de Fronteiras e Costeira graças a um meio de acesso seguro através da infraestrutura de comunicação com controlo de acesso e perfis de utilizador específicos unicamente para efeitos da apresentação de relatórios e estatísticas.

Devem ser adotadas normas pormenorizadas sobre o funcionamento do repositório central e normas sobre a proteção e segurança de dados aplicáveis ao repositório através de medidas de execução adotadas em conformidade com o procedimento de exame a que se refere o artigo 72.º, n.º 2.

7. Dois anos após o início do funcionamento do SIS e, subsequentemente, de dois em dois anos, a Agência apresenta ao Parlamento Europeu e ao Conselho um relatório sobre o funcionamento técnico do SIS Central e da infraestrutura de comunicação, incluindo sobre a sua segurança e o intercâmbio bilateral e multilateral de informações suplementares entre Estados-Membros.
8. Três anos após o início do funcionamento do SIS e, subsequentemente, de quatro em quatro anos, a Comissão apresenta uma avaliação global do SIS Central e do intercâmbio bilateral e multilateral de informações suplementares entre Estados-Membros. Essa avaliação global deve incluir uma análise dos resultados obtidos relativamente aos objetivos fixados e uma avaliação sobre se os princípios de base continuam válidos, bem como sobre a aplicação do presente regulamento a respeito do SIS Central, da segurança do SIS Central e das implicações para as operações futuras. A Comissão deve transmitir a avaliação ao Parlamento Europeu e ao Conselho.

#### *Artigo 72.º*

##### *Procedimento de comité*

1. A Comissão é assistida por um comité nos termos do Regulamento (UE) n.º 182/2011.
2. Sempre que se faça referência ao presente número, aplica-se o artigo 5.º do Regulamento (UE) n.º 182/2011.

#### *Artigo 73.º*

##### *Alterações ao Regulamento (UE) n.º 515/2014*

O Regulamento (UE) n.º 515/2014<sup>76</sup> é alterado do seguinte modo:

No artigo 6.º, é inserido o seguinte n.º 6:

«6. Durante a fase de desenvolvimento, os Estados-Membros recebem uma dotação suplementar de 36,8 milhões de EUR para ser distribuída através de um montante fixo para a sua atribuição de base, devendo afetar integralmente este financiamento aos sistemas nacionais do SIS para assegurar a sua modernização rápida e efetiva em consonância com a implementação do SIS Central, tal como previsto no Regulamento (UE) 2018/...<sup>\*</sup> e no Regulamento (UE) 2018/...<sup>\*\*</sup>

---

<sup>76</sup> 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 (JO L 150 de 20.5.2014, p. 143).

*\*Regulamento relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen (SIS) no domínio da cooperação policial e judiciária em matéria penal e Regulamento (JO...)*

*\*\*Regulamento (UE 2018/...relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen (SIS) no domínio dos controlos das fronteiras e Regulamento (JO...)».*

*Artigo 74.º  
Revogação*

A partir da data de aplicação do presente regulamento são revogados os seguintes atos jurídicos:

Regulamento (CE) n.º 1986/2006 do Parlamento Europeu e do Conselho, de 20 de dezembro de 2006, relativo ao acesso ao Sistema de Informação de Schengen de segunda geração (SIS II) dos serviços dos Estados-Membros competentes para a emissão dos certificados de matrícula dos veículos;

Decisão 533/2007/JAI do Conselho, de 12 de julho de 2007, relativa ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação Schengen de segunda geração (SIS II).

Decisão 2010/261/UE da Comissão, de 4 de maio de 2010, relativa ao plano de segurança para o SIS II Central e a infraestrutura de comunicação<sup>77</sup>.

*Artigo 75.º  
Entrada em vigor e aplicabilidade*

1. O presente regulamento entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.
2. O presente regulamento é aplicável a partir da data fixada pela Comissão, depois de:
  - (a) Terem sido adotadas as medidas de execução necessárias;
  - (b) Os Estados-Membros terem notificado a Comissão de que adotaram as disposições técnicas e jurídicas necessárias para efetuar o tratamento de dados do SIS e proceder ao intercâmbio de informações suplementares nos termos do presente regulamento;
  - (c) A Agência ter notificado a Comissão da conclusão de todas as atividades de teste com o CS-SIS e a interação entre o CS-SIS e os N.SIS.
3. O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros, em conformidade com o Tratado sobre o Funcionamento da União Europeia.

---

<sup>77</sup> Decisão 2010/261/UE da Comissão, de 4 de maio de 2010, relativa ao plano de segurança para o SIS II Central e a infraestrutura de comunicação (JO L 112 de 5.5.2010, p. 31).

Feito em Bruxelas, em

*Pelo Parlamento Europeu  
O Presidente*

*Pelo Conselho  
O Presidente*



## **FICHA FINANCEIRA LEGISLATIVA**

### **1. CONTEXTO DA PROPOSTA/INICIATIVA**

- 1.1. Denominação da proposta/iniciativa
- 1.2. Domínio(s) de intervenção abrangido(s) segundo a estrutura ABM/ABB
- 1.3. Natureza da proposta/iniciativa
- 1.4. Objetivo(s)
- 1.5. Justificação da proposta/iniciativa
- 1.6. Duração e impacto financeiro
- 1.7. Modalidade(s) de gestão prevista(s)

### **2. MEDIDAS DE GESTÃO**

- 2.1. Regras em matéria de acompanhamento e prestação de informações
- 2.2. Sistema de gestão e de controlo
- 2.3. Medidas de prevenção de fraudes e irregularidades

### **3. IMPACTO FINANCEIRO ESTIMADO DA PROPOSTA/INICIATIVA**

- 3.1. Rubrica(s) do quadro financeiro plurianual e rubrica(s) orçamental(ais) de despesa(s) envolvida(s)
- 3.2. Impacto estimado nas despesas
  - 3.2.1. *Síntese do impacto estimado nas despesas*
  - 3.2.2. *Impacto estimado nas dotações operacionais*
  - 3.2.3. *Impacto estimado nas dotações de natureza administrativa*
  - 3.2.4. *Compatibilidade com o atual quadro financeiro plurianual*
  - 3.2.5. *Participação de terceiros no financiamento*
- 3.3. Impacto estimado nas receitas

## FICHA FINANCEIRA LEGISLATIVA

### 1. CONTEXTO DA PROPOSTA/INICIATIVA

#### 1.1. Denominação da proposta/iniciativa

Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO 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 o Regulamento (UE) n.º 515/2014 e revoga o Regulamento (CE) n.º 1986/2006, a Decisão 2007/533/JAI do Conselho e a Decisão 2010/261/UE da Comissão

#### 1.2. Domínio(s) de intervenção abrangido(s) segundo a estrutura ABM/ABB<sup>78</sup>

Domínio de intervenção: Migração e Assuntos Internos (título 18)

#### 1.3. Natureza da proposta/iniciativa

- A proposta/iniciativa refere-se a **uma nova ação**
- A proposta/iniciativa refere-se a **uma nova ação na sequência de um projeto-piloto/ação preparatória**<sup>79</sup>
- A proposta/iniciativa refere-se à **prorrogação de uma ação existente**
- A proposta/iniciativa refere-se à **uma ação reorientada para uma nova ação**

#### 1.4. Objetivo(s)

##### 1.4.1. *Objetivo(s) estratégico(s) plurianual(ais) da Comissão visado(s) pela proposta/iniciativa*

Objetivo – «Combater a criminalidade organizada»

Objetivo – «Uma resposta firme da UE com vista a lutar contra o terrorismo e prevenir a radicalização»

A Comissão tem insistido, em diversas ocasiões, para a necessidade de rever a base jurídica do SIS para dar resposta aos novos desafios de segurança e de migração. A título de exemplo, na «Agenda Europeia para a Segurança»<sup>80</sup> a Comissão anunciou a sua intenção de avaliar o SIS em 2015-2016 e examinar se existem novas necessidades operacionais que exijam alterações legislativas. Além disso, a referida agenda salientou que o SIS está no cerne do intercâmbio de informações policiais, preconizando um reforço acrescido do sistema. Mais recentemente, na sua comunicação intitulada «Sistemas de informação mais sólidos e mais inteligentes para controlar as fronteiras e garantir a segurança»<sup>81</sup>, a Comissão referiu que seriam analisadas funcionalidades adicionais do sistema com base no relatório da avaliação global, com vista a apresentar propostas de revisão da base jurídica do SIS. Por último, em 20 de abril de 2016, na sua comunicação intitulada «Dar cumprimento à Agenda Europeia para a Segurança para combater o terrorismo e abrir caminho à

<sup>78</sup> ABM: *Activity Based Management* (gestão por atividades); ABB: *Activity Based Budgeting* (orçamentação por atividades).

<sup>79</sup> Tal como referido no artigo 54.º, n.º 2, alínea a) ou b), do Regulamento Financeiro.

<sup>80</sup> COM(2015) 185 final.

<sup>81</sup> COM(2016) 205 final.

criação de uma União da Segurança genuína e eficaz»<sup>82</sup>, a Comissão propôs uma série de alterações ao SIS a fim de melhorar o seu valor acrescentado para fins de aplicação coerciva da lei.

A avaliação global, realizada pela Comissão, confirmou que o SIS constitui um êxito operacional. Contudo, não obstante os seus vários aspetos bem-sucedidos, a avaliação também formulou uma série de recomendações, com o intuito de promover a eficácia e eficiência nos planos técnico e operacional do sistema.

Com base nas recomendações constantes do relatório da avaliação global e em total consonância com os objetivos da Comissão enunciados nas comunicações acima mencionadas e no Plano Estratégico 2016-2020 da DG Migração e Assuntos Internos<sup>83</sup>, a presente proposta visa implementar:

- O anúncio da Comissão de que vai reforçar o valor acrescentado do SIS para fins de aplicação coerciva da lei, a fim de responder às novas ameaças;
- As recomendações sobre modificações técnicas e processuais, decorrentes de uma avaliação exaustiva do SIS;
- Os pedidos dos utilizadores finais relativamente à introdução de aperfeiçoamentos técnicos;
- As conclusões preliminares do Grupo de Peritos de Alto Nível em matéria de Sistemas de Informação e Interoperabilidade no que respeita à qualidade dos dados.

*1.4.2. Objetivo(s) específico(s) e atividade(s) ABM/ABB em causa*

Objetivo específico n.º

Plano de Gestão da DG Migração e Assuntos Internos para 2017

Objetivo específico 2.1 – Uma resposta firme da UE com vista a lutar contra o terrorismo e prevenir a radicalização;

Objetivo específico 2.2 – Combater a criminalidade transnacional grave e organizada.

Atividade(s) ABM/ABB em causa

Capítulo 18 02 – Segurança Interna

<sup>82</sup> COM(2016) 230 final.

<sup>83</sup> Ares(2016)2231546 – 12/05/2016.

### 1.4.3. Resultados e impacto esperados

*Especificar os efeitos que a proposta/iniciativa poderá ter nos beneficiários/na população visada.*

O objetivo primordial das alterações jurídicas e técnicas propostas no SIS consiste em tornar o sistema mais eficaz no plano operacional. A avaliação global do SIS, realizada pela DG HOME em 2015-2016, recomendou aperfeiçoamentos técnicos do sistema e uma harmonização dos procedimentos nacionais no domínio da cooperação em matéria de aplicação coerciva da lei.

A nova proposta cria medidas que respondem às necessidades operacionais e técnicas dos utilizadores finais. Concretamente, os novos campos de dados para as indicações já existentes permitirão que os agentes de polícia tenham à sua disposição todas as informações necessárias para o desempenho eficaz das suas tarefas. Além disso, a proposta destaca especificamente a importância da disponibilidade ininterrupta do SIS, já que os períodos de inatividade podem afetar significativamente o trabalho dos agentes com funções coercivas. Além disso, a presente proposta prevê modificações técnicas que vão tornar o sistema mais eficiente e simples.

Após serem adotadas e postas em prática, as presentes propostas aumentarão a continuidade das atividades, pois os Estados-Membros serão obrigados a dispor de uma cópia nacional integral ou parcial e de um sistema de salvaguarda. Deste modo, o sistema poderá manter-se totalmente funcional e operacional para os agentes no terreno.

A proposta introduz novos identificadores biométricos – impressões palmares, imagens faciais e perfis de ADN – em casos específicos e limitados. Combinada com as alterações previstas aos artigos 32.º e 33.º (indicações relativas a pessoas desaparecidas) no sentido de autorizar a inserção de indicações preventivas e a categorização dos casos de pessoas desaparecidas, esta inovação permitirá, em primeiro lugar, um reforço significativo da proteção dos menores não acompanhados e, em segundo lugar, a sua identificação com base nos perfis de ADN dos próprios ou dos seus pais e/ou irmãos (com o seu consentimento).

As autoridades dos Estados-Membros terão igualmente a possibilidade de emitir indicações relativamente a indivíduos desconhecidos procurados devido a um crime, exclusivamente com base em impressões digitais ou impressões palmares latentes ou encontradas no local de um crime. Esta opção não é possível ao abrigo do atual quadro jurídico e técnico e, por conseguinte, representa uma importante evolução.

### 1.4.4. Indicadores de resultados e de impacto

*Especificar os indicadores que permitem acompanhar a execução da proposta/iniciativa.*

Durante a melhoria do sistema:

Após a aprovação da proposta e a adoção das especificações técnicas, o SIS será objeto de um aperfeiçoamento para aprofundar a harmonização dos procedimentos nacionais relativos à utilização do sistema, alargar o âmbito de aplicação do sistema, através da introdução de novos elementos nas categorias de indicações existentes, e introduzir alterações técnicas destinadas a melhorar a segurança e ajudar a reduzir a carga administrativa. A eu-LISA, a quem competirá coordenar a gestão do projeto de melhoria do sistema, estabelecerá uma estrutura de gestão de projeto e fornecerá um calendário pormenorizado, com metas relativas à aplicação das alterações propostas, o que permitirá à Comissão um acompanhamento rigoroso da execução da proposta.

Objetivo específico – Entrada em serviço das funcionalidades atualizadas do SIS em 2020

Indicador – realização bem-sucedida de testes de pré-lançamento completos do sistema revisto.

Quando o sistema estiver operacional:

Quando o sistema estiver operacional, a eu-LISA assegurará o estabelecimento de procedimentos para acompanhar o funcionamento do Sistema de Informação de Schengen relativamente aos objetivos fixados em termos de resultados, relação custo-eficácia, segurança e qualidade do serviço. Dois anos após o início do funcionamento do SIS e, subsequentemente, de dois em dois anos, compete à eu-LISA apresentar ao Parlamento Europeu e ao Conselho um relatório sobre o funcionamento técnico do SIS Central e da infraestrutura de comunicação, incluindo a sua segurança, e sobre o intercâmbio bilateral e multilateral de informações suplementares entre os Estados-Membros. Além disso, a eu-LISA deve elaborar estatísticas diárias, mensais e anuais de que constem o número de registos por categoria de indicações, o número anual de acertos por categoria de indicações, o número de consultas no SIS e o número de acessos ao sistema para fins de inserção, atualização ou supressão de indicações sob a forma de totais e repartidos por Estado-Membro. Além disso, caberá igualmente à Agência fornecer estatísticas anuais sobre a utilização da funcionalidade que torna uma indicação emitida ao abrigo do artigo 26.º do presente regulamento temporariamente não consultável, sob a forma de totais e repartidas por Estado-Membro, incluindo eventuais prorrogações do período de conservação de 48 horas.

Três anos após o início do funcionamento do SIS e, subsequentemente, de quatro em quatro anos, a Comissão apresenta uma avaliação global do SIS Central e do intercâmbio bilateral e multilateral de informações suplementares entre os Estados-Membros. Essa avaliação global inclui uma análise dos resultados obtidos relativamente aos objetivos fixados, avalia se os princípios subjacentes continuam a ser válidos, faz o ponto da situação sobre a aplicação do presente regulamento ao SIS Central e a segurança proporcionada por este sistema as eventuais implicações para o funcionamento futuro. A Comissão transmitirá a avaliação ao Parlamento Europeu e ao Conselho.

Objetivo específico 1 – Combater a criminalidade organizada.

Indicador – Utilização de mecanismos de intercâmbio de informações da UE. Este indicador pode ser avaliado em função do aumento do número de acertos obtidos no SIS. Os indicadores consistem em relatórios estatísticos publicados pela eu-LISA e pelos Estados-Membros. Permitirão à Comissão avaliar a forma como estão a ser utilizadas as novas funcionalidades do sistema.

Objetivo específico 2 – Uma resposta firme da UE com vista a lutar contra o terrorismo e prevenir a radicalização.

Indicador – Aumento do número de indicações e acertos, particularmente quanto ao artigo 36.º, n.º 3, da proposta no que respeita às indicações relativas a pessoas e objetos para efeitos de vigilância discreta, controlo de verificação ou controlo específico.

## 1.5. Justificação da proposta/iniciativa

### 1.5.1. *Necessidade(s) a satisfazer a curto ou a longo prazo*

1. Contribuir para manter um elevado nível de segurança no espaço de liberdade, de segurança e de justiça da UE;
2. Harmonizar mais eficazmente os procedimentos nacionais relativos à utilização do SIS;
3. Ampliar a lista de utilizadores institucionais com acesso aos dados do SIS, facultando um acesso integral ao sistema por parte da Europol e da nova Guarda Europeia de Fronteiras e Costeira;
4. Instituir novos elementos nas indicações do SIS e novas funcionalidades, a fim de alargar o âmbito de aplicação do sistema, permitir que este dê resposta ao atual clima de segurança, reforçar a cooperação entre as autoridades com funções coercivas e as autoridades responsáveis pela segurança dos Estados-Membros e reduzir a carga administrativa;
5. Cobrir a utilização integral de extremo a extremo do SIS, não só dos sistemas central e nacionais, mas também garantindo que os utilizadores finais recebem todos os dados necessários ao exercício das suas funções;
6. Reforçar a continuidade das atividades e assegurar o funcionamento ininterrupto do SIS aos níveis central e nacional;
7. Promover a luta contra a criminalidade internacional, o terrorismo e a cibercriminalidade, como domínios interligados e com forte dimensão transnacional.

### 1.5.2. *Valor acrescentado da participação da UE*

O SIS é, na Europa, a principal base de dados em matéria de segurança. Na ausência de controlos nas fronteiras internas, a luta efetiva contra a criminalidade e o terrorismo ganhou uma dimensão europeia. Os objetivos da proposta referem-se a melhorias técnicas com vista a promover a eficiência e a eficácia do sistema, bem como harmonizar a sua utilização em todos os Estados-Membros participantes. A natureza transnacional destas metas, a par dos desafios relativos a um intercâmbio de informações eficaz que combata as ameaças em constante mutação, significa que a UE está especialmente bem posicionada para propor soluções para estes problemas. Os objetivos de promoção da eficiência e de uma utilização harmonizada do SIS, nomeadamente o aumento do volume, da qualidade e da rapidez do intercâmbio de informações por intermédio de um sistema de informação centralizado e de grande escala, gerido por uma agência reguladora (eu-LISA), não podem ser atingidos pelos Estados-Membros isoladamente, exigindo uma intervenção ao nível da UE. Se estas questões não forem tratadas, o SIS continuará a funcionar de acordo com as regras atualmente aplicáveis, gorando, assim, as oportunidades de maximizar a eficiência e o valor acrescentado da UE, identificadas na avaliação do SIS e da sua utilização pelos Estados-Membros.

Só em 2015, as autoridades competentes dos Estados-Membros acederam ao sistema em quase 2,9 mil milhões de ocasiões, o que demonstra de forma clara a contribuição fulcral do sistema para a cooperação em matéria de aplicação coerciva da lei no espaço Schengen. Este grande volume de intercâmbio de informações entre os Estados-Membros não teria sido alcançado por meio de soluções nacionais descentralizadas e não teria sido possível obter estes resultados ao nível dos Estados-

Membros. Além disso, o SIS demonstrou ser o instrumento de intercâmbio de informações mais eficaz para fins de luta contra o terrorismo e gera valor acrescentado da UE, ao permitir que os serviços de segurança nacionais cooperem de modo rápido, confidencial e eficiente. As novas propostas proporcionarão um intercâmbio de informações e uma cooperação mais fácil entre os Estados-Membros da UE. Além disso, no âmbito das respetivas competências, a Europol e a nova Agência Europeia da Guarda de Fronteiras e Costeira passarão a dispor de um acesso integral ao sistema, um sinal inequívoco do valor acrescentado gerado pela participação da UE.

### 1.5.3. *Lições retiradas de experiências anteriores semelhantes*

1. A fase de desenvolvimento deve arrancar somente depois de as necessidades operacionais e os requisitos dos utilizadores finais estarem totalmente definidos. O desenvolvimento apenas poderá ser efetuado uma vez definitivamente adotados os instrumentos jurídicos subjacentes, relativos à definição do seu objeto, âmbito de aplicação, funções e características técnicas.

2. A Comissão procedeu (e continua a proceder) a consultas regulares das partes interessadas, incluindo delegados do Comité SIS-VIS, no âmbito do procedimento de comitologia. Este comité conta com os representantes dos Estados-Membros quer para questões operacionais ligadas às SIRENE (cooperação transfronteiriça em relação ao SIS) quer para questões técnicas sobre o desenvolvimento e a manutenção do SIS e a aplicação SIRENE conexas. As alterações propostas pelo presente regulamento têm sido analisadas de forma muito transparente e exaustiva em reuniões e sessões de trabalho temáticas. Internamente, a Comissão criou um grupo diretor interserviços, que engloba o Secretariado-Geral e as Direções-Gerais da Migração e dos Assuntos Internos, da Justiça e dos Consumidores, dos Recursos Humanos e da Segurança, e da Informática. Este grupo diretor acompanhou o processo de avaliação e formulou orientações sempre que necessário.

3. A Comissão também recorreu a conhecimentos especializados externos, materializados em dois estudos, cujas conclusões foram incorporadas na elaboração da presente proposta:

- Avaliação Técnica do SIS – a avaliação identificou os principais problemas respeitantes ao SIS e as necessidades que importará ter em conta no futuro; assinalou as preocupações relativas à maximização da continuidade das atividades e à efetiva adaptação da arquitetura global ao aumento das exigências de capacidade;

- Avaliação de impacto de possíveis aperfeiçoamentos da arquitetura do SIS II no âmbito das TIC (*ICT Impact Assessment of Possible Improvements to the SIS II Architecture*) – o estudo avaliou os custos atuais do funcionamento do SIS ao nível nacional e ponderou três possíveis cenários técnicos de aperfeiçoamento do sistema. Todos os cenários abrangem um conjunto de propostas técnicas que incidem em aperfeiçoamentos do sistema central e da arquitetura global.

### 1.5.4. *Compatibilidade e eventual sinergia com outros instrumentos adequados*

A presente proposta deve ser encarada como a implementação das ações mencionadas na Comunicação, de 6 de abril de 2016, intitulada «Sistemas de informação mais sólidos e mais inteligentes para controlar as fronteiras e garantir a

segurança»<sup>84</sup>, que destaca a necessidade de a UE reforçar e melhorar os seus sistemas informáticos, a sua arquitetura de dados e o seu intercâmbio de informações nos domínios da aplicação coerciva da lei, da luta contra o terrorismo e da gestão das fronteiras.

Além disso, a presente proposta está estreitamente associada a outras políticas da União, que complementa, ou seja:

a) A segurança interna, tal como sublinhado na Agenda Europeia para a Segurança<sup>85</sup>, para efeitos de prevenir, detetar, investigar e julgar crimes graves e atos terroristas, dando às autoridades com funções coercivas a possibilidade de tratar dados pessoais de indivíduos suspeitos de estarem implicados em atos terroristas ou crimes graves;

b) A proteção dos dados, na medida em que a presente proposta deve garantir a proteção dos direitos fundamentais de respeito da vida privada dos indivíduos cujos dados pessoais são tratados no SIS.

A proposta é, por outro lado, compatível com a legislação em vigor da União, ou seja:

a) A Guarda Europeia de Fronteiras e Costeira<sup>86</sup> no que se refere, em primeiro lugar, à possibilidade de o pessoal da Agência efetuar análises de risco e, em segundo lugar, aceder ao SIS para os fins do ETIAS proposto. A proposta visa igualmente fornecer uma interface técnica de acesso ao SIS, a fim de garantir aos membros das equipas da Guarda Europeia de Fronteiras e Costeira, das equipas envolvidas em operações de regresso, bem como das equipas de apoio à gestão da migração, o direito de, no âmbito dos seus mandatos, acederem e consultarem dados introduzidos no SIS;

b) A Europol, na medida em que a presente proposta confere à Europol direitos adicionais de acesso e consulta de dados introduzidos no SIS, no âmbito do seu mandato;

c) O Tratado de Prüm<sup>87</sup>, na medida em que os desenvolvimentos da presente proposta visando permitir a identificação de pessoas com base em impressões digitais (assim como imagens faciais e perfis de ADN) complementem as disposições em vigor do Tratado de Prüm sobre o acesso mútuo transfronteiras em linha a bases de dados nacionais designadas de perfis de ADN e aos sistemas automatizados de identificação por impressões digitais.

A proposta é, por outro lado, compatível com a legislação futura da União, ou seja:

<sup>84</sup> COM(2016) 205 final.

<sup>85</sup> COM(2015) 185 final.

<sup>86</sup> 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).

<sup>87</sup> Decisão 2008/615/JAI do Conselho, de 23 de junho de 2008, relativa ao aprofundamento da cooperação transfronteiras, em particular no domínio da luta contra o terrorismo e a criminalidade transfronteiras (JO L 210 de 6.8.2008, p. 1); e Decisão 2008/616/JAI do Conselho, de 23 de junho de 2008, referente à execução da Decisão 2008/615/JAI, relativa ao aprofundamento da cooperação transfronteiras, em particular no domínio da luta contra o terrorismo e da criminalidade transfronteiras (JO L 210 de 6.8.2008, p. 12).



- a) A gestão das fronteiras externas. A proposta complementa o novo princípio previsto no Código das Fronteiras Schengen que consiste na realização de controlos sistemáticos, a partir das bases de dados pertinentes, de todos os viajantes, incluindo cidadãos da UE, à entrada e à saída do espaço Schengen, em resposta ao fenómeno dos combatentes terroristas estrangeiros;
- b) O Sistema de Entrada/Saída<sup>88</sup> (EES), na medida em que a presente proposta visa refletir a utilização proposta de uma combinação de impressões digitais e imagens faciais enquanto identificadores biométricos para fins de funcionamento do EES;
- c) O ETIAS, na medida em que a presente proposta tem em conta a proposta de criação do ETIAS que prevê sujeitar os nacionais de países terceiros que pretendem viajar para a UE a uma avaliação completa de segurança, incluindo através de uma verificação no SIS.

---

<sup>88</sup> Proposta de regulamento do Parlamento Europeu e do Conselho que estabelece o Sistema de Entrada/Saída (EES) para registo dos dados das entradas e saídas e dos dados das recusas de entrada dos nacionais de países terceiros aquando da passagem das fronteiras externas dos Estados-Membros da União Europeia, que determina as condições de acesso ao EES para efeitos de aplicação da lei e que altera o Regulamento (CE) n.º 767/2008 e o Regulamento (UE) n.º 1077/2011 (COM(2016) 194 final).

## 1.6. Duração e impacto financeiro

- Proposta/iniciativa de **duração limitada**
  - Proposta/iniciativa válida entre [DD/MM]AAAA e [DD/MM]AAAA
  - Impacto financeiro no período compreendido entre AAAA e AAAA
- Proposta/iniciativa de **duração ilimitada**
  - Período preparatório de 2017
  - Aplicação com um período de arranque entre 2018 e 2020,
  - seguido de um período de aplicação a um ritmo de cruzeiro.

## 1.7. Modalidade(s) de gestão prevista(s)<sup>89</sup>

- Gestão direta** por parte da Comissão
  - por parte dos seus serviços, incluindo do seu pessoal nas delegações da União;
  - pelas agências de execução
- Gestão partilhada** com os Estados-Membros
- Gestão indireta**, confiando tarefas de execução orçamental:
  - a países terceiros ou aos organismos por estes designados;
  - às organizações internacionais e respetivas agências (a especificar);
  - ao BEI e ao Fundo Europeu de Investimento;
  - aos organismos referidos nos artigos 208.º e 209.º do Regulamento Financeiro;
  - aos organismos de direito público;
  - aos organismos regidos pelo direito privado com uma missão de serviço público na medida em que prestem garantias financeiras adequadas;
  - aos organismos regidos pelo direito privado de um Estado-Membro com a responsabilidade pela execução de uma parceria público-privada e que prestem garantias financeiras adequadas;
  - a pessoas encarregadas da execução de ações específicas no quadro da PESC por força do título V do Tratado da União Europeia, identificadas no ato de base pertinente.
- *Se for indicada mais de uma modalidade de gestão, queira especificar na secção «Observações».*

### Observações

A Comissão será responsável pela gestão global da política em apreço e a eu-LISA será responsável pelo desenvolvimento, funcionamento e manutenção do sistema.

**O SIS constitui um sistema de informação único. Como tal, as despesas previstas em duas das propostas (a presente proposta e a proposta de regulamento relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen (SIS) no domínio dos controlos das fronteiras) não devem ser tidas em conta como dois montantes distintos, mas antes como um montante único. A incidência orçamental das**

<sup>89</sup> As explicações sobre as modalidades de gestão e as referências ao Regulamento Financeiro estão disponíveis no sítio BudgWeb: [http://www.cc.cec/budg/man/budgmanag/budgmanag\\_en.html](http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html)

**alterações necessárias para a implementação das duas propostas está incluída numa  
única ficha financeira legislativa.**

## **2. MEDIDAS DE GESTÃO**

### **2.1. Regras em matéria de acompanhamento e prestação de informações**

*Especificar a periodicidade e as condições.*

A Comissão, os Estados-Membros e a Agência avaliarão e acompanharão regularmente a utilização do SIS, a fim de garantir que continua a funcionar com eficácia e eficiência. A Comissão será assistida pelo Comité na aplicação das medidas técnicas e operacionais, conforme descrito na presente proposta.

Além disso, a presente proposta de regulamento prevê (artigo 71.º, n.ºs 7 e 8) um processo de revisão e avaliação formal e periódico.

De dois em dois anos, a eu-LISA deve apresentar ao Parlamento Europeu e ao Conselho um relatório sobre o funcionamento técnico do SIS, incluindo sobre a segurança, a infraestrutura de comunicação que o apoia e o intercâmbio bilateral e multilateral de informações suplementares entre os Estados-Membros.

Além disso, de quatro em quatro anos, a Comissão deve realizar e partilhar com o Parlamento e o Conselho, uma avaliação global do SIS e do intercâmbio de informações entre os Estados-Membros, com as seguintes finalidades:

- a) Aferir os resultados obtidos relativamente aos objetivos fixados;
- b) Avaliar se os princípios subjacentes continuam a ser válidos;
- c) Analisar a forma como o regulamento é aplicado ao sistema central;
- d) Avaliar a segurança do sistema central;
- e) Explorar as implicações para o funcionamento do sistema no futuro.

Além disso, a eu-LISA passa a ter de facultar estatísticas diárias, mensais e anuais sobre a utilização do SIS, assegurando um acompanhamento constante do sistema e do seu funcionamento comparativamente com os seus objetivos.

### **2.2. Sistema de gestão e de controlo**

#### **2.2.1. *Risco(s) identificado(s)***

Foram identificados os seguintes riscos.

1. Potenciais dificuldades para a eu-LISA na gestão dos desenvolvimentos apresentados na presente proposta em paralelo com outros desenvolvimentos em curso (p. ex., a implementação do AFIS no SIS) e desenvolvimentos futuros (p. ex., o Sistema de Entrada/Saída, o ETIAS e a melhoria do Eurodac). Este risco pode ser mitigado através da afetação à eu-LISA de pessoal e recursos suficientes para o exercício destas atribuições e assegurar a gestão corrente do contratante encarregado da manutenção em estado de funcionamento (MWO).

2. Dificuldades para os Estados-Membros:

2.1 Estas dificuldades são principalmente de cariz financeiro. Por exemplo, as propostas legislativas incluem a elaboração obrigatória de uma cópia nacional parcial em cada N.SIS II. Os Estados-Membros que ainda não tenham elaborado uma cópia terão de realizar esse investimento. Analogamente, a implementação do Documento de Controlo das Interfaces deve ser completada. Os Estados-Membros que ainda não o tenham implementado terão de prever a dotação correspondente nos orçamentos dos ministérios competentes. Este risco pode ser mitigado através da disponibilização

de verbas da UE aos Estados-Membros, por exemplo, provenientes da componente «Fronteiras» do Fundo para a Segurança Interna (FSI).

2.2 Os sistemas nacionais devem alinhar-se com os requisitos centrais, e as conversações com os Estados-Membros nesta matéria poderão gerar atrasos no desenvolvimento. Este risco pode ser mitigado através de uma interação atempada com os Estados-Membros sobre esta questão, a fim de assegurar que as medidas sejam tomadas no momento oportuno.

#### 2.2.2. *Informações sobre o sistema de controlo interno criado*

As responsabilidades pelas componentes centrais do SIS cabem à eu-LISA. Com vista a possibilitar um melhor acompanhamento da utilização do SIS na análise das tendências relativas às pressões migratórias, à gestão das fronteiras e à criminalidade, a eu-LISA deve ter condições para conceber um dispositivo de última geração destinado à comunicação de estatísticas aos Estados-Membros e à Comissão.

As contas da eu-LISA estarão sujeitas à aprovação do Tribunal de Contas e ao procedimento de quitação. O Serviço de Auditoria Interna da Comissão efetuará auditorias em cooperação com o auditor interno da eu-LISA.

#### 2.2.3. *Estimativa dos custos e benefícios dos controlos e avaliação do nível previsto de risco de erro*

Não aplicável.

### 2.3. **Medidas de prevenção de fraudes e irregularidades**

*Especificar as medidas de prevenção e de proteção existentes ou previstas*

As medidas previstas para lutar contra a fraude constam do artigo 35.º do Regulamento (UE) n.º 1077/2011, que determina o seguinte:

1. Para efeitos da luta contra a fraude, a corrupção e outras atividades ilícitas, aplica-se o Regulamento (CE) n.º 1073/1999.

2. A Agência adere ao Acordo Interinstitucional relativo aos inquéritos internos efetuados pelo Organismo Europeu de Luta Antifraude (OLAF) e publica sem demora as disposições relevantes aplicáveis a todo o pessoal da Agência.

3. As decisões de financiamento, bem como quaisquer contratos e instrumentos de execução delas decorrentes, devem estabelecer expressamente que o Tribunal de Contas e o OLAF podem, se necessário, proceder a controlos no terreno dos beneficiários dos fundos da Agência e dos agentes responsáveis pela respetiva distribuição.

Em conformidade com esta disposição, a decisão do Conselho de Administração da Agência europeia para a gestão operacional de sistemas informáticos de grande escala no espaço de liberdade, segurança e justiça, relativa às condições e modalidades dos inquéritos internos em matéria de prevenção da fraude, da corrupção e de todas as atividades ilegais lesivas dos interesses da União, foi adotada em 28 de junho de 2012.

A estratégia de prevenção e de deteção da fraude da DG HOME será aplicável.

### 3. IMPACTO FINANCEIRO ESTIMADO DA PROPOSTA/INICIATIVA

#### 3.1. Rubrica(s) do quadro financeiro plurianual e rubrica(s) orçamental(ais) de despesa(s) envolvida(s)

- Atuais rubricas orçamentais

Segundo a ordem das rubricas do quadro financeiro plurianual e das respetivas rubricas orçamentais.

| Rubrica do quadro financeiro plurianual | Rubrica orçamental   | Natureza das dotações | Participação                  |                                     |                     |   |
|---|--|-----------------------|-------------------------------|-------------------------------------|---------------------|---|
|   | Rubrica 3 – Segurança e cidadania  | DD/DND <sup>90</sup>  | dos países EFTA <sup>91</sup> | dos países candidatos <sup>92</sup> | de países terceiros | na aceção do artigo 21.º, n.º 2, alínea b), do Regulamento Financeiro |
|   | 18.0208 – Sistema de Informação de Schengen  | DD                    | NÃO                           | NÃO                                 | SIM                 | NÃO   |
|   | 18.020101 – Apoio à gestão das fronteiras e à política comum de vistos para facilitar as deslocações legítimas                                       | DD                    | NÃO                           | NÃO                                 | SIM                 | NÃO   |
|   | 18.0207 – Agência europeia para a gestão operacional de sistemas informáticos de grande escala no espaço de liberdade, segurança e justiça (eu-LISA) | DD                    | NÃO                           | NÃO                                 | SIM                 | NÃO   |

<sup>90</sup> DD = dotações diferenciadas / DND = dotações não diferenciadas.

<sup>91</sup> EFTA: Associação Europeia de Comércio Livre.

<sup>92</sup> Países candidatos e, se for caso disso, potenciais países candidatos dos Balcãs Ocidentais.

### 3.2. Impacto estimado nas despesas

#### 3.2.1. Síntese do impacto estimado nas despesas

|  |   |                       |
|--|---|-----------------------|
| <b>Rubrica do quadro financeiro plurianual</b> | 3 | Segurança e Cidadania |
|--|---|-----------------------|

| DG HOME                                   |              |             | Ano 2018 | Ano 2019 | Ano 2020 | TOTAL         |
|---|--------------|-------------|----------|----------|----------|---------------|
| • Dotações operacionais                   |              |             |          |          |          |               |
| 18.0208 Sistema de Informação de Schengen | Autorizações | (1)         | 6,234    | 1,854    | 1,854    | <b>9,942</b>  |
|   | Pagamentos   | (2)         | 6,234    | 1,854    | 1,854    | <b>9,942</b>  |
| 18.020101 (Fronteiras e Vistos)           | Autorizações | (1)         |          | 18,405   | 18,405   | <b>36,810</b> |
|   | Pagamentos   | (2)         |          | 18,405   | 18,405   | <b>36,810</b> |
| <b>TOTAL das dotações para a DG HOME</b>  | Autorizações | =1+1a<br>+3 | 6,234    | 20,259   | 20,259   | <b>46,752</b> |
|   | Pagamentos   | =2+2a<br>+3 | 6,234    | 20,259   | 20,259   | <b>46,752</b> |

|  |   |                       |
|--|---|-----------------------|
| <b>Rubrica do quadro financeiro plurianual</b> | 3 | Segurança e Cidadania |
|--|---|-----------------------|

| eu-LISA   |              |             | Ano 2018 | Ano 2019 | Ano 2020 | TOTAL         |
|---|--------------|-------------|----------|----------|----------|---------------|
| • Dotações operacionais                               |              |             |          |          |          |               |
| Título 1: Despesas com pessoal                        | Autorizações | (1)         | 0,210    | 0,210    | 0,210    | <b>0,630</b>  |
|   | Pagamentos   | (2)         | 0,210    | 0,210    | 0,210    | <b>0,630</b>  |
| Título 2: Infraestruturas e despesas de funcionamento | Autorizações | (1a)        | 0        | 0        | 0        | <b>0</b>      |
|   | Pagamentos   | (2 a)       | 0        | 0        | 0        | <b>0</b>      |
| Título 3: Despesas operacionais                       | Autorizações | (1a)        | 12,893   | 2,051    | 1,982    | <b>16,926</b> |
|   | Pagamentos   | (2 a)       | 2,500    | 7,893    | 4,651    | <b>15,044</b> |
| <b>TOTAL das dotações para a eu-LISA</b>              | Autorizações | =1+1a<br>+3 | 13,103   | 2,261    | 2,192    | <b>17,556</b> |
|   | Pagamentos   | =2+2a<br>+3 | 2,710    | 8,103    | 4,861    | <b>15,674</b> |

### 3.2.2. Impacto estimado nas dotações operacionais

|  |              |      |  |  |  |  |  |  |  |
|--|--------------|------|--|--|--|--|--|--|--|
| • TOTAL das dotações operacionais  | Autorizações | (4)  |  |  |  |  |  |  |  |
|  | Pagamentos   | (5)  |  |  |  |  |  |  |  |
| • TOTAL das dotações de natureza administrativa financiadas a partir da dotação de programas específicos |              | (6)  |  |  |  |  |  |  |  |
| <b>TOTAL das dotações</b>  | Autorizações | =4+6 |  |  |  |  |  |  |  |



|   |            |       |  |  |  |  |  |  |  |  |
|---|------------|-------|--|--|--|--|--|--|--|--|
| <b>no âmbito da RUBRICA &lt;...&gt;<br/>do quadro financeiro plurianual</b> | Pagamentos | =5+ 6 |  |  |  |  |  |  |  |  |
|---|------------|-------|--|--|--|--|--|--|--|--|

**Se o impacto da proposta/iniciativa incidir sobre mais de uma rubrica:**

|   |              |       |        |        |        |  |  |  |               |
|---|--------------|-------|--------|--------|--------|--|--|--|---------------|
| • TOTAL das dotações operacionais   | Autorizações | (4)   |        |        |        |  |  |  |               |
|   | Pagamentos   | (5)   |        |        |        |  |  |  |               |
| • TOTAL das dotações de natureza administrativa financiadas a partir da dotação de programas específicos                    |              | (6)   |        |        |        |  |  |  |               |
| <b>TOTAL das dotações<br/>no âmbito das RUBRICAS 1 a 4<br/>do quadro financeiro plurianual<br/>(Montante de referência)</b> | Autorizações | =4+ 6 | 19,337 | 22,520 | 22,451 |  |  |  | <b>64,308</b> |
|   | Pagamentos   | =5+ 6 | 8,944  | 28,362 | 25,120 |  |  |  | <b>62,426</b> |

3.2.3. *Impacto estimado nas dotações de natureza administrativa*

|  |          |                            |
|--|----------|----------------------------|
| <b>Rubrica do quadro financeiro plurianual</b> | <b>5</b> | «Despesas administrativas» |
|--|----------|----------------------------|

|                                   |          | Ano N | Ano N+1 | Ano N+2 | Ano N+3 | Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6) | TOTAL |
|-----------------------------------|----------|-------|---------|---------|---------|--|-------|
| DG: <.....>                       |          |       |         |         |         |  |       |
| • Recursos humanos                |          |       |         |         |         |  |       |
| • Outras despesas administrativas |          |       |         |         |         |  |       |
| <b>TOTAL DG &lt;.....&gt;</b>     | Dotações |       |         |         |         |  |       |

Em milhões de EUR (até três casas decimais)

|  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|
| <b>TOTAL das dotações<br/>no âmbito da RUBRICA 5<br/>do quadro financeiro plurianual</b> | (Total das autorizações =<br>Total dos pagamentos) |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

Em milhões de EUR (até três casas decimais)

|  |            | Ano<br>N <sup>93</sup>   | Ano<br>N+1   | Ano<br>N+2 | Ano<br>N+3 | Inserir os anos necessários para<br>refletir a duração do impacto<br>(ver ponto 1.6) |  |  | TOTAL |
|--|------------|--|--------------|------------|------------|--|--|--|-------|
|  |            | <b>TOTAL das dotações<br/>no âmbito das RUBRICAS 1 a 5<br/>do quadro financeiro plurianual</b> | Autorizações |            |            |  |  |  |       |
|  | Pagamentos |  |              |            |            |  |  |  |       |

<sup>93</sup> O ano N é o do início da aplicação da proposta/iniciativa.

### 3.2.3.1 Impacto estimado nas dotações da DG HOME

- A proposta/iniciativa não acarreta a utilização de dotações operacionais
- A proposta/iniciativa acarreta a utilização de dotações operacionais, tal como explicitado seguidamente:

| Indicar os objetivos e as realizações<br>↓                                     |                    |             | Ano 2018 | Ano 2019 | Ano 2020 | Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6) |     |        |     |       |     |       |     |       |     | TOTAL |     |       |           |             |
|--|--------------------|-------------|----------|----------|----------|--|-----|--------|-----|-------|-----|-------|-----|-------|-----|-------|-----|-------|-----------|-------------|
|  | REALIZAÇÕES        |             |          |          |          |  |     |        |     |       |     |       |     |       |     |       |     |       |           |             |
|  | Tipo <sup>94</sup> | Custo médio | N.º      | Custo    | N.º      | Custo  | N.º | Custo  | N.º | Custo | N.º | Custo | N.º | Custo | N.º | Custo | N.º | Custo | N.º total | Custo total |
| OBJETIVO ESPECÍFICO N.º 1 <sup>95</sup><br>Desenvolvimento do sistema nacional |                    |             | 1        |          | 1        | 1,221  | 1   | 1,221  |     |       |     |       |     |       |     |       |     |       |           | 2,442       |
| OBJETIVO ESPECÍFICO N.º 2<br>Infraestrutura                                    |                    |             | 1        |          | 1        | 17,184   | 1   | 17,184 |     |       |     |       |     |       |     |       |     |       |           | 34,368      |
| <b>CUSTO TOTAL</b>   |                    |             |          |          |          | 18,405   |     | 18,405 |     |       |     |       |     |       |     |       |     |       |           | 36,810      |

<sup>94</sup> As realizações dizem respeito aos produtos fornecidos e serviços prestados (p. ex., número de intercâmbios de estudantes financiados, número de quilómetros de estradas construídas, etc.).

<sup>95</sup> Tal como descrito no ponto 1.4.2. «Objetivo(s) específico(s)...».

### 3.2.3.2 Impacto estimado nas dotações operacionais da eu-LISA

- A proposta/iniciativa não acarreta a utilização de dotações operacionais
- A proposta/iniciativa acarreta a utilização de dotações operacionais, tal como explicitado seguidamente:

Dotações de autorização em milhões de EUR (até três casas decimais)

| Indicar os objetivos e as realizações<br>↓                                    |                    |             | Ano 2018 | Ano 2019 | Ano 2020 | Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6) |     |       |     |       |     |       |     |       |     | TOTAL |           |             |
|---|--------------------|-------------|----------|----------|----------|--|-----|-------|-----|-------|-----|-------|-----|-------|-----|-------|-----------|-------------|
|   | REALIZAÇÕES        |             |          |          |          |  |     |       |     |       |     |       |     |       |     |       |           |             |
|   | Tipo <sup>96</sup> | Custo médio | N.º      | Custo    | N.º      | Custo  | N.º | Custo | N.º | Custo | N.º | Custo | N.º | Custo | N.º | Custo | N.º total | Custo total |
| OBJETIVO ESPECÍFICO N.º 1 <sup>97</sup><br>Desenvolvimento do sistema central |                    |             |          |          |          |  |     |       |     |       |     |       |     |       |     |       |           |             |
| - Contratante   |                    |             | 1        | 5,013    |          |  |     |       |     |       |     |       |     |       |     |       |           | 5,013       |
| - Programas   |                    |             | 1        | 4,050    |          |  |     |       |     |       |     |       |     |       |     |       |           | 4,050       |
| - Equipamento   |                    |             | 1        | 3,692    |          |  |     |       |     |       |     |       |     |       |     |       |           | 3,692       |
| Subtotal do objetivo específico n.º 1   |                    |             |          | 12,755   |          |  |     |       |     |       |     |       |     |       |     |       |           | 12,755      |
| OBJETIVO ESPECÍFICO N.º 2<br>Manutenção do sistema central                    |                    |             |          |          |          |  |     |       |     |       |     |       |     |       |     |       |           |             |
| - Contratante   |                    |             | 1        | 0        | 1        | 0,365  | 1   | 0,365 |     |       |     |       |     |       |     |       |           | 0,730       |
| Programas   |                    |             | 1        | 0        | 1        | 0,810  | 1   | 0,810 |     |       |     |       |     |       |     |       |           | 1,620       |
| Equipamento   |                    |             | 1        | 0        | 1        | 0,738  | 1   | 0,738 |     |       |     |       |     |       |     |       |           | 1,476       |

<sup>96</sup> As realizações dizem respeito aos produtos fornecidos e serviços prestados (p. ex., número de intercâmbios de estudantes financiados, número de quilómetros de estradas construídas, etc.).

<sup>97</sup> Tal como descrito no ponto 1.4.2. «Objetivo(s) específico(s)...».

|   |   |        |   |       |   |       |  |  |  |  |  |  |  |  |  |        |
|---|---|--------|---|-------|---|-------|--|--|--|--|--|--|--|--|--|--------|
| Subtotal do objetivo específico n.º 2                 |   |        |   | 1,913 |   | 1,913 |  |  |  |  |  |  |  |  |  | 3,826  |
| <b>OBJETIVO ESPECÍFICO N.º 3</b><br>Reuniões/formação |   |        |   |       |   |       |  |  |  |  |  |  |  |  |  |        |
| Atividades de formação                                | 1 | 0,138  | 1 | 0,138 | 1 | 0,069 |  |  |  |  |  |  |  |  |  | 0,345  |
| Subtotal do objetivo específico n.º 3                 |   | 0,138  |   | 0,138 |   | 0,069 |  |  |  |  |  |  |  |  |  | 0,345  |
| <b>CUSTO TOTAL</b>                                    |   | 12,893 |   | 2,051 |   | 1,982 |  |  |  |  |  |  |  |  |  | 16,926 |

### 3.2.3.3 Impacto estimado nos recursos humanos da eu-LISA

#### Síntese

- A proposta/iniciativa não acarreta a utilização de dotações de natureza administrativa
- A proposta/iniciativa acarreta a utilização de dotações de natureza administrativa, tal como explicitado seguidamente:

Em milhões de EUR (até três casas decimais)

|  | Ano<br>2018 | Ano<br>2019 | Ano<br>2020 | TOTAL |
|--|-------------|-------------|-------------|-------|
|--|-------------|-------------|-------------|-------|

|                              |       |       |       |       |
|------------------------------|-------|-------|-------|-------|
| Funcionários (Graus AD)      |       |       |       |       |
| Funcionários (Graus AST)     |       |       |       |       |
| Agentes contratuais          | 0,210 | 0,210 | 0,210 | 0,630 |
| Agentes temporários          |       |       |       |       |
| Peritos nacionais destacados |       |       |       |       |

|              |              |              |              |              |
|--------------|--------------|--------------|--------------|--------------|
| <b>TOTAL</b> | <b>0,210</b> | <b>0,210</b> | <b>0,210</b> | <b>0,630</b> |
|--------------|--------------|--------------|--------------|--------------|

O recrutamento está previsto para janeiro de 2018. Todo o pessoal deve estar disponível no início de 2018, a fim de permitir iniciar o período de desenvolvimento em tempo útil para assegurar a entrada em funcionamento da reformulação do SIS II em 2020. Os três novos agentes contratuais são necessários para responder às exigências tanto na execução do projeto como no apoio operacional e na manutenção após a implantação e a passagem para a produção. Estes recursos serão utilizados para:

- Apoiar a execução do projeto enquanto membros da equipa de projeto, incluindo atividades como: a definição de requisitos e especificações técnicas, cooperação e assistência aos Estados-Membros durante a execução, atualizações do Documento de Controlo das Interfaces (DCI), acompanhamento das prestações contratuais, entrega e atualizações de documentação, etc.
- Apoiar as atividades de transição relativas à colocação em funcionamento do sistema, em cooperação com o contratante (acompanhamento das novas versões, atualizações do processo operacional, formações, incluindo atividades de formação dos Estados-Membros), etc.
- Apoiar as atividades a longo prazo, a definição das especificações, as reformulações contratuais em caso de reconfiguração do sistema (p. ex., devido ao reconhecimento de imagens) ou caso o contrato de manutenção em estado de funcionamento (MWO) do novo SIS II careça de alterações para abranger modificações adicionais (de um ponto de vista técnico e orçamental).

- Executar o segundo nível de apoio na sequência da entrada em funcionamento, durante a manutenção contínua e a fase operacional.

Importa referir que os três novos recursos (agentes contratuais em ETC) exercerão funções complementares aos recursos das equipas internas, que também terão a seu cargo atividades de acompanhamento financeiro/operacionais relativas aos projeto/contratos. A utilização de agentes contratuais permitirá uma duração e continuidade adequadas dos contratos, a fim de assegurar a continuidade das atividades e a afetação dos mesmos recursos especializados às atividades de apoio operacional após a conclusão do projeto. Além disso, as atividades de apoio operacional exigem acessos ao ambiente de produção que não podem ser concedidos aos contratantes ou a pessoal externo.

### 3.2.3.4 Necessidades estimadas de recursos humanos

- A proposta/iniciativa não acarreta a utilização de recursos humanos.
- A proposta/iniciativa acarreta a utilização de recursos humanos, tal como explicitado seguidamente:

*Estimativa expressa em unidades equivalentes a tempo completo*

|  | Ano N            | Ano N+1 | Ano N+2 | Ano N+3 | Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6) |  |  |
|--|------------------|---------|---------|---------|--|--|--|
| <b>• Lugares do quadro do pessoal (funcionários e agentes temporários)</b>   |                  |         |         |         |  |  |  |
| XX 01 01 01 (na sede e nos gabinetes de representação da Comissão)           |                  |         |         |         |  |  |  |
| XX 01 01 02 (nas delegações)   |                  |         |         |         |  |  |  |
| XX 01 05 01 (investigação indireta)  |                  |         |         |         |  |  |  |
| 10 01 05 01 (investigação direta)  |                  |         |         |         |  |  |  |
| <b>• Pessoal externo (em equivalente a tempo completo: ETC)<sup>98</sup></b> |                  |         |         |         |  |  |  |
| XX 01 02 01 (AC, PND, TT da «dotação global»)                                |                  |         |         |         |  |  |  |
| XX 01 02 02 (AC, AL, PND, TT e JPD nas delegações)                           |                  |         |         |         |  |  |  |
| <b>XX 01 04 aa<sup>99</sup></b>  | - na sede        |         |         |         |  |  |  |
|  | - nas delegações |         |         |         |  |  |  |
| XX 01 05 02 (AC, PND e TT – Investigação indireta)                           |                  |         |         |         |  |  |  |
| 10 01 05 02 (AC, PND e TT — Investigação direta)                             |                  |         |         |         |  |  |  |
| Outras rubricas orçamentais (especificar)                                    |                  |         |         |         |  |  |  |
| <b>TOTAL</b>   |                  |         |         |         |  |  |  |

**XX** constitui o domínio de intervenção ou título orçamental em causa.

As necessidades de recursos humanos serão cobertas pelos efetivos da DG já afetados à gestão da ação e/ou reafetados internamente ao nível da DG, complementadas, caso necessário, por eventuais dotações adicionais que sejam atribuídas à DG gestora no quadro do processo anual de atribuição e no limite das disponibilidades orçamentais.

Descrição das tarefas a executar:

|                                    |  |
|------------------------------------|--|
| Funcionários e agentes temporários |  |
| Pessoal externo                    |  |

<sup>98</sup> AC = agente contratual; AL = agente local; PND = peritos nacionais destacados; TT = trabalhador temporário; JPD = jovem perito nas delegações.

<sup>99</sup> Sublimite para o pessoal externo coberto pelas dotações operacionais (antigas rubricas «BA»).



### 3.2.4. *Compatibilidade com o atual quadro financeiro plurianual*

- A proposta/iniciativa é compatível com o atual quadro financeiro plurianual.
- A proposta/iniciativa requer uma reprogramação da rubrica pertinente do quadro financeiro plurianual.

Está prevista uma reprogramação da parte remanescente da dotação reservada às fronteiras inteligentes no âmbito do Fundo para a Segurança Interna, no intuito de implementar as funcionalidades e modificações previstas nas duas propostas. O Regulamento relativo ao FSI-Fronteiras é o instrumento financeiro no qual foi incluído o orçamento para a aplicação do pacote sobre as fronteiras inteligentes. No seu artigo 5.º, prevê que 791 milhões de EUR devem ser aplicados através de um programa para a criação de sistemas informáticos de apoio à gestão dos fluxos migratórios nas fronteiras externas, nos termos do artigo 15.º Destes 791 milhões de EUR, 480 milhões de EUR estão reservados ao desenvolvimento do Sistema de Entrada/Saída e 210 milhões de EUR ao desenvolvimento do Sistema Europeu de Informação e Autorização de Viagem (ETIAS). A parte remanescente (100,828 milhões de EUR) será parcialmente utilizada para cobrir os custos das alterações relativas à melhoria das funcionalidades do SIS II, previstas nas duas propostas.

- A proposta/iniciativa requer a aplicação do instrumento de flexibilidade ou a revisão do quadro financeiro plurianual.

Explicitar as necessidades, especificando as rubricas orçamentais em causa e as quantias correspondentes.

### 3.2.5. *Participação de terceiros no financiamento*

- A proposta/iniciativa não prevê o cofinanciamento por terceiros.
- A proposta/iniciativa prevê o cofinanciamento estimado seguinte:

Dotações em milhões de EUR (até três casas decimais)

|   | Ano<br>N | Ano<br>N+1 | Ano<br>N+2 | Ano<br>N+3 | Inserir os anos necessários para<br>refletir a duração do impacto<br>(ver ponto 1.6) |  |  | Total |
|---|----------|------------|------------|------------|--|--|--|-------|
| Especificar o organismo<br>de cofinanciamento |          |            |            |            |  |  |  |       |
| TOTAL das dotações<br>cofinanciadas           |          |            |            |            |  |  |  |       |

### 3.3. Impacto estimado nas receitas

- A proposta/iniciativa não tem impacto financeiro nas receitas.
- A proposta/iniciativa tem o impacto financeiro a seguir descrito:
  - nos recursos próprios
  - nas receitas diversas

Em milhões de EUR (até três casas decimais)

| Rubrica orçamental das receitas:   | Dotações disponíveis para o exercício em curso | Impacto da proposta/iniciativa <sup>100</sup> |      |      |      |  | Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6) |  |  |
|--|--|---|------|------|------|--|--|--|--|
|  |  | 2018  | 2019 | 2020 | 2021 |  |  |  |  |
| Artigo 6313 – contribuição de países associados a Schengen (CH, NO, LI, IS). |  | p.m.  | p.m. | p.m. | p.m. |  |  |  |  |

Relativamente às receitas diversas que serão «afetadas», especificar a(s) rubrica(s) orçamental(ais) de despesas envolvida(s).

18.02.08 (Sistema de Informação de Schengen), 18.02.07 (eu-LISA)

Especificar o método de cálculo do impacto nas receitas

O orçamento inclui uma contribuição financeira dos países associados à execução, à aplicação e ao desenvolvimento do acervo de Schengen.

<sup>100</sup>

No que diz respeito aos recursos próprios tradicionais (direitos aduaneiros e quotizações sobre o açúcar), as quantias indicadas devem ser apresentadas em termos líquidos, ou seja, quantias brutas após dedução de 25 % a título de despesas de cobrança.