Parecer do Comité Económico e Social Europeu sobre a «Proposta de regulamento do Parlamento Europeu e do Conselho relativo à criação de um quadro para a interoperabilidade entre os sistemas de informação da UE (fronteiras e vistos) e que altera a Decisão 2004/512/CE do Conselho, o Regulamento (CE) n.º 767/2008, a Decisão 2008/633/JAI do Conselho, o Regulamento (UE) 2016/399 e o Regulamento (UE) 2017/2226»

[COM(2017) 793 final — 2017/0351 (COD)]

e sobre a «Proposta de regulamento do Parlamento Europeu e do Conselho relativo à criação de um quadro para a interoperabilidade entre os sistemas de informação da UE (cooperação policial e judiciária, asilo e migração)»

[COM(2017) 794 final — 2017/0352 (COD)]

(2018/C 283/07)

Relatora: **Laure BATUT**

Consulta	Comissão Europeia, 18.1.2018
	Parlamento Europeu, 28.2.2018
Base jurídica	Artigo 304.º do Tratado sobre o Funcionamento da União Europeia
Competência	Secção Especializada de Emprego, Assuntos Sociais e Cidadania
Adoção em secção	25.4.2018
Adoção em plenária	23.5.2018
Reunião plenária n.º	535
Resultado da votação	160/3/2
(votos a favor/votos contra/abstenções)	

1. **Conclusões e recomendações**

1.1. O CESE considera útil e positiva a proposta da Comissão Europeia de melhorar a interoperabilidade dos sistemas de informação da UE, tanto no que respeita a fronteiras e vistos como à cooperação policial e judiciária, asilo e migração.

1.2. O CESE considera que esta interoperabilidade deve ser um objetivo estratégico da UE para que esta continue a ser um espaço aberto e de salvaguarda dos direitos fundamentais e da mobilidade. A UE e os Estados-Membros têm a obrigação de proteger a vida e a segurança de todos os seres humanos; o princípio da não repulsão deve ser plenamente respeitado.

1.3. As medidas que visam a interoperabilidade serão mais bem entendidas se:

— garantirem, no quadro da estratégia da UE para a migração, as condições de equilíbrio entre liberdade e segurança no respeito da separação de poderes;

— garantirem os direitos fundamentais das pessoas em causa, em especial a segurança dos seus dados pessoais e da sua vida privada, e o direito de acesso, de retificação e de apagamento dos seus dados, num prazo razoável e através de procedimentos acessíveis;

— reafirmarem, nomeadamente em todos os atos de execução, o requisito de integração dos princípios da proteção de dados desde a conceção;

— não criarem novos obstáculos à circulação normal de passageiros e de mercadorias.

1.4. O CESE solicita procedimentos e garantias no que se refere à utilização dos dados para efeitos de aplicação da lei, que:

— prevejam a aplicação da lei europeia que oferece maior proteção (Regulamento Geral sobre a Proteção de Dados — RGPD);

— permitam acelerar o processo de identificação do Estado-Membro responsável pela análise dos pedidos de proteção internacional;

— garantam às pessoas em causa o direito a um duplo grau de jurisdição;

— garantam aos menores, em particular os não acompanhados, independentemente de se encontrarem em situação irregular, de serem alvo de perseguição ou de terem cometido uma infração criminal, o direito de obter um visto e de serem protegidos e integrados, bem como o direito a «serem esquecidos» num prazo mais curto do que o aplicável aos adultos.

1.5. O CESE considera que a atual base jurídica dos sistemas de informação deve ser reforçada e ter em conta a evolução dos sistemas de recolha de dados. Nesse sentido, preconiza:

— o reforço da segurança das bases de dados existentes e dos respetivos canais de comunicação;

— a avaliação do impacto do reforço do controlo *a priori* na gestão dos riscos;

— um controlo e uma avaliação permanente da arquitetura pelas autoridades de proteção de dados (Autoridade Europeia para a Proteção de Dados — AEPD), exigindo que as entidades responsáveis apresentem às autoridades de decisão e à Comissão relatórios anuais sobre a segurança dos componentes de interoperabilidade, bem como relatórios bianuais sobre o impacto das medidas nos direitos fundamentais.

1.6. O CESE considera que o projeto se deve apoiar em pessoal competente, sendo, para tanto, necessário haver:

— programas de formação sólidos para as autoridades em causa e os agentes da Agência Europeia para a Gestão Operacional de Sistemas Informáticos de Grande Escala no Espaço de Liberdade, Segurança e Justiça (eu-LISA);

— um controlo rigoroso das competências dos agentes e candidatos a agentes desta agência.

1.7. O CESE manifesta-se apreensivo quanto ao financiamento do novo sistema. O acompanhamento da planificação será crucial para evitar a derrapagem dos orçamentos e concluir o projeto até 2029.

1.8. O CESE recomenda que os cidadãos sejam informados sobre as várias etapas do projeto até à sua conclusão e que as pessoas recebam informação pedagógica sobre os controlos a que são submetidas. Considera que se deve prever a possibilidade de interromper o processo caso a liberdade e os direitos fundamentais sejam prejudicados por uma utilização abusiva do sistema.

2. **Introdução**

2.1. No contexto internacional de 2017, que foi um ano considerado instável tanto a nível geopolítico, como a nível da segurança interna dos Estados-Membros, o Conselho instou por diversas vezes a Comissão a providenciar os meios necessários para o rastreamento de pessoas consideradas «em risco» que já tenham sido objeto de registo num dos Estados-Membros. A identificação das suas passagens nas fronteiras, das suas viagens e dos seus itinerários na Europa poderá ser crucial para a segurança no território da União.

2.2. Na sua resolução de 6 de julho de 2016, o Parlamento Europeu instou a Comissão Europeia a fornecer as salvaguardas necessárias em matéria de proteção de dados.

2.3. As propostas em apreço inscrevem-se no objetivo de preservar e reforçar Schengen ([1]). A União já se muniu de diversos instrumentos regulamentares e serviços digitalizados de informação nos domínios relacionados com o controlo da passagem de pessoas e de mercadorias nas fronteiras.

2.4. Importa recordá-los:

— **SIS: Sistema de informação Schengen** — é um dos mecanismos mais antigos, tendo já sido revisto, que gera uma grande diversidade de alertas sobre pessoas e mercadorias;

([1]) COM(2017) 570 final.

— **Sistema «Eurodac» de comparação de impressões digitais** de requerentes de asilo e nacionais de países terceiros em situação irregular nas fronteiras e nos Estados-Membros e de determinação do Estado-Membro responsável pela análise dos pedidos (parecer do CESE 2016-02981, relator: José Antonio Moreno Díaz ([2]));

— **VIS: Sistema de Informação sobre Vistos** (Código de Vistos) que gere os vistos para as estadas de curta duração (parecer do CESE 2014-02932, relatores: Antonello Pezzini e Luis Miguel Pariza Castaños ([3]));

— **SES: Sistema de Entrada/Saída** (decisão em curso) que deverá gerir de forma eletrónica os dados dos passaportes e as datas de entrada e de saída dos nacionais de países terceiros que visitam o espaço Schengen (parecer do CESE 2016--03098, SOC/544, relator: Cristian Pîrvulescu ([4]));

— **ETIAS: Sistema Europeu de Informação e Autorização de Viagem** (decisão em curso) que deverá ser um vasto sistema automatizado de armazenamento e verificação *ex ante* de dados dos nacionais de países terceiros isentos da obrigação de visto para circular no espaço Schengen (parecer do CESE 2016-06889, SOC/556, relator: Jan Simons ([5]));

— **ECRIS-TCN: Sistema Europeu de Informação sobre Registos Criminais dos nacionais de países terceiros**, proposto pela Comissão, é um sistema digital de troca de informações sobre decisões judiciais proferidas pelos tribunais nacionais.

2.5. Pode estabelecer-se uma analogia entre os meios atualmente à disposição de uma autoridade habilitada e um telemóvel inteligente com diferentes aplicações, que são todas independentes e fornecem informações específicas.

2.6. Com exceção do SIS, estes sistemas centram-se na **gestão dos nacionais de países terceiros**. Existem seis sistemas, que são complementares e descentralizados. As informações recolhidas são a soma das diferentes respostas obtidas de diversas bases de dados pelos serviços de investigação, em função das respetivas autorizações de acesso.

2.7. A Comissão pretende responder à seguinte questão:

— qual o método que permite, sem alterar as estruturas já adquiridas e conservando a sua complementaridade, colocar todas as bases de dados em sintonia, no mesmo momento, para que, num ponto de entrada no território europeu e através de uma única consulta do sistema, todas as informações já recolhidas nas bases de dados existentes estejam disponíveis para a autoridade de controlo autorizada a consultá-las, respeitando sempre a regulamentação em matéria de proteção dos dados e dos direitos fundamentais.

2.8. Nas propostas em análise, a Comissão Europeia pretende:

2.8.1. proporcionar mais possibilidades de acesso às bases de dados da Europol e da Interpol, as quais cooperam já com as autoridades de controlo europeias;

2.8.2. «sincronizar» as pesquisas de informação para reduzir os tempos de resposta no que diz respeito aos dossiês de migrantes e acelerar a reação em termos de segurança em caso de necessidade. Para tal, propõe a criação de novas entidades que permitiriam que as bases atuais funcionassem em simbiose.

2.9. **A Comissão tem por objetivos colmatar tanto quanto possível as lacunas dos diferentes sistemas; melhorar a** gestão das fronteiras externas do espaço Schengen; contribuir para a segurança interna da União; gerir as fraudes de identidade e resolver os casos de identidades múltiplas; localizar as pessoas suspeitas ou já condenadas e verificar a sua identidade dentro do espaço Schengen.

2.10. Retomando a imagem do telemóvel inteligente, a autoridade habilitada não só teria diversas aplicações à sua disposição, como poderia também recolher em simultâneo e numa mesma pesquisa, utilizando os seus códigos de acesso, os dados armazenados em todos os seus suportes — computador de mesa, computador portátil, telemóvel, táblete, notebook, etc.

([2]) JO C 34 de 2.2.2017, p. 144.
([3]) JO C 458 de 19.12.2014, p. 36.
([4]) JO C 487 de 28.12.2016, p. 66.
([5]) JO C 246 de 28.7.2017, p. 28.

3. **Funcionamento do sistema**

3.1. A Comissão realizou consultas e reuniu um grupo de peritos de alto nível em matéria de sistemas de informação e interoperabilidade ([6]), nomeados pelos Estados-Membros, pelos países do espaço Schengen e por agências europeias como a eu-LISA ([7]) e a FRA ([8]), sob a coordenação da Direção-Geral da Migração e dos Assuntos Internos da Comissão (DG HOME).

O método: interconectividade ou interoperabilidade?

3.1.1. A **interconectividade** dos sistemas de informação é a possibilidade de serem ligados entre si de modo que os dados registados num sistema possam ser automaticamente consultados por outro sistema.

3.1.2. A **interoperabilidade** ([9]) é a capacidade de diferentes sistemas para comunicarem, trocarem dados e utilizarem a informação partilhada, respeitando os direitos de acesso aos sistemas.

3.2. *A opção pela interoperabilidade*

3.2.1. A Comissão considera que a opção pela interoperabilidade não afeta o acervo nem as competências atuais das estruturas e que os dados permanecerão em silos isolados. Não obstante o aumento da comunicabilidade, esta opção apresentaria uma vantagem em termos de segurança para os sistemas e os dados, que, como é evidente, não serão acessíveis através da Internet. As propostas em apreço apresentam semelhanças substanciais, mas

— uma incide na interoperabilidade dos sistemas de informação relativos às fronteiras e aos vistos [COM(2017) 793],

— a outra é relativa à cooperação entre a polícia e a justiça, ao asilo e à migração [COM(2017) 794].

3.3. *Os novos instrumentos*

3.3.1. Para funcionar na interoperabilidade, uma nova arquitetura de quatro novos instrumentos deverá complementar as seis bases de dados para trabalhar com celeridade consultando apenas uma vez o sistema e mantendo as pessoas habilitadas na origem dos pedidos de acesso.

3.4. *O ESP (European Search Portal), um portal europeu de pesquisa*

3.4.1. A autoridade de controlo habilitada (o utilizador final) deverá poder aceder a todo o sistema através de um único acesso. Em vez de efetuar seis pesquisas, lançaria apenas uma para interrogar várias bases de dados simultaneamente (polícias, alfândegas, etc.), mas sem armazenar nenhum dos dados pesquisados. Se os dados existirem, o sistema encontrá-los-á. Em caso de suspeita de crime ou de atividade terrorista, uma primeira pesquisa com um dado de uma pessoa alvo de consulta poderá ser neutra («no-hit» ou resposta negativa), mas se o dado corresponder a uma segunda informação («hit» ou resposta positiva) existente nas bases de dados, como o SIS, o SES e o ETIAS, poderá dar azo a pesquisas aprofundadas e a uma investigação.

3.5. *O BMS (Shared Biometric Matching Service), um serviço partilhado de correspondências biométricas*

3.5.1. Esta plataforma partilhada de correspondências permitirá a pesquisa e comparação simultâneas de dados matematizados, biométricos, impressões digitais e fotografias de identidade, a partir das diferentes bases de dados, como o SIS, o Eurodac, o VIS, o *SES* ([10]), o *ECRIS*, mas não o *ETIAS*; os seus dados deverão ser compatíveis.

3.5.2. Os dados matematizados não serão conservados na sua forma original.

3.6. *O CIR (Common Identity Repository), um repositório comum de dados de identificação*

3.6.1. Um repositório comum de dados de identificação reunirá os dados relativos à identidade biográfica e biométrica dos nacionais de países terceiros controlados, quer se encontrem na fronteira ou no interior dos Estados-Membros (de Schengen). Um indicador de respostas positivas das diferentes bases de dados acelerará as pesquisas. Sob a responsabilidade e com os meios de segurança da agência eu-LISA, estes dados serão salvaguardados de modo que ninguém possa aceder a mais do que uma linha alfanumérica de cada vez. Desenvolvido a partir do SES e do ETIAS, o CIR não deverá conduzir à duplicação dos dados. O repositório poderá também ser utilizado para investigações civis.

([6]) DG HOME, unidade B/3, Decisão C/2016/3780 da Comissão, de 17 de junho de 2016, http://ec.europa.eu/transparency/regexpert//index.cfm?Lang=PThttp://ec.europa.eu/transparency/regexpert/index.cfm?Lang=PT

([7]) Agência Europeia para a Gestão Operacional de Sistemas Informáticos de Grande Escala no Espaço de Liberdade, Segurança e Justiça.

([8]) FRA — Agência dos Direitos Fundamentais da União Europeia.

([9]) Comunicação da Comissão — Sistemas de informação mais sólidos e mais inteligentes para controlar as fronteiras e garantir a segurança [COM(2016) 205 final].

([10]) O itálico assinala que os textos relativos a estes organismos ainda não foram adotados.

3.7. *O MID (Multiple-Identity Detector), um detetor de identidades múltiplas*

3.7.1. A função deste instrumento será a de verificar a identidade correta das pessoas de boa-fé e combater as fraudes de identidade, através de uma pesquisa simultânea em todas as bases de dados. Até à data, nenhuma administração utilizou um tal instrumento, que permitirá evitar usurpações de identidade.

3.8. *O papel da agência eu-LISA* ([11])

3.8.1. A agência, criada em 2011, tem por missão facilitar as políticas da UE nos domínios da justiça, da segurança e da liberdade. Sediada em Taline, na Estónia, assegura já o intercâmbio de informações entre as diferentes autoridades responsáveis pela aplicação da lei dos Estados-Membros, o funcionamento sem descontinuidades dos sistemas informáticos de grande escala e a liberdade de circulação das pessoas no espaço Schengen.

3.8.2. A agência está a trabalhar no projeto «Fronteiras Inteligentes» e, no âmbito da nova arquitetura de intercâmbio de dados, desempenhará um papel de conservação dos elementos relacionados com as pessoas, como os relativos às autoridades, às investigações e aos investigadores. Controlará os direitos de acesso dos requerentes e garantirá a segurança dos dados, nomeadamente em caso de «incidente» [artigo 44.º das propostas COM(2017) 793 e 794].

3.8.3. **A utilização do formato de mensagem universal** (UMF — *Universal Message Format*), que ainda está por criar, deverá facilitar o trabalho com os novos sistemas, que serão obrigatórios, impondo a criação de interfaces nos Estados-Membros que ainda não as possuírem e de um sistema temporário de tradução de uma linguagem para outra.

3.9. *A proteção de dados pessoais (artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia):*

3.9.1. A proposta de regulamento reconhece a possibilidade de ocorrerem incidentes de segurança. Os Estados-Membros e os respetivos sistemas de dados devem ser os primeiros a respeitar os princípios em matéria de proteção de dados previstos pelos textos em apreço, pelo Tratado, pela Carta dos Direitos Fundamentais da União Europeia e pelo RGPD ([12]), que entrará em vigor em 25 de maio de 2018.

4. **Observações gerais**

4.1. *Valor acrescentado da interoperabilidade em democracia*

4.1.1. A UE necessita de regulação e de meios de investigação que a protejam contra a criminalidade. A interoperabilidade dos sistemas de informação é uma oportunidade para fazer valer o primado do direito e a defesa dos direitos humanos.

4.1.2. O *SES e o ETIAS*, conjugados com o BMS e o CIR, permitirão controlar as passagens nas fronteiras de pessoas suspeitas, bem como conservar os respetivos dados. No entanto, a possibilidade de as autoridades de aplicação da lei acederem através do BMS aos sistemas de informação com finalidades não coercivas a nível da UE [artigo 17.º «Repositório comum de dados de identificação» das propostas de regulamento COM(2017) 794 e 793] não pode ser compatível com os fins enunciados como bases das propostas em apreço. A este respeito, o Comité (artigo 300.º, n.º 4, do TFUE) não pode deixar de evocar o princípio da proporcionalidade e exorta a Comissão a abster-se de criar um regime de tipo «Big Brother» ([13]) e de colocar obstáculos à liberdade de circulação dos cidadãos europeus (artigo 3.º do TUE).

4.1.3. O modelo proposto para a recolha e utilização dos dados pessoais obtidos na fronteira e no território da União aquando de controlos da circulação e de documentos é apresentado como estanque, aberto apenas a pessoas autorizadas e para fins de segurança e gestão, permitindo uma maior fluidez dos procedimentos.

4.1.4. O Comité interroga-se sobre a estanquidade: continuam a subsistir lacunas, a construção faseada em nove anos assenta em «fundações» que ainda não existem, como as bases de dados SES ou ETIAS ou as interfaces nacionais. O contexto tecnológico está em constante evolução; o projeto assenta necessariamente no estado da técnica, mas não prevê dotações orçamentais para a gestão da obsolescência que possa surgir em alguns setores digitais.

([11]) 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).

([12]) 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). Pareceres do CESE: JO C 229 de 31.7.2012, p. 90, e JO C 345 de 13.10.2017, p. 138.

([13]) George Orwell, *1984*.

4.1.5. Além disso, o rápido aumento da utilização de algoritmos ditos de inteligência artificial (IA) poderia ter sido considerado no projeto, quer como instrumento de controlo dos sistemas, quer como chave de segurança a confiar às autoridades de decisão para garantir a utilização democrática da arquitetura.

4.1.6. A proposta desenvolve um sistema para as pessoas de boa-fé, que respeitam a lei. O facto de serem seres humanos a estar aos comandos é tranquilizador, mas eles podem também ser os «elos fracos». O Comité propõe o aditamento de um artigo que preveja «disjuntores diferenciais» a aplicar em caso de crise política e/ou de «gestão», uma vez que qualquer problema numa base de dados poderá representar um risco para a arquitetura no seu conjunto ([14]). A utilização de um formato de mensagem universal (UMF) que poderia vir a tornar-se internacional, embora sendo muito positiva, acarretará riscos significativos no tocante à proteção de dados e depositará nas autoridades habilitadas uma enorme responsabilidade. Estes aspetos não são abordados nas propostas em análise.

4.2. *Proteção dos direitos fundamentais*

4.2.1. Os direitos fundamentais são absolutos e qualquer restrição ao seu exercício deve limitar-se ao estritamente necessário, corresponder efetivamente a objetivos de interesse geral reconhecidos pela União e respeitar o conteúdo essencial desses direitos (artigos 8.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia). O Comité interroga-se sobre o modo como a proporcionalidade das medidas de controlo pode ser avaliada no caso dos migrantes que fogem de perseguições e requerem asilo quando desembarcam na União. [COM(2017) 794 final, Exposição de motivos — Direitos fundamentais]. A localização de suspeitos com vista a prevenir atos criminosos, nomeadamente de terrorismo, **não deve aproximar as democracias europeias do conceito de «delito por antecipação»**; deve continuar a existir uma diferença entre «atividades» que perturbam a ordem pública e «opiniões».

4.2.2. O respeito, relativamente a todas as pessoas, dos direitos enunciados na Carta dos Direitos Fundamentais da União Europeia deve assegurar o equilíbrio entre a segurança e a liberdade, sem o qual a democracia perece. O Comité considera que este equilíbrio é fundamental e deve ser um objetivo permanente para todas as autoridades, incluindo as de controlo, tanto a nível nacional como a nível europeu.

4.2.3. A cadeia de autoridades associadas a uma pesquisa, bem como os metadados conexos serão conservados no sistema. Os direitos fundamentais das próprias autoridades habilitadas devem ser respeitados relativamente aos dados gerados, nomeadamente no que se refere à sua segurança e à sua vida privada, em caso de intrusão maliciosa na estrutura e de utilização abusiva dos dados entre o momento da sua introdução e o do seu apagamento.

4.3. *Proteção dos dados*

4.3.1. As propostas em análise reconhecem o princípio da proteção de dados pessoais desde a conceção e por defeito, embora as suas exposições de motivos recordem que, segundo o Tribunal de Justiça da União Europeia (TJUE), o direito à proteção de dados pessoais não é um direito absoluto. O Comité reconhece as vantagens das medidas preventivas para salvaguardar a segurança, do combate às falsas identidades e da garantia do direito de asilo. No entanto, faz questão de sublinhar os limites da matematização e da anonimização dos dados: as pessoas em causa podem vir a precisar mais tarde dos seus dados.

4.3.2. O Comité sublinha igualmente que o tipo de dados conservados, designadamente biométricos e biológicos, reveste-se de especial interesse para algumas empresas e para pessoas com intenções criminosas. A cibersegurança é aqui tão importante quanto a segurança física, mas não é suficientemente evocada nas propostas. Os dados conservados serão armazenados num único local físico que, mesmo que seja religiosamente protegido, poderá ficar exposto.

4.3.3. O CESE lembra que, no respeitante à proteção de dados e ao direito ao apagamento dos dados (direito «a ser esquecido»), as instituições e organismos da União estão sujeitos à observância do Regulamento (CE) n.º 45/2001, que proporciona menos proteção do que o RGPD ([15]) de 2016 (que entrará em vigor em maio de 2018), que deve ser respeitado pelos Estados-Membros. O Comité sublinha a complexidade do exercício deste direito e receia que os viajantes, migrantes e requerentes de asilo não estejam em condições de o fazer respeitar:

1) a proteção de dados pessoais deve ser válida para todas as bases de dados existentes, tanto nacionais como europeias, para que a arquitetura global seja protegida;

2) a proteção de dados pessoais é fundamental para que os cidadãos aceitem a imensa rede de vigilância a que estão sujeitos.

4.3.4. O período de conservação dos dados recolhidos pelas autoridades habilitadas não é claramente especificado no texto das propostas, as quais definem o procedimento do direito à retificação e/ou apagamento dos dados, que é partilhado entre o Estado ao qual foi apresentado o pedido e o Estado responsável, mas não definem um prazo de conservação dos dados (artigo 47.º das propostas de regulamento). O Comité recomenda que esse prazo seja fixado e que seja estabelecido um prazo mais curto para os menores (artigo 24.º da Carta dos Direitos Fundamentais da União Europeia), salvo em caso de terrorismo, para que estes possam ter oportunidades de integração.

([14]) AEPD, anexo do relatório final do grupo de peritos de alto nível, maio de 2017.
([15]) Regulamento (UE) 2016/679 (Regulamento Geral sobre a Proteção de Dados).

4.4. *Governação e prestação de contas*

4.4.1. As bases de dados internacionais não estão sujeitas às mesmas regras que os sistemas informatizados europeus. A criação de um formato universal de acesso, que poderá vir a tornar-se internacional, será apenas um elemento técnico que não unificará as regulamentações, ainda que a Interpol tenha certamente de respeitar o artigo 17.º do Pacto das Nações Unidas ([16]). Além disso, a concessão dos direitos de acesso continuará a ser da competência dos Estados-Membros. O CESE considera que este ponto deveria ser abordado nas propostas.

4.4.2. Uma única consulta, e a simbiose das bases de dados europeias emitirá o seu veredito. O Comité sublinha que a burocracia gerada será mais do que proporcional à rapidez ganha. A governação será assegurada pela Comissão no âmbito de um procedimento de controlo em conjunto com os Estados-Membros. O eixo central será a agência eu-LISA, que será responsável, nomeadamente, por criar os procedimentos de recolha de informações sobre o funcionamento da interoperabilidade; receberá as informações dos Estados-Membros e da Europol e apresentará ao Conselho, ao Parlamento Europeu e à Comissão, de quatro em quatro anos, um relatório de avaliação técnica, devendo a própria Comissão elaborar um relatório global um ano após cada relatório da eu-LISA (artigo 68.º das propostas). Para o Comité, estes períodos são excessivamente longos. A avaliação da segurança dos componentes de interoperabilidade [artigo 68.º, n.º 5, alínea d)] deveria ter lugar, pelo menos, anualmente, e a avaliação do impacto nos direitos fundamentais [artigo 68.º, n.º 5, alínea b)] deveria ter lugar, pelo menos, de dois em dois anos.

4.4.3. O Comité lamenta que questões tão fundamentais como as abordadas pelas propostas em apreço sejam deixadas a cargo de agências europeias, cujos processos de recrutamento e funcionamento são obscuros para muitos cidadãos. Considera que é necessário proceder ao cruzamento das boas práticas e associar, para emissão de parecer, todas as autoridades independentes de controlo da utilização de dados (AEPD) e outras agências como a FRA e a Agência da União Europeia para a Segurança das Redes e da Informação (ENISA).

4.4.4. Todas estas novas estruturas e procedimentos serão estabelecidos por meio de atos delegados e atos de execução da Comissão. O Comité gostaria que o objetivo de respeito dos direitos fundamentais e de proteção dos dados pessoais permanecesse inscrito em todos esses atos ao longo do tempo, numa abordagem de melhoria do acolhimento das pessoas nas fronteiras. O CESE recomenda que os cidadãos europeus sejam informados sobre as várias etapas do projeto até à sua conclusão e que as pessoas recebam informação pedagógica sobre os controlos a que são submetidas.

5. **Formação necessária das autoridades de controlo em toda a União**

5.1. O Comité considera que serão necessárias numerosas ações de formação no primeiro período (após 2021), contrariamente ao que avança a Comissão na sua síntese da avaliação de impacto. A Comissão refere um orçamento de 76 milhões de euros por ano. A transição para novos procedimentos exige sempre uma atualização. Neste caso, estão em causa todas as fronteiras da União e os sistemas nacionais. Alguns Estados-Membros, que ainda não possuem sistemas compatíveis, terão de desenvolver um esforço importante e criar interfaces que lhes permitam participar. Para que a interoperabilidade funcione, há que atenuar as disparidades entre Estados-Membros.

5.2. A formação sobre a utilização de dados de qualidade e do UMF será fundamental. O Comité propõe a organização, em conjunto com a CEPOL ([17]), a Frontex, a Europol, etc., de um polo de formação comum para as autoridades habilitadas, incluindo a agência eu-LISA, cujos membros deverão ser objeto de uma rigorosa verificação de competências.

5.3. O sistema MID é único no mundo e, se for bem-sucedido, será um instrumento poderoso. A nova arquitetura exigirá dados da mais alta qualidade. Para que a arquitetura global corresponda às expectativas do projeto, todos os Estados-Membros devem participar ao mesmo nível, sob pena de agravamento das atuais lacunas. Nesse caso, o direito de asilo e o direito de acesso a proteção internacional (artigos 18.º e 19.º da Carta dos Direitos Fundamentais da União Europeia) seriam fragilizados.

6. **Financiamento**

6.1. A arquitetura global proposta assenta ainda em algumas hipóteses: a adoção pelas autoridades de decisão dos sistemas *SES* e *ETIAS*, o *UMF*, o bom funcionamento do *MID* e a segurança do *CIR*. O Comité pergunta-se se dois organismos, designadamente a AEPD e a agência eu-LISA, e eventualmente também a agência ENISA, disporão de recursos humanos e financeiros suficientes. A Comissão propõe um cofinanciamento pela UE e pelos Estados-Membros. O Comité observa que a gestão do Semestre Europeu ainda é efetuada com orçamentos de austeridade e que, além disso, a utilização atual das bases de dados existentes (SIS, VIS, Prüm, *SES*) precisa de ser otimizada em conformidade com os requisitos legais (relatório do grupo de peritos).

([16]) Pacto Internacional sobre os Direitos Civis e Políticos, Organização das Nações Unidas (ONU), artigo 17.º: «1. Ninguém será objeto de intervenções arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem de atentados ilegais à sua honra e à sua reputação. 2. Toda e qualquer pessoa tem direito à proteção da lei contra tais intervenções ou tais atentados».

([17]) CEPOL — Agência da União Europeia para a Formação Policial, com sede em Budapeste, na Hungria.

6.2. O CESE interroga-se sobre o impacto orçamental do Brexit, embora o Reino Unido não faça parte dos países do espaço Schengen, e, de modo mais geral, sobre a futura complexidade da gestão da interoperabilidade nos países europeus que não utilizam o SIS mas que participam noutros sistemas, como o Eurodac.

6.3. O fundo previsto é o Fundo para a Segurança Interna (FSI) — Fronteiras. A entrada em funcionamento está prevista para 2023. O Comité interroga-se se cinco anos serão suficientes para reduzir as disparidades europeias e reunir as condições necessárias para o êxito. O orçamento previsto é de 424,7 milhões de euros num período de nove anos (2019--2027). A União (através do FSI) e os Estados-Membros deverão assumir o encargo. Os Estados deverão tomar as medidas necessárias para que os sistemas atuais funcionem corretamente com a nova arquitetura informática. O Comité considera que a retoma do crescimento deverá ser favorável à realização desses investimentos.

Bruxelas, 23 de maio de 2018.

O Presidente
do Comité Económico e Social Europeu
Luca JAHIER