COMISSÃO EUROPEIA

Bruxelas, 20.7.2010

COM(2010)385 final

COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO

Apresentação geral da gestão da informação no domínio da liberdade, segurança e justiça

COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO

Apresentação geral da gestão da informação no domínio da liberdade, segurança e justiça

1. INTRODUÇÃO

A União Europeia percorreu um longo caminho desde que, em 1985, os líderes de cinco países europeus decidiram, em Schengen, suprimir os controlos nas suas fronteiras comuns. Este acordo deu origem à Convenção de Schengen de 1990, que continha as bases de muitas das políticas de gestão da informação de hoje. A supressão dos controlos nas fronteiras internas impulsionou o desenvolvimento de uma vasta gama de medidas aplicáveis nas fronteiras externas, sobretudo em matéria de emissão de vistos, coordenação das políticas de asilo e de imigração e reforço da cooperação policial, judiciária e aduaneira a nível da luta contra o crime transfronteiras. Nem o espaço Schengen nem o mercado interno da UE poderiam funcionar hoje em dia sem o intercâmbio de dados transfronteiras.

Os atentados terroristas nos Estados Unidos em 2001, bem como os atentados à bomba em Madrid e Londres em 2004 e 2005, desencadearam uma nova dinâmica de desenvolvimento de políticas de gestão da informação da Europa. O Conselho e o Parlamento Europeu adoptaram, em 2006, a Directiva relativa à conservação de dados, destinada a permitir que as autoridades nacionais combatam as formas graves de criminalidade através da conservação dos dados de tráfego de telecomunicações e de dados de localização[1]. O Conselho aprovou subsequentemente a Iniciativa sueca visando simplificar o intercâmbio de informações transfronteiras para efeitos de investigações criminais e de operações de informações criminais. Em 2008, aprovou a Decisão Prüm para acelerar o intercâmbio de perfis de ADN, impressões digitais e dados de registo de veículos no âmbito da luta contra o terrorismo e outras formas de crime. A cooperação transfronteiriça entre unidades de informação financeira, gabinetes de recuperação de bens e plataformas de cibercrime e o recurso dos Estados-Membros à Europol e à Eurojust, constituem instrumentos suplementares na luta contra as formas graves de criminalidade no espaço Schengen.

Imediatamente após os atentados terroristas de 11 de Setembro de 2001, o Governo dos EUA adoptou o Programa de Detecção do Financiamento do Terrorismo para evitar atentados semelhantes através do controlo de transacções financeiras suspeitas. O Parlamento Europeu autorizou recentemente a celebração do acordo entre a União Europeia e os Estados Unidos da América sobre o tratamento de dados de mensagens de pagamentos financeiros e a sua

---

[1] Não há neste momento uma definição harmonizada de «criminalidade grave» a nível da UE. A título de exemplo, a Decisão do Conselho que confere à Europol poderes para consultar o VIS (Decisão 2008/633/JAI do Conselho, JO L 218 de 13.8.2008, p. 129) define «infracções penais graves» remetendo para a lista de infracções constante do mandado de detenção europeu (Decisão 2002/584/JAI do Conselho, JO L 190 de 18.7.2002, p. 1). A Directiva da conservação de dados (Directiva 2002/58/CE, JO L 201 de 31.7.2002, p. 37) deixa aos Estados-Membros a definição de «criminalidade grave». A Decisão Europol (Decisão 2009/371/JAI, JO L 121 de 15.5.2009, p. 37) inclui outra lista de «infracções graves» que é muito semelhante, mas não idêntica, à referida lista do mandado de detenção europeu.

transferência da União Europeia para os Estados Unidos para efeitos do Programa de Detecção do Financiamento do Terrorismo (Acordo TFTP UE-EUA)[2]. O intercâmbio de registos de identificação de passageiros (PNR) e de informações prévias sobre passageiros com países terceiros permitiu igualmente à UE combater o terrorismo e outras formas graves de criminalidade[3]. Tendo celebrado acordos PNR com os EUA, a Austrália e o Canadá, a Comissão decidiu recentemente reconsiderar a abordagem a seguir para estabelecer um sistema de PNR na UE e partilhar esses dados com países terceiros.

As medidas atrás referidas permitiram a livre circulação no espaço Schengen, contribuíram para a prevenção e a luta contra ataques terroristas e outras formas graves de criminalidade e fomentaram o desenvolvimento de uma política comum de vistos e de asilo.

A presente comunicação apresenta, pela primeira vez, uma análise completa das medidas em vigor a nível da UE, já aplicadas, em vias de aplicação ou em estudo que regulam a recolha, o armazenamento e o intercâmbio transfronteiriço de informações pessoais para efeitos de aplicação da lei ou de gestão das migrações. Os cidadãos têm o direito de saber quais os dados pessoais tratados e objecto de intercâmbio, por quem e para que efeitos. O presente documento dá uma resposta clara a estas perguntas. Esclarece a principal finalidade destes instrumentos, a sua estrutura, os tipos de dados pessoais que abrangem, a lista de autoridades que tem acesso aos dados e as disposições que regulam a sua protecção e conservação. Além disso, inclui um número limitado de exemplos que ilustram os resultados práticos destes instrumentos (ver Anexo I). Por último, a comunicação apresenta os princípios essenciais que devem estar na base da concepção e avaliação dos instrumentos de gestão da informação no domínio da liberdade, segurança e justiça.

Ao proceder a uma apresentação geral das medidas que a nível da UE regulam a gestão das informações pessoais e ao propor um conjunto de princípios para o desenvolvimento e a avaliação dessas medidas, a presente comunicação contribui para um diálogo informado entre todos os intervenientes sobre a política a seguir. Em simultâneo, dá uma primeira resposta aos pedidos dos Estados-Membros no sentido do desenvolvimento de uma abordagem «coerente» do intercâmbio de informações pessoais para efeitos da aplicação da lei, recentemente abordada na Estratégia de Gestão da Informação da UE[4], e constitui uma primeira reflexão sobre a eventual necessidade de desenvolver um modelo europeu de intercâmbio de informações baseado numa avaliação das medidas actualmente em vigor neste domínio[5].

A finalidade limitada constitui um elemento essencial da maior parte dos instrumentos analisados na presente comunicação. Um sistema de informações único, que cobrisse toda a União e servisse finalidades múltiplas, ofereceria o nível mais elevado de partilha de informações. Porém, a criação de um sistema deste tipo constituiria uma restrição grosseira e

---

2 Resolução do Parlamento Europeu, P7_TA-PROV(2010)0279 de 8.7.2010.

3 Em contraste com a criminalidade grave, as «infracções terroristas» encontram-se claramente definidas na Decisão-Quadro relativa à luta contra o terrorismo (Decisão-Quadro 2002/475/JAI, JO L 164 de 22.6.2002, p. 3; com a redacção que lhe foi dada pela Decisão-Quadro 2008/919/JAI do Conselho, JO L 330 de 9.12.2008, p. 21).

4 Conclusões do Conselho sobre uma Estratégia de Gestão da Informação para a segurança interna da UE, Conselho da Justiça e Assuntos Internos de 30.11.2009 (Estratégia de Gestão da Informação da UE); *Freedom, Security, Privacy — European Home Affairs in an open world*, relatório do Grupo Consultivo Informal de Alto Nível sobre o Futuro da Política Europeia de Assuntos Internos (Grupo do Futuro), Junho de 2008.

5 Programa de Estocolmo — Uma Europa aberta e segura que sirva e proteja os cidadãos, Documento 5731/10 do Conselho, de 3.3.2010, ponto 4.2.2.

ilegítima do direito à privacidade e à protecção dos dados pessoais e acarretaria grandes dificuldades em termos de concepção e funcionamento. Na prática, as políticas no domínio da liberdade, segurança e justiça foram desenvolvidas de forma gradual, introduzindo uma série de sistemas e instrumentos de informação com várias dimensões, âmbitos e finalidades. A estrutura compartimentada da gestão da informação que foi emergindo nas últimas décadas é mais adequada para salvaguardar o direito dos cidadãos à privacidade do que qualquer alternativa centralizada.

A presente comunicação não abrange as medidas que implicam o intercâmbio de dados não pessoais para efeitos estratégicos, como as análises gerais de risco ou as avaliações de ameaças; também não se analisa aqui em pormenor as disposições de protecção de dados dos instrumentos actualmente em discussão, visto que a Comissão está neste momento a proceder, com base no artigo 16.º do Tratado sobre o Funcionamento da União Europeia, a um exercício separado relativo a um novo quadro normativo abrangente para a protecção de dados pessoais na UE. O Conselho está neste momento a analisar as propostas de directrizes de negociação para um acordo UE-EUA sobre a protecção de dados pessoais transferidos e tratados para efeitos de prevenção, investigação, detecção e repressão de crimes, incluindo o terrorismo, no contexto da cooperação policial e judiciária em matéria penal. Visto que estas negociações deverão definir as formas em que as duas partes poderão assegurar um elevado nível de protecção dos direitos e liberdades fundamentais ao transferirem ou tratarem dados pessoais, mais do que o conteúdo efectivo dessas transferências ou tratamentos de dados, a presente comunicação não abrange esta iniciativa[6].

2. INSTRUMENTOS DA UE QUE REGULAM A RECOLHA, O ARMAZENAMENTO OU O INTERCÂMBIO DE DADOS PESSOAIS PARA EFEITOS DE APLICAÇÃO DA LEI OU DE GESTÃO DA MIGRAÇÃO

Este ponto apresenta uma visão geral dos instrumentos da União Europeia que regulam a recolha, o armazenamento ou o intercâmbio transfronteiriço de dados pessoais para efeitos de aplicação da lei ou gestão da migração. O ponto 2.1 aborda as medidas actualmente em vigor, em vias de aplicação ou em estudo; o ponto 2.2 refere-se às iniciativas previstas no Plano de acção do Programa de Estocolmo[7], fornecendo informações sobre os seguintes aspectos de cada instrumento:

– Antecedentes (medida proposta pelos Estados-Membros ou pela Comissão)[8];

– Finalidade (s) da recolha, armazenamento e intercâmbio de dados;

– Estrutura (sistema de informação centralizado ou intercâmbio de dados descentralizado);

---

6 COM(2010) 252 de 26.5.2010.

7 COM(2010) 171 de 20.4.2010 (Plano de acção do Programa de Estocolmo).

8 No contexto do anterior terceiro pilar da União Europeia, os Estados-Membros e a Comissão partilhavam o direito de iniciativa em matéria de cooperação policial e judiciária. O Tratado de Amesterdão integrou os domínios do controlo das fronteiras externas, vistos, asilo e imigração no (primeiro) pilar comunitário, relativamente ao qual a Comissão tem um direito exclusivo de iniciativa. O Tratado de Lisboa eliminou a estrutura da União em pilares, reafirmando o direito de iniciativa da Comissão. No domínio da cooperação policial e judiciária em matéria penal (incluindo a cooperação administrativa), porém, a legislação continua a poder ser proposta por iniciativa de um quarto dos Estados-Membros.

– Dados pessoais abrangidos;

– Autoridades com acesso aos dados;

– Disposições em matéria de protecção dos dados;

– Normas aplicáveis à conservação dos dados;

– Fase de aplicação;

– Mecanismo de revisão.

2.1. Instrumentos em vigor, em vias de aplicação ou em estudos

Instrumentos da UE que visam reforçar o funcionamento do espaço Schengen e da união aduaneira

O **Sistema de Informação de Schengen** (SIS) nasceu da vontade dos Estados-Membros de criar um espaço sem controlos nas fronteiras internas, facilitando em simultâneo a circulação das pessoas através das suas fronteiras externas[9]. Criado em 1995, este sistema procura assegurar a segurança pública, incluindo a segurança nacional, no espaço Schengen e facilitar a circulação das pessoas utilizando informações comunicadas através deste sistema. O SIS é um sistema de informação centralizado que inclui uma parte nacional em cada país participante e um centro de apoio técnico em França. Os Estados-Membros pode emitir alertas para pessoas procuradas para efeitos de extradição; pode ser recusada a entrada a nacionais de países terceiros; pessoas desaparecidas; testemunhas ou outras pessoas intimadas a comparecer em tribunal; pessoas e veículos sujeitos a controlos excepcionais devido à ameaça que representam para a segurança pública ou nacional; veículos, documentos e armas de fogo perdidos ou roubados e notas de banco suspeitas. Os dados inseridos no SIS incluem nomes e pseudónimos, características físicas, local e data de nascimento, nacionalidade e indicações de pessoas armadas e de pessoas violentas. A polícia, as autoridades aduaneiras e de controlo das fronteiras e as autoridades judiciais no contexto de acções penais têm acesso a esses dados, nos termos das respectivas competências legais. Os serviços de estrangeiros e fronteiras e os postos consulares têm acesso aos dados relativos aos nacionais de países terceiros que constam da lista de proibição de entrada e aos alertas sobre documentos perdidos ou roubados. A Europol também tem acesso a determinadas categorias de dados SIS, incluindo os alertas para a detenção de pessoas para efeitos de extradição e os alertas sobre pessoas sujeitas a controlos excepcionais devido à ameaça que representam para a segurança pública ou nacional. A Eurojust tem acesso aos alertas para a detenção de pessoas para efeitos de extradição e os alertas relativos a testemunhas ou a pessoas convocadas pelos tribunais. Os dados pessoais só podem ser utilizados para efeitos dos alertas específicos para os quais foram fornecidos. Os dados pessoais inseridos no SIS para efeitos de procura de pessoas só podem ser conservados durante o período necessário para cumprir os fins para os quais tiverem sido fornecidos e nunca mais de três anos após a data de inserção. Os dados sobre as pessoas sujeitas a controlos excepcionais devido à ameaça que representam para a segurança pública ou nacional devem ser apagados após um ano. Os Estados-Membros devem adoptar normas nacionais que consagrem um nível de protecção de dados pelo menos semelhante ao que

[9] Convenção 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, JO L 239 de 22.9.2000, p. 19.

decorre da Convenção do Conselho da Europa de 1981 para a protecção das pessoas singulares no que respeita ao tratamento informático dos dados pessoais e da Recomendação de 1987 do seu Comité de Ministros que regula a utilização de dados pessoais no sector da polícia[10]. Embora a Convenção de Schengen não preveja um mecanismo de revisão, os signatários podem propor alterações, na sequência das quais a nova redacção do texto da convenção deve ser aprovada por unanimidade e ratificada pelos parlamentos nacionais. O SIS é plenamente aplicável em 22 Estados-Membros e também na Suíça, Noruega e Islândia. O Reino Unido e a Irlanda participam nos aspectos de cooperação policial da Convenção de Schengen e do SIS, à excepção dos alertas relacionados com nacionais de países terceiros que constam da lista de proibição de entrada. Chipre assinou a Convenção de Schengen, mas ainda não a aplicou. O Liechtenstein deverá começar a aplicá-la em 2010 e estima-se que a Bulgária e a Roménia o façam em 2011. As buscas no SIS dão um resultado quando os dados de uma pessoa ou objecto procurado coincidem com os dados de um alerta lançado. Depois de obterem um resultado, as autoridades estatais podem, através da rede de gabinetes SIRENE, solicitar informações complementares acerca das pessoas visadas por um alerta[11].

A integração de novos Estados-Membros no espaço Schengen implicou um aumento correspondente da dimensão da base de dados do SIS: entre Janeiro de 2008 e 2010, o número total de alertas SIS passou de 22,9 para 31,6 milhões[12]. Antecipando este incremento do volume de dados e a alteração das necessidades dos utilizadores, os Estados-Membros decidiram, em 2001, desenvolver um **Sistema de Informações de Schengen de segunda geração** (SIS II), confiando esta tarefa à Comissão[13]. Actualmente em fase de desenvolvimento, o objectivo do SIS II consiste em garantir um elevado nível de segurança no domínio da liberdade, segurança e justiça, mediante o reforço das funções do sistema de primeira geração, e facilitar a circulação das pessoas utilizando as informações comunicadas através deste sistema. Além das categorias de dados originalmente abrangidas pelo sistema de primeira geração, o SIS II terá capacidade para tratar impressões digitais, fotografias, cópias de mandados de detenção europeus e incluirá disposições de protecção das pessoas cuja identidade esteja a ser indevidamente utilizada e ligações entre diversos alertas. O SIS II permitirá, nomeadamente, a ligação de alertas relativos a uma pessoa procurada por rapto, à pessoa raptada e ao veículo utilizado para a prática do crime. Os direitos de acesso e as regras aplicáveis à conservação de dados são idênticos aos previstos no actual sistema. Os dados pessoais só podem ser utilizados para efeitos dos alertas específicos para os quais foram fornecidos. Os dados pessoais constantes do SIS II devem ser tratados nos termos das disposições específicas previstas nos instrumentos legislativos de base que regulam o sistema (Regulamento (CE) n.º 1987/2006 e Decisão 2007/533/JAI do Conselho], que esclarecem os princípios consagrados na Directiva 95/46/CE, e do Regulamento (CE) n.º 45/2001, da Convenção n.º 108 do Conselho da Europa, do seu Protocolo n.º 181 e da Recomendação das Polícias[14]. O SIS II utilizará a s-TESTA, a rede segura de comunicação de dados da

---

10 Convenção para a protecção das pessoas singulares no que respeita ao tratamento informático dos dados pessoais (ETS n.º 108), Conselho da Europa, 28.1.1981 (Convenção n.º 108 do Conselho da Europa); Recomendação n.º R (87) 15 do Comité de Ministros que regula a utilização de dados pessoais no sector da polícia, Conselho da Europa, 17.9.1987 (Recomendação das Polícias).

11 SIRENE quer dizer *Supplementary Information Request at National Entry*.

12 Documento 5441/08 de 30.1.2008 do Conselho; Documento 6162/10 do Conselho, de 5.2.2010.

13 Regulamento (CE) n.° 1986/2006, JO L 381 de 28.12.2006, p. 1; Regulamento (CE) n.° 1987/2006, JO L 381 de 28.12.2006, p. 4; Decisão 2007/533/JAI, JO L 205 de 7.8.2007, p. 63.

14 Regulamento (CE) n.° 1987/2006, JO L 381 de 28.12.2006, p. 4; Decisão 2007/533/JAI, JO L 205 de 7.8.2007, p. 63; Directiva 95/46/CE, JO L 281 de 23.11.1995, p. 31; Regulamento (CE) n.° 45/2001, JO L 8 de 12.1.2001, p. 1; Convenção para a protecção das pessoas singulares no que respeita ao

Comissão[15]. Quando estiver pronto a funcionar, o sistema será aplicável nos 27 Estados-Membros, Suíça, Liechtenstein, Noruega e Islândia[16]. A Comissão deve apresentar ao Parlamento Europeu e ao Conselho um relatório bienal sobre o desenvolvimento do SIS II e sobre a potencial migração a partir do SIS de primeira geração[17].

O desenvolvimento do **EURODAC** remonta à supressão das fronteiras internas, que tornou necessário estabelecer regras claras para o tratamento dos pedidos de asilo. O EURODAC é um sistema centralizado e automatizado de identificação de impressões digitais, que contém as impressões digitais de determinados nacionais de países terceiros. Em funcionamento desde Janeiro de 2003, destina-se a ajudar a determinar qual o Estado-Membro responsável, nos termos do Regulamento de Dublim, pela apreciação de um pedido de asilo[18]. As impressões digitais dos requerentes com 14 anos ou mais que peçam asilo num Estado-Membro são automaticamente registadas, tal como as dos nacionais de países terceiros retidos devido à entrada ilegal por uma fronteira externa. Comparando essas impressões digitais com os dados do EURODAC, as autoridades nacionais procuram determinar onde é que essas pessoas poderão ter apresentado um pedido de asilo ou terão entrado pela primeira vez na União Europeia. As autoridades podem também comparar as impressões digitais de nacionais de países terceiros que se encontram ilegalmente no seu território com os dados do EURODAC. Os Estados-Membros devem fornecer a lista de autoridades que têm acesso a esta base de dados, que inclui geralmente autoridades responsáveis pelo asilo e imigração, guardas de fronteira e polícia. Os Estados-Membros transferem os dados relevantes para a base de dados central através dos respectivos pontos nacionais de acesso. Os dados pessoais inseridos no EURODAC só podem ser utilizados para facilitar a aplicação do Regulamento de Dublim, estando qualquer outra utilização sujeita a sanções. As impressões digitais dos requerentes de asilo são conservadas durante dez anos; as dos imigrantes clandestinos, durante dois anos. Os registos de requerentes de asilo são apagados depois de estes terem adquirido a nacionalidade de um Estado-Membro; os registos dos imigrantes clandestinos são apagados depois de estes terem obtido uma autorização de residência ou a nacionalidade ou se pura e simplesmente abandonarem o território dos Estados-Membros. A Directiva 95/46/CE é aplicável ao tratamento de dados pessoais ao abrigo deste instrumento[19]. O EURODAC utiliza a rede s-TESTA da Comissão e é aplicável em todos os Estados-Membros, bem como na Noruega, Islândia e Suíça. Está em vias de celebração um acordo que permitirá a ligação do Liechtenstein. A Comissão deve apresentar ao Parlamento Europeu e ao Conselho relatórios anuais sobre o funcionamento da unidade central do EURODAC.

---

tratamento informático dos dados pessoais (ETS n.º 108), Conselho da Europa, 28.1.1981 (Convenção n.º 108 do Conselho da Europa); Recomendação n.º R (87) 15 do Comité de Ministros que regula a utilização de dados pessoais no sector da polícia, Conselho da Europa, 17.9.1987 (Recomendação das Polícias).

15 S-TESTA, que significa *Secure Trans-European Services for Telematics between Administrations*, é uma rede de comunicação de dados financiada pela Comissão que permite o intercâmbio seguro e criptado de informações entre administrações nacionais, instituições, agências e organismos da UE.

16 O Reino Unido e a Irlanda participarão no SIS II, à excepção dos alertas relativos a nacionais de países terceiros que constem da lista de proibição de entrada.

17 Regulamento (CE) n.º 1104/2008 do Conselho, JO L 299 de 8.11.2008, p. 1; Decisão 2008/839/JAI do Conselho, JO L 299 de 8.11.2008, p. 43.

18 Regulamento (CE) n.º 343/2003 do Conselho, JO L 50 de 25.2.2003, p. 1 (Regulamento de Dublim), Regulamento (CE) n.º 2725/2000 do Conselho, JO L 316 de 15.12.2000, p. 1 (Regulamento EURODAC). Estes instrumentos basearam-se na Convenção de Dublim de 1990 (JO C 254 de 19.8.1997, p. 1), que visava determinar qual o Estado-Membro competente para apreciar pedidos de asilo. O sistema de avaliação dos pedidos de asilo é conhecido como o «sistema de Dublim».

19 Directiva 95/46/CE, JO L 281 de 23.11.1995, p. 31.

Na sequência dos atentados do 11 de Setembro de 2001, os Estados-Membros decidiram intensificar a aplicação de uma política comum de vistos, mediante a criação de uma forma de intercâmbio de informações relativas aos vistos de curta duração[20]. A supressão das fronteiras internas veio tornar mais fácil abusar dos regimes de vistos dos Estados-Membros. O **Sistema de Informação sobre Vistos** (SIV) procura dar resposta a ambas as preocupações: destina-se a ajudar a aplicar uma política comum em matéria de asilo, facilitando a apreciação dos pedidos de asilo e os controlos nas fronteiras externas, e contribui para a prevenção de ameaças à segurança interna dos Estados-Membros[21]. O SIS é um sistema de informação centralizado que inclui uma componente nacional em cada país participante e um centro de apoio técnico em França. Utilizará um sistema de correspondências biométricas que permite a comparação fiável de impressões digitais, também utilizado nas fronteiras externas para verificar a identidade dos titulares de vistos. O VIS incluirá dados sobre pedidos de vistos, fotografias, impressões digitais, decisões conexas das autoridades responsáveis pela emissão de vistos e ligações entre pedidos relacionados. As autoridades responsáveis pela emissão de vistos e pelo controlo da imigração e os guardas de fronteira terão acesso a esta base de dados para efeitos de verificação da identidade dos titulares de vistos e da sua autenticidade; a polícia e a Europol podem consultá-la para efeitos de prevenção e combate ao terrorismo e outras formas graves de criminalidade[22]. Os pedidos de vistos podem ser conservados durante cinco anos. Os dados pessoais constantes do VIS devem ser tratados nos termos das disposições específicas previstas nos instrumentos legislativos de base que regulam o sistema (Regulamento (CE) n.º 767/2008 e Decisão 2008/633/JAI do Conselho), que complementam o disposto na Directiva 95/46/CE, no Regulamento (CE) n.º 45/2001, na Decisão-Quadro 2008/977/JAI do Conselho, da Convenção n.º 108 do Conselho da Europa, do seu Protocolo n.º 181 e da Recomendação das Polícias[23]. O VIS será utilizado em todos os Estados-Membros (excepto o Reino Unido e a Irlanda), bem como na Suíça, Noruega e Islândia, com base na rede de comunicação de dados s-TESTA da Comissão. A Comissão avaliará este sistema três anos após o lançamento e, subsequentemente, de quatro em quatro anos.

Por iniciativa da Espanha, o Conselho adoptou em 2004 uma directiva que regula a transmissão de **informações prévias sobre passageiros** (API) pelas transportadoras aéreas às autoridades de controlo de fronteiras[24]. O objectivo deste instrumento é melhorar o controlo das fronteiras e combater a imigração clandestina. Se lhes for solicitado, as transportadoras aéreas devem comunicar às autoridades de controlo de fronteiras o nome, data de nascimento, nacionalidade, ponto de embarque e ponto de entrada na fronteira de passageiros que viajem

---

20 Conselho Extraordinário da Justiça e Assuntos Internos de 20.9.2001.

21 Decisão 2004/512/CE do Conselho, JO L 213 de 15.6.2004, p. 5; Regulamento (CE) n.° 767/2008, JO L 218 de 13.8.2008, p. 60; Decisão 2008/633/JAI do Conselho, JO L 218 de 13.8.2008, p. 129. Ver também a Declaração sobre a luta contra o terrorismo, Conselho Europeu, 25.3.2004.

22 Decisão 2008/633/JAI do Conselho, JO L 218 de 13.8.2008, p. 129.

23 Regulamento (CE) n.° 767/2008, JO L 218 de 13.8.2008, p. 60; Decisão 2008/633/JAI do Conselho, JO L 218 de 13.8.2008, p. 129. Directiva 95/46/CE, JO L 281 de 23.11.1995, p. 31; Regulamento (CE) n.° 45/2001, JO L 8 de 12.1.2001, p. 1; Decisão-Quadro 2008/977/JAI do Conselho, JO L 350 de 30.12.2008, p. 60; Convenção para a protecção das pessoas singulares no que respeita ao tratamento informático dos dados pessoais (ETS n.º 108), Conselho da Europa, 28.1.1981 (Convenção n.º 108 do Conselho da Europa); Protocolo Adicional à Convenção para a protecção das pessoas singulares no que respeita ao tratamento informático dos dados pessoais, relativo às autoridades de controlo e aos fluxos transfronteiriços de dados (ETS n.º 181), Conselho da Europa, 8.11.2001 (Protocolo Adicional n.º 181). Recomendação n.º R (87) 15 do Comité de Ministros que regula a utilização de dados pessoais no sector da polícia, Conselho da Europa, 17.9.1987 (Recomendação das Polícias).

24 Directiva 2004/82/CE do Conselho, JO L 261 de 6.8.2004, p. 24.

de países terceiros para a UE. Esses dados pessoais são obtidos, em geral, da parte dos passaportes de leitura óptica e comunicados às autoridades depois de feito o *check-in*. Após a chegada do voo, as autoridades e as transportadoras podem conservar os dados API durante 24 horas. O sistema API funciona de forma descentralizada, mediante a partilha de informações entre operadores privados e autoridades públicas. Embora este instrumento não permita o intercâmbio de dados API entre Estados-Membros, outras autoridades policiais além dos guardas de fronteira podem solicitar o acesso a essas informações para efeitos de aplicação da lei. Os dados pessoais só podem ser utilizados pelas autoridades públicas para efeitos de controlo de fronteiras e combate à imigração clandestina e devem ser tratados em conformidade com o disposto na Directiva 95/46/CE[25]. Em vigor em toda a UE, este instrumento é utilizado apenas por um número reduzido de Estados-Membros. A Comissão irá rever esta directiva em 2011.

Uma parte importante do Programa de 1992 da Comissão de criação do mercado interno dizia respeito à supressão de todos os controlos e formalidades aplicáveis às mercadorias que circulavam dentro da Comunidade[26]. A eliminação dessas formalidades nas fronteiras internas teve como consequência o aumento dos riscos de fraude, tornando necessário que os Estados-Membros criassem, por um lado, um mecanismo de assistência administrativa mútua para dar apoio à prevenção, investigação e repressão das operações que violem a legislação aduaneira e agrícola da UE e, por outro, promovessem a cooperação aduaneira de modo a permitir a detecção e a repressão da violação das normas aduaneiras nacionais, reforçando nomeadamente o intercâmbio transfronteiriço de informações. Sem prejuízo das competências da UE em relação à união aduaneira[27], a **Convenção de Nápoles II** relativa à assistência mútua e à cooperação entre as administrações aduaneiras destina-se a dar às autoridades aduaneiras nacionais os meios para prevenir e detectar as violações das normas aduaneiras nacionais e ajudá-las a reprimir e punir as violações de normas aduaneiras comunitárias e nacionais[28]. No contexto deste instrumento, um conjunto de unidades de coordenação central solicitam por escrito a assistência das suas congéneres noutros Estados-Membros em investigações criminais relacionadas com a violação de normas aduaneiras nacionais e comunitárias. Estas unidades só podem tratar dados pessoais para as finalidades previstas na Convenção de Nápoles II. Podem transmitir essas informações a autoridades aduaneiras nacionais, organismos de investigações e judiciais e, com o consentimento prévio do Estado-Membro que tiver fornecido os dados, a outras entidades. Os dados podem ser conservados por um período que não exceda o exigido pela finalidade para a qual tiverem sido fornecidos. Os dados pessoais no Estado-Membro receptor beneficiam pelo menos do mesmo nível de protecção previsto no Estado-Membro que fornece os dados e o seu tratamento deve respeitar o disposto na Directiva 95/46/CE e na Convenção n.º 108 do Conselho da Europa[29]. A Convenção de Nápoles II foi ratificada por todos os Estados-Membros. Estes têm a faculdade

---

25 Directiva 95/46/CE, JO L 281 de 23.11.1995, p. 31.

26 Regulamento (CEE) n.º 2913/92, JO L 302 de 19.10.1992.

27 Regulamento (CE) nº 515/97 do Conselho, de 13 de Março de 1997, relativo à assistência mútua entre as autoridades administrativas dos Estados-membros e à colaboração entre estas e a Comissão, tendo em vista assegurar a correcta aplicação das regulamentações aduaneira e agrícola , JO L 82 de 22.3.1997, p. 1, com a redacção que lhe foi dada pelo Regulamento (CE) n.º 766/2008, JO L 218 de 13.8.2008, p. 48.

28 Convenção estabelecida com base no artigo K.3 do Tratado da União Europeia, relativa à assistência mútua e à cooperação entre as administrações aduaneiras, JO C 24 de 23.1.1998, p. 2 (Convenção de Nápoles II).

29 Directiva 95/46/CE, JO L 281 de 23.11.1995, p. 31; Convenção para a protecção das pessoas singulares no que respeita ao tratamento informático dos dados pessoais (ETS n.º 108), Conselho da Europa, 28.1.1981 (Convenção n.º 108 do Conselho da Europa).

de propor alterações, na sequência das quais a nova redacção do texto da convenção deve ser adoptada pelo Conselho de Ministros e ratificada pelos Estados-Membros.

Constituindo um complemento da Convenção de Nápoles II, a Convenção SIA prevê um **Serviço de Informação Aduaneira** (SIA) para dar apoio à prevenção, investigação e repressão de violações graves das legislações nacionais, mediante o aumento – através da divulgação rápida da informação – da eficácia da cooperação entre as autoridades aduaneiras dos Estados-Membros[30]. O SIA, que é gerido pela Comissão, é um sistema de informação centralizado acessível através de terminais em cada Estado-Membro e na Comissão. Inclui dados pessoais relacionados com produtos de base, meios de transporte, empresas, pessoas e mercadorias e numerário retido, apreendido ou confiscado. Estes dados pessoais incluem nomes e pseudónimos, data e lugar de nascimento, nacionalidade, sexo, características físicas, documentos de identidade, morada, eventuais registos de violência, motivo de inserção dos dados no SIA, acção proposta e registo dos meios de transporte. Em caso de retenção, apreensão ou confisco de mercadorias e numerário, só podem ser inseridos no SIA dados biográficos e uma morada. Essas informações só podem ser utilizadas para efeitos de observação, transmissão de informações ou realização de determinadas inspecções ou verificações sobre ou para efeito de análises estratégicas ou operacionais relativas a pessoas suspeitas de terem violado normas aduaneiras nacionais. As autoridades nacionais aduaneiras, fiscais, agrícolas, sanitárias e policiais, a Europol e a Eurojust podem aceder aos dados do SIA[31]. O tratamento de dados pessoais deve respeitar as normas específicas do SIA e o disposto na Directiva 95/46/CE, no Regulamento (CE) n.º 45/2001, na Convenção n.º 108 do Conselho da Europa e na Recomendação das Polícias[32]. Os dados pessoais só podem ser copiados do SIA para outros sistemas de tratamento de dados para efeitos de gestão de riscos ou análises operacionais, a que só os analistas designados pelos Estados-Membros ou a Comissão têm acesso Os dados pessoais copiados do CIS só podem ser conservados durante o tempo exigido pela finalidade para a qual tiverem sido copiados e nunca por mais de 10 anos. O SIA prevê ainda o **ficheiro de identificação dos processos de inquérito aduaneiro** (FIDE) para dar apoio à prevenção, investigação e repressão das violações graves das legislações nacionais[33]. Este ficheiro permite que as autoridades nacionais responsáveis pela realização de investigações aduaneiras identifiquem, ao abrirem um processo de investigação, outras autoridades que possam ter investigado determinadas pessoas ou empresas. Estas autoridades podem inserir no FIDE dados das respectivas investigações, incluindo dados

---

30 Convenção estabelecida com base no artigo K.3 do Tratado da União Europeia sobre a utilização da informática no domínio aduaneiro, JO C 316 de 27.11.1995, p. 34, com a redacção que lhe foi dada pela Decisão 2009/917/JAI, JO L 323 de 10.12.2009, p. 20.

31 A partir de Maio de 2011, a Europol e a Eurojust passarão a ter acesso à leitura dos dados do CIS, nos termos da Decisão 2009/917/JAI do Conselho, JO L 323 de 10.12.2009, p. 20.

32 Convenção estabelecida com base no artigo K.3 do Tratado da União Europeia sobre a utilização da informática no domínio aduaneiro, JO C 316 de 27.11.1995, p. 34, com a redacção que lhe foi dada pela Decisão 2009/917/JAI, JO L 323 de 10.12.2009, p. 20; Directiva 95/46/CE, JO L 281 de 23.11.1995, p. 31; Regulamento (CE) n.° 45/2001, JO L 8 de 12.1.2001, p. 1; Convenção para a protecção das pessoas singulares no que respeita ao tratamento informático dos dados pessoais (ETS n.º 108), Conselho da Europa, 28.1.1981 (Convenção n.º 108 do Conselho da Europa); Recomendação n.º R (87) 15 do Comité de Ministros que regula a utilização de dados pessoais no sector da polícia, Conselho da Europa, 17.9.1987 (Recomendação das Polícias).

33 O FIDE, que significa *Fichier d'Identification des Dossiers d'Enquêtes douanières*, tem como base o Regulamento (CE) n.º 766/2008 do Conselho e o Protocolo estabelecido ao abrigo do artigo 34.º do Tratado da União Europeia, que altera, no que se refere à criação de um ficheiro de identificação dos processos de inquérito aduaneiro, a Convenção sobre a utilização da informática no domínio aduaneiro, JO C 139 de 13.6.2003, p. 1.

biográficos de pessoas sob investigação e a designação, a firma, o número do IVA e a morada da empresa sob investigação. Os dados provenientes de processos de investigação em que não tenham sido detectadas fraudes aduaneiras podem ser conservados por um período máximo de três anos; os dados provenientes de processos de investigação em que tenham sido detectadas fraudes aduaneiras podem ser conservados por um período máximo de seis anos; e os dados provenientes de processos que deram origem a uma condenação ou sanção podem ser conservados por um período máximo de dez anos. O SIA e o FIDE utilizam a rede de comunicação comum, o sistema de interface comum ou o acesso seguro à Internet facultado pela Comissão. O SIA está em vigor em todos os Estados-Membros. A Comissão, em cooperação com os Estados-Membros, apresenta anualmente ao Parlamento Europeu e ao Conselho um relatório sobre o funcionamento do SIA.

Instrumentos da UE destinados a prevenir e combater o terrorismo e outras formas graves de criminalidade transfronteiriça

Na sequência dos atentados terroristas de Março de 2004 em Madrid, foram tomadas várias novas medidas a nível da UE. A pedido do Conselho Europeu, a Comissão apresentou em 2005 uma proposta de instrumento que regula o intercâmbio de informações com base no princípio da disponibilidade[34]. Em vez de aprovar esta proposta, o Conselho adoptou, em 2006, a chamada **Iniciativa sueca**, que racionaliza a partilha, entre Estados-Membros, de eventuais informações disponíveis, também em matéria criminal, que possam ser necessárias para a investigação ou a obtenção de informações criminais[35]. Este instrumento assenta no princípio do «acesso equivalente», segundo o qual as condições a aplicar aos intercâmbios transfronteiriços de dados não devem ser mais restritivas do que as que se aplicam aos intercâmbios nacionais. A Iniciativa sueca funciona de forma descentralizada e permite que as autoridades policiais, aduaneiras ou outras com competência para a investigação de crimes (à excepção dos serviços de informações de segurança, que geralmente lidam com informações mais relacionadas com a segurança nacional) partilhem informações gerais e de natureza criminal com as suas homólogas em toda a UE. Os Estados-Membros devem designar os pontos de contacto nacionais competentes para receber os pedidos urgentes de informação. Esta medida prevê prazos bem definidos para o intercâmbio de informações e exige que os Estados-Membros preencham um formulário para solicitar os dados. Os Estados-Membros devem responder aos pedidos no prazo de 8 horas nos casos urgentes, de uma semana nos casos não urgentes e de duas semanas em todos os restantes casos. A utilização de informações obtidas através deste instrumento está sujeita às legislações nacionais de protecção de dados, segundo as quais os Estados-Membros não podem tratar de forma diferente as informações obtidas de fontes nacionais e as informações provenientes de outros Estados-Membros. O Estado-Membro que fornece as informações pode, contudo, fixar condições para a sua utilização noutros Estados-Membros. Os dados pessoais devem ser tratados nos termos das legislações nacionais de protecção de dados, bem como da Convenção n.º 108 do Conselho da Europa, do seu Protocolo Adicional n.º 181 e da Recomendação das Polícias[36]. Dos 31 signatários desta medida (incluindo os Estados-Membros da UE, bem como

---

34 COM(2005) 490 de 12.10.2005; Conclusões da Presidência – Programa da Haia, 4/5.11.2004. Ver também a Declaração sobre a luta contra o terrorismo, Conselho Europeu, 25.3.2004.

35 Decisão-Quadro 2006/960/JAI do Conselho, JO L 386 de 29.12.2006, p. 89.

36 Convenção para a protecção das pessoas singulares no que respeita ao tratamento informático dos dados pessoais (ETS n.º 108), Conselho da Europa, 28.1.1981 (Convenção n.º 108 do Conselho da Europa); Protocolo Adicional à Convenção para a protecção das pessoas singulares no que respeita ao tratamento informático dos dados pessoais, relativo às autoridades de controlo e aos fluxos transfronteiriços de dados (ETS n.º 181), Conselho da Europa, 8.11.2001 (Protocolo Adicional n.º 181); Recomendação n.º

a Noruega, Islândia, Suíça e Liechtenstein), 12 aprovaram legislação nacional de execução; cinco países preenchem regularmente o formulário de pedido de informações, mas só dois deles o utilizam frequentemente para trocar informações[37]. A Comissão deve apresentar o seu relatório de avaliação ao Conselho até ao final de 2010.

A **Decisão Prüm** tem como base um acordo celebrado em 2005 pela Alemanha, França, Espanha, países do Benelux e Áustria para reforçar a cooperação na luta contra o terrorismo, os crimes transfronteiriços e a imigração clandestina. Em resposta ao interesse manifestado por vários Estados-Membros em assinar esse acordo, a Alemanha propôs, durante a sua Presidência do Conselho de 2007, transformá-lo num instrumento da UE. A Decisão Prüm de 2008, que deve ser transposta até Agosto de 2011, estabelece as normas aplicáveis ao intercâmbio transfronteiriço de perfis de ADN, impressões digitais, dados de registo de veículos e informações acerca de presumíveis autores de planos de ataques terroristas[38]. Visa reforçar a prevenção do crime, em particular o terrorismo e os crimes transfronteiriços, e manter a ordem pública em eventos importantes. Este sistema funcionará de forma descentralizada mediante a interconexão, através dos pontos de contacto nacionais, das bases de dados de ADN, impressões digitais e registo de veículos dos países participantes. Utilizando a rede s-TESTA da Comissão, os pontos de contacto coordenarão a recepção e o envio de pedidos de comparação transfronteiriça de perfis de ADN, impressões digitais e dados de registo de veículos. Os poderes de que dispõem para transmitir este tipo de dados aos utilizadores finais são regulados pela lei nacional. A partir de Agosto de 2011, a comparação de dados será totalmente automatizada. Porém, os Estados-Membros devem ser submetidos a um processo de avaliação rigoroso (que avalia, em especial, o cumprimento dos requisitos técnicos e de protecção de dados) para obterem a autorização para poder passar a partilhar dados de forma automatizada. Os dados pessoais não podem ser trocados ao abrigo deste instrumento antes de os Estados-Membros garantirem um nível de protecção dos dados pelo menos equivalente ao que decorre da Convenção do Conselho da Europa 108, do seu Protocolo Adicional n.º 181 e da Recomendação das Polícias[39]. O Conselho decidirá por unanimidade se estas condições se encontram preenchidas. As informações pessoais só podem ser utilizadas para a finalidades para as quais foram fornecidas, a menos que o Estado-Membro que os fornecer autorizar a sua utilização para outros efeitos. Os cidadãos podem igualmente dirigir-se às respectivas autoridades nacionais de protecção de dados, designadas nos termos da Directiva 95/46/CE, para exercer os direitos que lhes assistem relativamente ao tratamento de dados pessoais ao abrigo deste instrumento. A comparação de perfis de ADN e impressões digitais funcionará numa base «resultado/inexistência de resultado» (anónimo), segundo a qual as autoridades só poderão requerer informações pessoais sobre alguém se a primeira pesquisa que fizeram tiver tido resultados. Esses pedidos de informações adicionais

---

R (87) 15 do Comité de Ministros que regula a utilização de dados pessoais no sector da polícia, Conselho da Europa, 17.9.1987 (Recomendação das Polícias).

37 Estes elementos baseiam-se nas respostas a um questionário, cujos resultados foram apresentados pela Presidência espanhola numa reunião grupo de trabalho *ad hoc* para o intercâmbio de informações do Conselho, em 22 de Junho de 2010.

38 Decisão 2008/615/CE do Conselho, JO L 210 de 6.8.2008, p. 1; Decisão 2008/616/JAI do Conselho, JO L 210 de 6.8.2008, p. 12.

39 Convenção para a protecção das pessoas singulares no que respeita ao tratamento informático dos dados pessoais (ETS n.º 108), Conselho da Europa, 28.1.1981 (Convenção n.º 108 do Conselho da Europa); Protocolo Adicional à Convenção para a protecção das pessoas singulares no que respeita ao tratamento informático dos dados pessoais, relativo às autoridades de controlo e aos fluxos transfronteiriços de dados (ETS n.º 181), Conselho da Europa, 8.11.2001 (Protocolo Adicional n.º 181); Recomendação n.º R (87) 15 do Comité de Ministros que regula a utilização de dados pessoais no sector da polícia, Conselho da Europa, 17.9.1987 (Recomendação das Polícias).

serão geralmente canalizados através da iniciativa sueca. A Decisão Prüm está a ser transposta na UE-27, encontrando-se a Noruega e a Islândia em vias de a assinar[40]. A Comissão deve apresentar um relatório de avaliação ao Conselho em 2012.

Em resposta aos atentados à bomba de Julho de 2005, em Londres, o Reino Unido, a Irlanda, a Suécia e a França propuseram a adopção de um instrumento da UE de harmonização das normas nacionais aplicáveis à conservação de dados. A **Directiva conservação de dados** de 2006 obriga os prestadores de serviços de telefonia e Internet a conservar, para efeitos de investigação, detecção e repressão da criminalidade grave, os dados relativos ao tráfego das comunicações electrónicas e de localização, bem como informações sobre os subscritores (incluindo número de telefone, endereço IP e identificador do equipamento móvel)[41]. A directiva da conservação de dados não regula o acesso aos dados conservados pelas autoridades nacionais nem a sua utilização. O seu âmbito exclui expressamente o conteúdo das comunicações electrónicas; por outras palavras, este instrumento não permite a realização de escutas telefónicas. Esta medida deixa ao critério dos Estados-Membros a definição de «criminalidade grave». Os Estados-Membros podem igualmente determinar quais as autoridades nacionais que têm acesso a esses dados, numa apreciação caso a caso, e quais os procedimentos e condições para permitir o acesso às informações. O período de conservação dos dados varia entre 6 e 24 meses. As Directiva 95/46/CE e 2002/58/CE regulam a protecção de dados pessoais ao abrigo deste instrumento[42]. Seis Estados-Membros ainda não transpuseram plenamente esta medida e os tribunais constitucionais da Alemanha e da Roménia declararam a inconstitucionalidade das respectivas legislações nacionais de transposição. O Tribunal Constitucional alemão considerou que as normas que regulam o acesso e a utilização dos dados, na redacção da legislação nacional, eram inconstitucionais[43]. O Tribunal Constitucional da Roménia considerou que a conservação dos dados, em si, violava o artigo 8.º da Convenção para a Protecção dos Direitos do Homem e das Liberdades Fundamentais (Convenção Europeia dos Direitos do Homem), sendo portanto inconstitucional[44]. A Comissão está actualmente a avaliar este instrumento e deverá apresentar um relatório ao Parlamento Europeu e ao Conselho no final de 2010.

A origem da criação em curso de um **sistema europeu de informação sobre os registos criminais** (ECRIS) remonta a uma iniciativa belga de 2004 que visava impedir que as pessoas condenadas por crimes sexuais pudessem trabalhar com crianças noutros Estados-Membros. No passado, os Estados-Membros recorriam à Convenção de auxílio judiciário mútuo em matéria penal do Conselho da Europa para proceder ao intercâmbio de informações sobre condenações dos respectivos cidadãos, mas o sistema revelou-se insuficiente[45]. O Conselho deu um primeiro passo para a reforma mediante a adopção da Decisão 2005/876/JAI, que exigia que cada Estado-Membro instituísse uma autoridade central responsável pelo envio periódico das condenações dos não nacionais aos Estados-Membros de origem[46]. Este

---

40 Até hoje, dez Estados-Membros foram já autorizados a proceder ao intercâmbio automatizado de perfis de X, cinco foram autorizados a partilhar impressões digitais e sete foram autorizados a partilhar dados de registo de veículos. A Alemanha, Áustria, Espanha e Países Baixos enviaram à Comissão estatísticas parciais da utilização deste instrumento.

41 Directiva 2006/24/CE, JO L 105 de 13.4.2006, p. 54.

42 Directiva 95/46/CE, JO L 281 de 23.11.1995, p. 31; Directiva 2002/58/CE, JO L 201 de 31.7.2002, p. 37 (directiva da privacidade das comunicações electrónicas).

43 Acórdão do Tribunal Constitucional alemão, *Bundesverfassunggericht* 1 BvR 256/08, 11.3.2008.

44 Acórdão n.º 1258 do Tribunal Constitucional da Roménia, 8.10.2009.

45 Convenção europeia de auxílio judiciário mútuo em matéria penal (ETS n.º 30), Conselho da Europa, 20.4.1959. Ver também COM(2005) 10 de 25.1.2005.

46 Decisão 2005/876/JAI do Conselho, JO L 322 de 9.12.2005, p. 33.

instrumento permitiu que os Estados-Membros obtivessem, pela primeira vez e nos termos da legislação nacional, informações sobre condenações anteriores dos seus nacionais noutros Estados-Membros. Era possível requerer estas informações preenchendo um formulário-tipo, em vez de recorrer aos procedimentos de assistência jurídica mútua. Em 2006 e 2007, a Comissão apresentou um pacote legislativo abrangente, composto por três instrumentos: Decisão-Quadro 2008/675/JAI do Conselho, que obriga os Estados-Membros a tomarem em consideração as anteriores decisões de condenação nas novas acções penais; Decisão-Quadro 2009/315/JAI do Conselho, relativa à organização e ao conteúdo do intercâmbio de informações extraídas do registo criminal; e Decisão 2009/316/JAI do Conselho relativa à criação do sistema europeu de informação sobre os registos criminais (ECRIS)[47]. As Decisões-Quadro 2009/315/JAI e 2009/316/JAI do Conselho, que devem ser transpostas até Abril de 2012, destinam-se a definir a forma como os Estados-Membros devem transmitir informações sobre as suas decisões de condenação aos Estados-Membros dos quais os condenados sejam nacionais e também as regras de conservação dos dados e um quadro para o funcionamento do sistema computorizado de intercâmbio das informações. O ECRIS é um sistema de informação descentralizado que interliga as bases de dados dos registos criminais dos Estados-Membros através da rede s-TESTA da Comissão. Um conjunto de autoridades centrais procederá ao intercâmbio de dados sobre novas condenações e registos criminais de cidadãos. Os dados serão cifrados e estruturados segundo um formato pré-determinado, incluindo o seguinte: dados biográficos; a condenação, a sentença e o crime que as justificou; quaisquer informações complementares (incluindo impressões digitais, se for possível). A partir de Abril de 2012, os extractos de registos criminais devem ser fornecidos para acções penais em curso e enviados para as autoridades administrativas ou judiciais competentes, como os organismos com poderes para impedir o acesso de certas pessoas a actividades profissionais sensíveis ou à licença de porte de arma. Os dados pessoais fornecidos para acções penais só podem ser utilizados para este efeito, carecendo a utilização para qualquer outro efeito da autorização do Estado-Membro de que provêm os dados. O tratamento de dados pessoais deve respeitar as normas específicas estabelecidas pela Decisão-Quadro 2009/315/JAI, que incorpora as regras da Decisão 2005/876/JAI do Conselho, pela Decisão-Quadro 2008/977/JAI do Conselho e pela Convenção n.º 108 do Conselho da Europa[48]. Ao eventual tratamento de dados pessoais pelas instituições da UE no contexto do sistema ECRIS, nomeadamente as que se revelem necessárias para garantir a segurança dos dados, é aplicável o Regulamento (CE) n.º 45/2001[49]. Este pacote legislativo não contém normas relativas à conservação de dados, visto que o armazenamento de informações relativas a condenações penais é regulada pela lei nacional. Quinze Estados-Membros participam actualmente num projecto-piloto, tendo nove de entre eles já dado início ao intercâmbio electrónico de informações extraídas de registos criminais. A Comissão deve apresentar ao Parlamento Europeu e ao Conselho dois relatórios de avaliação sobre a aplicação deste pacote legislativo: a Decisão-Quadro 2008/675/JAI deve ser reapreciada em 2011 e a Decisão-Quadro 2009/315/JAI em 2015. A partir de 2016, a Comissão deve também publicar relatórios periódicos sobre o funcionamento do ECRIS.

---

47 Decisão-Quadro 2008/675/JAI do Conselho, JO L 220 de 15.8.2008, p. 32; Decisão-Quadro 2009/315/JAI do Conselho, JO L 93 de 7.4.2009, p. 23; Decisão 2009/316/JAI do Conselho, JO L 93 de 7.4.2009, p. 33. Ver também COM(2005) 10 de 25.1.2005.

48 Decisão-Quadro 2009/315/JAI do Conselho, JO L 93 de 7.4.2009, p. 23; Decisão 2005/876/CE do Conselho, JO L 322 de 9.12.2005, p. 33; Decisão-Quadro 2008/977/JAI do Conselho, JO L 350 de 30.12.2008, p. 60; Convenção para a protecção das pessoas singulares no que respeita ao tratamento informático dos dados pessoais (ETS n.º 108), Conselho da Europa, 28.1.1981 (Convenção n.º 108 do Conselho da Europa).

49 Regulamento (CE) n.° 45/2001, JO L 8 de 12.1.2001, p. 1.

Na sequência de uma iniciativa finlandesa, o Conselho adoptou em 2000 um instrumento que organiza o intercâmbio de informações entre as **unidades de informação financeira** (UIF) dos Estados-Membros para efeitos de combate ao branqueamento de capitais e, mais tarde, ao financiamento do terrorismo[50]. Em regra, as unidades de informação financeira são criadas no âmbito de corpos policiais, autoridades judiciais ou órgãos administrativos que dependem de autoridades financeiras. Devem partilhar os dados financeiros ou de aplicação da lei necessários, incluindo pormenores das transacções financeiras, com os seus homólogos na UE, excepto nos casos em que a divulgação dos dados seja desproporcionada relativamente aos interesses das pessoas singulares ou colectivas. As informações fornecidas para efeitos de análise ou investigação do branqueamento de capitais ou do financiamento do terrorismo podem também ser utilizadas em investigações ou acções penais, a menos que o Estado-Membro de que provêm os dados tenha proibido esta utilização. O tratamento de dados pessoais devem respeitar o disposto na Decisão-Quadro 2008/977/JAI do Conselho, na Convenção n.º 108 do Conselho da Europa e na Recomendação das Polícias[51]. Em 2002, vários Estados-Membros criaram a FIU.net, uma rede descentralizada que procede ao intercâmbio de dados entre unidades de informação financeira utilizando a rede s-TESTA da Comissão[52]. Esta iniciativa conta com vinte unidades de informação financeira. Está neste momento em debate o recurso à aplicação SIENA da Europol para o funcionamento da FIU.net[53]. Depois de avaliar o cumprimento deste instrumento por parte dos Estados-Membros, o Conselho conferiu às UIF, na terceira directiva de luta contra o branqueamento de capitais, poderes para receber, analisar e divulgar avisos de transacções suspeitas relacionadas com o branqueamento de capitais *e* o financiamento do terrorismo[54]. No contexto do plano de acção para os serviços financeiros, a Comissão está a acompanhar, desde 2009, a aplicação da terceira directiva de luta contra o branqueamento de capitais[55].

Na sequência de uma iniciativa proposta pela Áustria, Bélgica e Finlândia, o Conselho adoptou em 2007 um instrumento que visa reforçar a cooperação entre **gabinetes de recuperação de bens** (ARO) para detectar e identificar os produtos do crime[56]. Tal como as unidades IIF, os gabinetes ARO cooperam de forma descentralizada, apesar de não disporem do apoio de uma plataforma em linha. Os gabinetes devem utilizar a Iniciativa sueca para trocar informações, especificando os pormenores dos bens em questão, nomeadamente contas bancárias, bens imóveis e veículos, bem como pormenores sobre as pessoas singulares ou colectivas procuradas, incluindo nome, morada, data de nascimento e informações sobre o accionista ou a empresa. A utilização de informações partilhadas ao abrigo deste instrumento está sujeita às legislações nacionais de protecção de dados sempre que os Estados-Membros não puderem tratar de forma diferente os dados de proveniência nacional e os dados provenientes de outros Estados-Membros. O tratamento de dados pessoais deve respeitar o disposto na Convenção n.º 108 do Conselho da Europa, no seu Protocolo Adicional n.º 181 e

---

50 Decisão 2000/642/JAI do Conselho, JO L 271 de 24.10.2000, p. 4.

51 Decisão-Quadro 2008/977/JAI do Conselho, JO L 350 de 30.12.2008, p. 60; Convenção para a protecção das pessoas singulares no que respeita ao tratamento informático dos dados pessoais (ETS n.º 108), Conselho da Europa, 28.1.1981 (Convenção n.º 108 do Conselho da Europa); Recomendação n.º R (87) 15 do Comité de Ministros que regula a utilização de dados pessoais no sector da polícia, Conselho da Europa, 17.9.1987 (Recomendação das Polícias).

52 http://www.fiu.net/.

53 SIENA quer dizer *Secure Information Exchange Network Application*.

54 Directiva 2005/60/CE, JO L 309 de 25.11.2005, p. 15 (terceira directiva de luta contra o branqueamento de capitais).

55 Ver, por exemplo, *Evaluation of the economic impacts of the Financial Services Action Plan – Final report* (para a Comissão Europeia, DG MARKT), CRA International, 03.2009.

56 Decisão 2007/845/JAI do Conselho, JO L 332 de 18.12.2007, p. 103.

na Recomendação das Polícias[57]. Até agora, mais de vinte Estados-Membros criaram gabinetes ARO. Dada a natureza sensível das informações partilhadas, está neste momento em debate o recurso à aplicação SIENA da Europol para a partilha de dados entre gabinetes ARO. Num projecto-piloto lançado em Maio de 2010, doze gabinetes ARO começaram a utilizá-la para o intercâmbio de informações relevantes para a detecção de bens. A Comissão deve apresentar um relatório de avaliação ao Conselho em 2010.

Em 2008, a Presidência francesa convidou os Estados-Membros a criarem **plataformas nacionais de alerta do cibercrime** e a Europol a criar uma plataforma europeia de alerta do cibercrime, para efeitos de recolha, análise e intercâmbio de informações sobre crimes cometidos na Internet[58]. Os cidadãos podem comunicar às respectivas plataformas nacionais casos de conteúdo ou comportamento ilícito detectados na Internet. A Plataforma Europeia do Cibercrime (ECCP), gerida pela Europol, seria um ponto central de recolha de informações, analisando e partilhando com autoridades policiais nacionais informações relativas ao cibercrime abrangido pelo âmbito das suas competências[59]. A Europol está a trabalhar na aplicação técnica da ECCP e, em breve, poderá recorrer à aplicação SIENA para reforçar a partilha de dados com as plataformas nacionais. Se essa partilha de informações incluir o tratamento de dados pessoais, a Europol deve respeitar o disposto na Decisão Europol (Decisão 2009/371/JAI do Conselho), bem como no Regulamento (CE) n.º 45/2001, na Convenção n.º 108 do Conselho da Europa, no seu Protocolo Adicional n.º 181 e na Recomendação das Polícias[60]. As disposições da Decisão-Quadro 2008/977/JAI do Conselho regulam o intercâmbio de dados pessoais entre os Estados-Membros e a Europol[61]. Na ausência de um instrumento jurídico, não existe qualquer mecanismo de avaliação das plataformas de alerta do cibercrime. No entanto, a Europol já abrange um vasto domínio e, no futuro, irá incluir informações sobre as actividades da ECCP no relatório anual que apresenta ao Conselho, para aprovação, e ao Parlamento Europeu, para informação.

---

57 Convenção para a protecção das pessoas singulares no que respeita ao tratamento informático dos dados pessoais (ETS n.º 108), Conselho da Europa, 28.1.1981 (Convenção n.º 108 do Conselho da Europa); Protocolo Adicional à Convenção para a protecção das pessoas singulares no que respeita ao tratamento informático dos dados pessoais, relativo às autoridades de controlo e aos fluxos transfronteiriços de dados (ETS n.º 181), Conselho da Europa, 8.11.2001 (Protocolo Adicional n.º 181); Recomendação n.º R (87) 15 do Comité de Ministros que regula a utilização de dados pessoais no sector da polícia, Conselho da Europa, 17.9.1987 (Recomendação das Polícias).

58 Conclusões do Conselho acerca da criação de plataformas nacionais de alerta e de uma plataforma europeia de alerta para assinalar infracções constatadas na Internet, Conselho da Justiça e Assuntos Internos, 24.10.2008; Conclusões do Conselho acerca do plano de acção para a aplicação da estratégia concertada de combate ao crime, Conselhos dos Assuntos Gerais, 26.4.2010. A Europol deu um novo nome ao projecto: Plataforma Europeia do Cibercrime (ECCP – *European Cybercrime Platform*).

59 O objectivo da Europol é prevenir e combater o crime organizado, o terrorismo e outras formas graves de criminalidade que afectem dois ou mais Estados-Membros. Ver Decisão 2009/371/JAI do Conselho, JO L 121 de 15.5.2009, p. 37.

60 Decisão 2009/371/CE do Conselho, JO L 121 de 15.5.2009, p. 37; Regulamento (CE) n.° 45/2001, JO L 8 de 12.1.2001, p. 1; Convenção para a protecção das pessoas singulares no que respeita ao tratamento informático dos dados pessoais (ETS n.º 108), Conselho da Europa, 28.1.1981 (Convenção n.º 108 do Conselho da Europa); Protocolo Adicional à Convenção para a protecção das pessoas singulares no que respeita ao tratamento informático dos dados pessoais, relativo às autoridades de controlo e aos fluxos transfronteiriços de dados (ETS n.º 181), Conselho da Europa, 8.11.2001 (Protocolo Adicional n.º 181); Recomendação n.º R (87) 15 do Comité de Ministros que regula a utilização de dados pessoais no sector da polícia, Conselho da Europa, 17.9.1987 (Recomendação das Polícias).

61 Decisão-Quadro 2008/977/JAI do Conselho, JO L 350 de 30.12.2008, p. 60.

Agências e organismos da UE mandatados para dar apoio aos Estados-Membros na prevenção e combate às formas graves de criminalidade transfronteiriça

Criado em 1995, o **Serviço Europeu de Polícia** (Europol) começou a funcionar em 1999 e tornou-se uma agência da UE em Janeiro de 2010[62]. O seu objectivo é ajudar os Estados-Membros a prevenir e combater o crime organizado, o terrorismo e outras formas graves de criminalidade que afectem dois ou mais Estados-Membros. As suas funções principais incluem a recolha, a conservação, o tratamento, a análise e a partilha de informações, o apoio durante as investigações e a prestação de informações e apoio analítico aos Estados-Membros. O principal elemento de ligação entre a Europol e os Estados-Membros são as unidades nacionais Europol (ENU), que destacam agentes de ligação para a Europol. Os chefes das ENU reúnem-se periodicamente para dar assistência à Europol em questões operacionais; o funcionamento da agência é gerido por um conselho de administração e um director. Os instrumentos de gestão da informação da Europol incluem o Sistema de Informações da Europol (SIE), os ficheiros de análise (AWF) e a aplicação SIENA. O EIS contém dados pessoais, nomeadamente identificadores biométricos, condenações penais e ligações ao crime organizado de suspeitos de crimes abrangidos pelo âmbito de competências da Europol. O acesso é limitado às ENU, aos agentes de ligação, ao pessoal autorizado e director da Europol. Os AWF, criados para dar apoio em investigações penais, incluem dados sobre pessoas ou quaisquer outras informações que as ENU decidam eventualmente juntar. O acesso é permitido aos agentes de ligação, mas só os analistas da Europol podem introduzir dados nestes ficheiros. Um sistema de índices permite às ENU e aos agentes de ligação verificar se um dos ficheiros contém informação de interesse para os respectivos Estados-Membros. A aplicação SIENA da Europol é cada vez mais utilizada pelos Estados-Membros para a partilha de dados sensíveis para efeitos de aplicação da lei. A Europol pode proceder ao tratamento de informações, incluindo dados pessoais, no desempenho das suas funções; os Estados-Membros só podem utilizar informações extraídas dos ficheiros da Europol para efeitos de prevenção e combate das formas graves de criminalidade de natureza transfronteiriça. As eventuais restrições impostas à utilização das informações pelo Estado-Membro que as tiver prestado aplicam-se também a outros utilizadores que extraiam esses dados dos ficheiros da Europol. A Europol pode ainda trocar informações pessoais com países terceiros que tenham celebrado acordos operacionais com a Europol e garantam um nível adequado de protecção de dados. Os dados só podem ser conservados durante o tempo necessário ao desempenho das referidas funções. Os AWF podem ser conservados por um período máximo de três anos, com uma possibilidade de prorrogação por mais três anos. O tratamento de dados pessoais pela Europol deve respeitar o disposto nas regras específicas nesta matéria do diploma que regula o seu funcionamento (Decisão 2009/371/JAI do Conselho) e no Regulamento (CE) n.º 45/2001, na Convenção n.º 108 do Conselho da Europa, no seu Protocolo Adicional n.º 181 e na Recomendação das Polícias[63]. As disposições da Decisão-Quadro 2008/977/JAI aplicam-se ao intercâmbio de

---

62 Decisão 2009/371/JAI do Conselho, JO L 121 de 15.5.2009, p. 37, que veio substituir a Convenção com base no artigo K.3 do Tratado da União Europeia que cria um Serviço Europeu de Polícia, JO L 316 de 27.11.1995, p. 2.

63 Decisão 2009/371/CE do Conselho, JO L 121 de 15.5.2009, p. 37; Regulamento (CE) n.° 45/2001, JO L 8 de 12.1.2001, p. 1; Convenção para a protecção das pessoas singulares no que respeita ao tratamento informático dos dados pessoais (ETS n.º 108), Conselho da Europa, 28.1.1981 (Convenção n.º 108 do Conselho da Europa); Protocolo Adicional à Convenção para a protecção das pessoas singulares no que respeita ao tratamento informático dos dados pessoais, relativo às autoridades de controlo e aos fluxos transfronteiriços de dados (ETS n.º 181), Conselho da Europa, 8.11.2001 (Protocolo Adicional n.º 181);

dados pessoais entre os Estados-Membros e a Europol[64]. O tratamento de dados pessoais e a transmissão destes dados a outras partes efectuados pela Europol são controlados por uma instância comum de controlo, composta por membros das autoridades nacionais de controlo, que apresenta relatórios periódicos ao Parlamento Europeu e ao Conselho. A Europol apresenta relatórios anuais de actividades ao Conselho, para aprovação, e ao Parlamento Europeu, para informação.

Além do impacto sobre os vários instrumentos atrás referidos, os atentados terroristas de 11 de Setembro de 2001 aceleraram a criação, em 2002, da **Unidade Europeia de Cooperação Judiciária** (Eurojust)[65]. É competente para intervir nos mesmos tipos de crimes e infracções que a Europol. No âmbito das suas competência e do desempenho das suas funções, os 27 membros nacionais da Eurojust, que constituem o seu Colégio, têm acesso aos dados pessoais de suspeitos e criminosos. Estes dados incluem, nomeadamente: informações biográficas, contactos, elementos do registo de veículos, perfis de ADN, fotografias, impressões digitais, bem como dados sobre tráfego, localização e subscrição fornecidos por prestadores de serviços de telecomunicações. Os Estados-Membros devem partilhar essas informações com a Eurojust para permitir que este organismo desempenhe as suas funções. Todos os dados pessoais relacionados com processos tratados pela Eurojust devem ser inseridos no sistema de gestão automatizada de processos deste organismo, que funciona na rede s-TESTA da Comissão. Um sistema de índices arquiva os dados pessoais e não pessoais relevantes para as investigações em curso. A Eurojust pode proceder ao tratamento de dados pessoais no desempenho das suas funções, mas esta operação deve respeitar o disposto nas normas de protecção de dados do diploma que regula o seu funcionamento (Decisão 2009/426/JAI do Conselho), bem como na Convenção n.º 108 do Conselho da Europa, no seu Protocolo Adicional n.º 181 e na Recomendação das Polícias. As disposições da Decisão-Quadro 2008/977/JAI aplicam-se ao intercâmbio de dados pessoais entre os Estados-Membros e a Eurojust[66]. A Eurojust pode partilhar dados com autoridades nacionais e países terceiros com os quais tiver celebrado acordos, desde que o membro nacional que forneceu os dados tenha autorizado essa partilha e os países terceiros garantam um nível adequado de protecção de dados pessoais. Os dados pessoais podem ser conservados pelo tempo necessário ao cumprimento dos objectivos da Eurojust, mas devem ser apagados depois da conclusão dos processos. Os Estados-Membros devem transpor a nova redacção da base jurídica da Eurojust até Junho de 2011. Até Junho de 2014, a Comissão deve avaliar e propor as alterações que considerar necessárias ao intercâmbio de informações entre os membros nacionais da Eurojust. Até Junho de 2013, a Eurojust deve apresentar ao Conselho e à Comissão um relatório sobre a experiência de conceder acesso ao seu sistema de gestão de processos. Os Estados-Membros podem avaliar, utilizando a mesma base, os direitos de acesso nacionais. Uma instância comum de controlo, composta por juízes nomeados pelos Estados-Membros, controla o tratamento de dados pessoais pela Eurojust e apresenta relatórios anuais ao Conselho. O Presidente do Colégio apresenta ao Conselho um relatório anual de actividades da Eurojust, que é depois enviado pelo Conselho ao Parlamento Europeu.

Recomendação n.º R (87) 15 do Comité de Ministros que regula a utilização de dados pessoais no sector da polícia, Conselho da Europa, 17.9.1987 (Recomendação das Polícias).

64 Decisão-Quadro 2008/977/JAI do Conselho, JO L 350 de 30.12.2008, p. 60.

65 Decisão 2002/187/JAI, JO L 63 de 6.3.2002, p. 1, com a redacção que lhe foi dada pela Decisão 2009/426/JAI, JO L 138 de 4.6.2009, p. 14. Ver também Conselho Extraordinário da Justiça e Assuntos Internos de 20.9.2001.

66 Decisão-Quadro 2008/977/JAI do Conselho, JO L 350 de 30.12.2008, p. 60.

Acordos internacionais que visam prevenir e combater o terrorismo e outras formas graves de criminalidade transnacional

Na sequência dos atentados terroristas de 11 de Setembro de 2001, os EUA adoptaram legislação que obriga as companhias aéreas que efectuam voos com destino, a partir ou através do seu território, a fornecerem às autoridades americanas os dados dos **registos de identificação dos passageiros** (PNR) conservados nos seus sistemas automatizados de reservas. Rapidamente, o Canadá e a Austrália decidiram fazer o mesmo. Uma vez que a legislação da UE na matéria exige uma avaliação prévia do nível de protecção de dados assegurado pelos países terceiros, a Comissão interveio a este respeito e negociou acordos PNR com estes países[67]. A UE assinou um acordo com os EUA em Julho de 2007, com a Austrália em Junho de 2008, bem como um acordo API/PNR com o Canadá em Outubro de 2005[68]. Os acordos concluídos com os EUA e a Austrália são aplicáveis a título provisório, enquanto o acordo com o Canadá permanece em vigor não obstante a cessação de vigência, em Setembro de 2009, da decisão da Comissão relativa à adequação do nível de protecção dos dados pelo Canadá[69]. Crítico em relação aos três acordos, o Parlamento Europeu solicitou à Comissão que os renegociasse com base num conjunto de princípios claro[70]. Graças à transmissão de dados PNR muito antes da partida de um voo, as autoridades policiais podem detectar mais facilmente as potenciais ligações entre certos passageiros e o terrorismo ou outras formas graves de criminalidade transnacional. Por conseguinte, o objectivo de cada acordo é a prevenção e combate de terrorismo e outras formas graves de criminalidade transnacional. Em contrapartida dos dados PNR provenientes da UE, o Departamento de Segurança Interna dos EUA (DHS) partilha os «indícios» resultantes da sua análise dos PNR com as autoridades policiais da UE, com a Europol e a Eurojust; e tanto o Canadá como os EUA se comprometeram, nos acordos respectivos, a cooperar com a UE para efeitos da instauração do seu próprio sistema PNR. Os acordos com os EUA e a Austrália dizem respeito a 19 categorias de dados, incluindo dados biográficos, informações relativas às reservas e aos pagamentos, e informações suplementares; o acordo canadiano prevê 25 tipos de dados semelhantes. As informações suplementares compreendem, nomeadamente, os dados relativos aos bilhetes de ida simples, aos passageiros em espera e aos passageiros registados como ausentes. O acordo dos EUA autoriza igualmente, sob certas condições, a utilização de informações sensíveis. O DHS pode proceder ao tratamento destas informações se a vida do interessado ou de outras pessoas estiverem em perigo, mas deve suprimi-las no prazo de 30 dias. Os dados PNR são enviados a um conjunto de unidades centrais a nível do DHS, do Serviço de fronteiras canadiano (Canada Border Services Agency) e do Serviço das alfândegas australiano (Australian Customs Service), que só podem transferir estes dados para outras autoridades internas competentes em matéria de repressão ou de luta antiterrorismo. No acordo com os EUA, o DHS espera que o nível de protecção de dados que deve assegurar ao tratamento de dados PNR originários da UE não seja «mais estrito» do que o assegurado pelas

---

67 Directiva 95/46/CE (Directiva relativa à protecção dos dados), JO L 281 de 23.11.1995, p. 31.

68 O «pacote» canadiano inclui um compromisso canadiano relativo ao tratamento dos dados API/PNR, a decisão da Comissão sobre a adequação do nível de protecção dos dados pelo Canadá e um acordo internacional (ver JO L 91 de 29.3.2006, p. 49; JO L 82 de 21.3.2006, p. 14). O acordo com os EUA pode ser consultado no JO L 204 de 4.8.2007, p. 16; o acordo com a Austrália pode ser consultado no JO L 213 de 8.8.2008, p. 47.

69 Em 2009, o Canadá apresentou à Comissão, à Presidência do Conselho e aos Estados-Membros da UE um compromisso no sentido de continuar a aplicar o seu compromisso anterior, de 2005, relativo à utilização dos dados PNR da UE. A decisão de adequação da Comissão baseava-se neste compromisso anterior.

70 Resolução do Parlamento Europeu , P7_TA(2010)0144 de 5.5.2010.

autoridades da UE nos seus sistemas PNR nacionais. Se tal não se vier a verificar, poderá suspender certas partes do acordo. A UE considera que o Canadá e a Austrália asseguram um nível de protecção «adequado» dos dados PNR originários da UE se respeitarem as condições dos seus acordos respectivos. Nos EUA, os dados PNR originários da UE são conservados durante sete anos numa base de dados activa e, durante oito anos suplementares, numa base de dados inactiva. Na Austrália, integram uma base de dados activa durante três anos e meio, e são conservados numa base de dados inactiva durante dois anos. Nestes dois países, a base de dados inactiva só é acessível mediante autorização especial. No Canadá, os dados são conservados durante três anos e meio, sendo as informações tornadas anónimas após 72 horas. Cada acordo prevê um reexame periódico e os acordos canadiano e australiano incluem igualmente uma cláusula de denúncia. Na UE, só o Reino Unido dispõe de um sistema PNR. A França, a Dinamarca, a Bélgica, a Suécia e os Países Baixos adoptaram uma legislação *ad hoc* ou testam actualmente a utilização de dados PNR a título de preparação para a introdução de sistemas PNR. Diversos outros Estados-Membros estão a considerar a hipótese de instituir um sistema PNR e o conjunto dos Estados-Membros utilizam, numa base casuística, os dados PNR para fins de aplicação da lei.

Na sequência dos atentados de 11 de Setembro de 2001, o Departamento do Tesouro dos EUA desenvolveu um **Programa de Detecção do Financiamento do Terrorismo** (TFTP) a fim de identificar, vigiar e reprimir os terroristas e os seus apoios financeiros. No âmbito do TFTP, o Departamento do Tesouro dos EUA obrigou, mediante intimações administrativas, a filial americana de uma empresa belga a transferir para os seus serviços conjuntos limitados de mensagens de pagamentos financeiros transmitidas através da sua rede. Em Janeiro de 2010, a referida empresa alterou a arquitectura do seu sistema, o que reduziu em mais de metade o volume dos dados da competência dos EUA que eram normalmente objecto das intimações do Departamento do Tesouro. Em Novembro de 2009, a Presidência do Conselho da União Europeia e o Governo dos Estados Unidos assinaram um acordo provisório relativo ao tratamento e à transferência de dados de mensagens de pagamentos financeiros da UE para os EUA para efeitos do TFTP, acordo este que não foi aprovado pelo Parlamento Europeu[71]. Com base num novo mandato, a Comissão Europeia negociou um novo projecto de acordo com os EUA, tendo apresentado ao Conselho, em 18 de Junho de 2010, uma proposta de decisão do Conselho relativa à conclusão do Acordo entre a União Europeia e os Estados Unidos da América sobre o tratamento de dados de mensagens de pagamentos financeiros e a sua transferência da União Europeia para os Estados Unidos para efeitos do Programa de Detecção do Financiamento do Terrorismo (Acordo TFTP UE-EUA)[72]. Em 8 de Julho de 2010 o Parlamento Europeu autorizou a celebração deste Acordo[73]. O Conselho deve agora adoptar uma decisão do Conselho relativa à celebração deste Acordo, na sequência da qual o Acordo entrará em vigor, através de uma troca de cartas entre as duas Partes. O Acordo TFTP UE-EUA tem por objectivo prevenir, investigar, detectar ou reprimir o terrorismo ou o seu financiamento. Obriga os fornecedores designados de serviços de mensagens de pagamentos financeiros a transferirem para o Departamento do Tesouro dos EUA, com base em avaliações específicas das ameaças geográficas e de pedidos adaptados às necessidades, conjuntos de dados relativos a mensagens de pagamentos financeiros que incluem, nomeadamente, o nome, número de conta, morada e número de identificação da pessoa de origem e do ou dos destinatários das transacções financeiras. O Departamento do Tesouro só pode solicitar estes dados para efeitos do TFTP, e apenas se tiver razões para considerar que existe uma ligação

---

71 Resolução do Parlamento Europeu, P7_TA(2010)0029 de 11.2.2010.

72 COM(2010) 316 final/2 de 18.6.2010.

73 Resolução do Parlamento Europeu, P7_TA-PROV(2010)0279 de 8.7.2010.

entre uma pessoa identificada e o terrorismo ou o seu financiamento. São proibidas a prospecção de dados e a sua transferência no que diz respeito a transacções dentro do Espaço Único de Pagamentos em euros. Os EUA fornecem aos Estados-Membros da UE, à Europol e à Eurojust qualquer «indício» relativo a potenciais planos terroristas na UE, e ajudá-la-ão a estabelecer um sistema equivalente ao TFTP. Se a UE vier a criar um programa deste tipo, as duas partes poderão adaptar os termos desse acordo. Antes de se poder proceder à transferência de dados, cada pedido de informação dos EUA deve ser verificado pela Europol a fim de assegurar que as condições do acordo são respeitadas. As informações extraídas das mensagens de pagamentos financeiros só podem ser conservadas durante o tempo necessário para efeitos de investigações ou acções repressivas específicas; os dados não extraídos só podem ser conservados durante cinco anos. Quando necessário para efeitos da investigação, prevenção ou repressão do terrorismo ou do seu financiamento, o Departamento do Tesouro pode transferir para as autoridades responsáveis pela aplicação da lei, pela segurança pública ou pela luta contra o terrorismo nos Estados Unidos, nos Estados-Membros da UE, para a Europol ou a Eurojust, quaisquer dados pessoais extraídos de mensagens FIN. Pode igualmente partilhar com países terceiros quaisquer indícios relativos a cidadãos e residentes da UE, sob reserva da autorização do Estado-Membro em causa. A observância, pelas Partes, da rigorosa limitação do âmbito de aplicação do acordo ao terrorismo e de outras salvaguardas está sujeita ao acompanhamento por supervisores independentes, incluindo uma pessoa nomeada pela Comissão. Tem a duração de cinco anos e qualquer das partes pode denunciá-lo ou suspendê-lo. Uma equipa de revisão da UE, liderada pela Comissão e que incluirá representantes das duas autoridades responsáveis pela protecção dos dados e um perito judicial, procederá a um reexame do acordo seis anos após a sua entrada em vigor, avaliando em especial a aplicação pelas partes das disposições relativas à limitação das finalidades e à proporcionalidade, bem como ao respeito das suas obrigações em matéria de protecção de dados. A Comissão apresentará um relatório ao Parlamento Europeu e ao Conselho.

2.2. Iniciativas a título do Plano de acção do Programa de Estocolmo

Propostas legislativas a apresentar pela Comissão

No âmbito do Programa de Estocolmo, o Conselho Europeu convidou a Comissão a apresentar três propostas com relevância directa para a presente comunicação: um sistema PNR da UE para efeitos de prevenção, detecção e repressão do terrorismo e de formas graves de criminalidade; um sistema de entrada/saída; e um programa de viajantes registados. O Conselho Europeu salientou que as duas últimas iniciativas deviam ser apresentadas «o mais rapidamente possível». A Comissão incorporou estes três pedidos no Plano de Acção de aplicação do Programa de Estocolmo[74]. Procurará seguidamente concretizar estes pedidos, devendo no futuro avaliar estes instrumentos com base nos princípios de elaboração das políticas enunciados na Secção 4.

Em Novembro de 2007, a Comissão apresentou uma proposta de decisão-quadro do Conselho relativa à utilização dos dados PNR para efeitos de aplicação da lei[75]. Esta iniciativa contou com o apoio do Conselho e viria a ser subsequentemente alterada para ter em conta as alterações propostas pelo Parlamento Europeu e a posição da Autoridade Europeia para a Protecção de Dados. Todavia, tornou-se caduca com a entrada em vigor do Tratado de Lisboa.

---

74 «Programa de Estocolmo — Uma Europa aberta e segura que sirva e proteja os cidadãos», documento do Conselho 5731/10 de 3.3.2010; COM(2010) 171 de 20.4.2010 (Plano de acção do Programa de Estocolmo).

75 COM(2007) 654 de 6.11.2007.

Tal como indicado no Plano de Acção do Programa de Estocolmo, a Comissão está agora a trabalhar para apresentar, no início de 2011, um pacote em matéria de **registo de identificação de passageiros**, que consiste no seguinte: uma comunicação relativa a uma estratégia PNR externa da UE que estabeleça os grandes princípios orientadores que deverão nortear a negociação de acordos com países terceiros; directrizes de negociação para a renegociação de acordos PNR com os EUA e a Austrália; e directrizes de negociação para um novo acordo com o Canadá. A Comissão encontra-se igualmente a elaborar uma nova proposta PNR da UE.

Em 2008, a Comissão avançou com um certo número de sugestões para desenvolver uma gestão integrada das fronteiras a nível da UE, facilitando as viagens para os nacionais de países terceiros e ao mesmo tempo reforçando a segurança interna[76]. Sublinhando que as pessoas que excedem o período de permanência autorizado constituíam a categoria mais numerosa de imigrantes em situação irregular na UE, propunha a introdução eventual de um **sistema de entrada/saída** para os nacionais de países terceiros que entram na UE para estadas de curta duração até três meses. Este sistema permitiria registar a data e o local de entrada, bem como o período de estada autorizado, e transmitiria alertas automáticos às autoridades competentes em caso de inobservância do período de estada autorizado. Baseado no controlo dos dados biométricos, exploraria o mesmo sistema de correspondências biométricas e o mesmo equipamento operacional utilizados pelo SIS II e pelo VIS. A Comissão está actualmente a realizar uma avaliação de impacto e, tal como referido no Plano de Acção do Programa de Estocolmo, tentará apresentar uma proposta legislativa em 2011.

O estabelecimento de um **programa de viajantes registados** (PVR) constituía a terceira proposta a examinar[77]. Este programa permitiria simplificar os controlos nas fronteiras para determinadas categorias de viajantes regulares provenientes de países terceiros que podiam, após serem submetidos a um adequado exame prévio, entrar na UE através de barreiras automáticas. O PVR basear-se-ia igualmente num controlo da identidade através de dados biométricos e permitiria uma passagem gradual do actual controlo geral nas fronteiras para uma nova abordagem baseada no risco individual. A Comissão realizou uma análise de impacto e, em consonância com o Plano de Acção do Programa de Estocolmo, espera apresentar uma proposta legislativa em 2011.

Iniciativas a estudar pela Comissão

No âmbito do Programa de Estocolmo, o Conselho Europeu convidou a Comissão a examinar três iniciativas com relevância directa para a presente comunicação: os meios que permitam detectar o financiamento do terrorismo a nível da UE; a possibilidade e utilidade de desenvolver um sistema europeu de autorização de viagem; e a necessidade e o valor acrescentado de criar um sistema europeu de indexação de ficheiros policiais. A Comissão incluiu igualmente estas iniciativas no seu Plano de Acção do Programa de Estocolmo. Deverá agora avaliar a sua viabilidade e oportunidade, se for caso disso, e a forma de os aplicar na prática com base nos princípios de elaboração de políticas enunciados na Secção 4.

O Acordo TFTP UE-EUA especifica que a Comissão Europeia realizará um estudo sobre a eventual introdução de um **sistema da UE de detecção do financiamento do terrorismo** equivalente ao TFTP dos EUA, que permita transferências de dados mais direccionadas da

[76] COM(2008) 69 de 13.2.2008.
[77] COM(2008) 69 de 13.2.2008.

UE para os EUA. O projecto de decisão do Conselho relativa à celebração deste acordo convida igualmente a Comissão a apresentar ao Parlamento Europeu e ao Conselho, o mais tardar um ano após a entrada em vigor do Acordo TFTP UE-EUA, um enquadramento jurídico e técnico para a extracção de dados no território da UE[78]. No prazo de três anos a contar da entrada em vigor do Acordo, a Comissão deve apresentar um relatório sobre o desenvolvimento de um sistema equivalente da UE. Se o mesmo não tiver sido criado no prazo de cinco anos a contar da data de entrada em vigor do Acordo, a UE pode decidir rescindir o Acordo. O Acordo TFTP UE-EUA prevê também um compromisso dos EUA para cooperar com a UE e prestar-lhe assistência e aconselhamento se a UE decidir criar um sistema deste tipo. Sem antecipar qualquer decisão sobre este ponto, a Comissão começou a estudar as implicações em matéria de protecção de dados e de recursos, bem como a nível prático, de uma decisão deste tipo. Tal como indicado no Plano de Acção do Programa de Estocolmo, a Comissão apresentará em 2011 uma comunicação sobre a viabilidade de um Programa da UE de Detecção do Financiamento do Terrorismo (TFTP UE).

Na sua comunicação de 2008 sobre a gestão integrada das fronteiras, a Comissão sugeriu a eventual criação de um **sistema electrónico de autorização de viagem** (ESTA) para nacionais de países terceiros não sujeitos à obrigação de visto[79]. No âmbito deste programa, seria solicitado aos nacionais de países terceiros elegíveis que apresentassem por via electrónica um pedido antes da viagem acompanhado dos dados biográficos, dos dados do passaporte e de informações sobre a sua viagem. Relativamente ao procedimento de visto, o ESTA proporcionaria um método mais rápido e mais simples para controlar se uma pessoa satisfaz as necessárias condições de entrada. A Comissão está a realizar um estudo sobre as vantagens, desvantagens e implicações práticas da introdução do ESTA. Tal como indicado no Plano de Acção do Programa de Estocolmo, tenciona apresentar em 2011 uma comunicação sobre a viabilidade de criação de um sistema deste tipo.

Durante a sua Presidência do Conselho em 2007, a Alemanha lançou um debate sobre a eventual criação de um **sistema europeu de indexação de ficheiros policiais** (EPRIS)[80]. O EPRIS ajudaria os agentes responsáveis pela aplicação da lei a localizar a informação no conjunto da UE, em especial no que se refere às relações entre pessoas suspeitas de participar na criminalidade organizada A Comissão apresentará ao Conselho em 2010 um projecto de especificações para a realização de um estudo sobre a viabilidade do EPRIS. Tal como indicado no Plano de Acção do Programa de Estocolmo, tenciona apresentar em 2012 uma comunicação sobre a viabilidade de criação de um sistema deste tipo.

3. ANÁLISE DOS INSTRUMENTOS EM VIGOR, EM IMPLEMENTAÇÃO OU EM ESTUDO

A apresentação geral acima descrita suscita as seguintes observações preliminares:

Estrutura descentralizada

Entre os vários instrumentos actualmente em vigor, em implementação ou em estudo, apenas seis implicam a recolha ou conservação de dados pessoais a nível da UE, a saber, o SIS (e o SIS II), o VIS, o EURODAC, o SIA, a Europol e a Eurojust. Todas as outras medidas regem o

[78] Documento do Conselho 11222/1/10 REV 1 de 24.6.2010; Documento do Conselho 11222/1/10 REV1 COR1 de 24.6.2010.

[79] COM(2008) 69 de 13.2.2008.

[80] Documento do Conselho 15526/1/09 de 2.12.2009.

intercâmbio ou a transferência descentralizada transfronteiras para países terceiros de dados pessoais recolhidos a nível nacional pelas autoridades públicas ou por empresas privadas. A maioria dos dados pessoais é recolhida e conservada a nível nacional; a UE procura introduzir valor acrescentado, permitindo, em determinadas condições, o intercâmbio de tais informações com parceiros da UE e países terceiros. A Comissão apresentou recentemente ao Parlamento Europeu e ao Conselho uma proposta alterada que cria uma agência para a gestão operacional de sistemas informáticos de grande escala no domínio da liberdade, da segurança e da justiça[81]. A tarefa da futura agência TI consistirá em assegurar a gestão operacional do SIS II, do VIS e do EURODAC, e de qualquer outro eventual sistema TI no domínio da liberdade, da segurança e da justiça, por forma a assegurar um funcionamento destes sistemas numa base permanente e, por conseguinte, um fluxo ininterrupto de informação.

Limitação da finalidade

A maioria dos instrumentos acima analisados tem uma finalidade única: o EURODAC destina-se a permitir o funcionamento do sistema de Dublim; o API a melhorar o controlo das fronteiras; a Iniciativa sueca a reforçar as investigações penais e as operações de informações criminais; a Convenção Nápoles II a ajudar a prevenir, detectar, reprimir e punir a fraude aduaneira; o SIA a dar apoio à prevenção, investigação e repressão de violações graves das legislações nacionais, mediante o aumento da eficácia da cooperação entre as autoridades aduaneiras nacionais; o ECRIS, as UIF e os ARO, a melhorar a partilha transfronteiras de dados relativos a domínios específicos; a Decisão Prüm, a Directiva relativa à conservação de dados, o TFTP e o PNR a combater o terrorismo e formas graves de criminalidade. O SIS, o SIS II e o VIS parecem constituir as principais excepções a este respeito: o objectivo inicial do VIS, que consistia em facilitar o intercâmbio transfronteiras de dados sobre vistos, viria a ser alargado posteriormente para abarcar também a prevenção e a luta contra o terrorismo e formas graves de criminalidade. O SIS e o SIS II destinam-se a assegurar um elevado nível de segurança no espaço de liberdade, de segurança e de justiça e a facilitar a circulação das pessoas através das informações comunicadas através deste sistema. Com excepção destes sistemas de informação centralizados, a limitação da finalidade parece constituir um elemento de base da estrutura das medidas de gestão da informação a nível da UE.

Sobreposições potenciais entre as funções dos diferentes instrumentos

Os mesmos dados pessoais podem ser recolhidos através de diversos sistemas diferentes, mas só podem ser utilizados para uma finalidade limitada ao abrigo de um determinado instrumento (à excepção do VIS, do SIS e do SIS II). Por exemplo, os dados biográficos de uma pessoa, incluindo o seu nome e a data e local de nascimento, podem ser tratados através do SIS, SIS II, VIS, API, SIA, Iniciativa sueca, Decisão Prüm, ECRIS, UIF, ARO, Europol, Eurojust e acordos PNR e TFTP. No entanto, tais dados só podem ser tratados para efeitos do controlo nas fronteiras no caso da API; para a prevenção, investigação e repressão da fraude aduaneira no caso da SIA; para investigações e operações de informações criminais no caso da Iniciativa sueca; para efeitos da prevenção do terrorismo e da criminalidade transfronteiras no caso da Decisão Prüm; para efeitos de análise dos antecedentes criminais no caso da ECRIS; para investigar as ligações de uma pessoa com redes de criminalidade organizada e de terrorismo no caso das UIF; para a detecção de bens no caso dos ARO; para investigar e ajudar a reprimir a criminalidade grave transfronteiriça no caso da Europol e da Eurojust; para prevenir e combater o terrorismo e outras formas graves de criminalidade transnacional no

[81] COM(2010) 93 de 19.3.2010.

caso do PNR; e para identificar e reprimir o terrorismo e os seus financiadores no caso do TFTP. Dados biométricos, como as impressões digitais e as fotografias, podem ser tratados através do SIS II, do VIS, do EURODAC, da Iniciativa sueca, da Decisão Prüm, da ECRIS, da Europol e da Eurojust — mas, de novo, em função apenas das suas finalidades respectivas. A Decisão Prüm é o único instrumento que permite o intercâmbio transfronteiras de perfis de ADN anónimos (embora tais dados possam igualmente ser transmitidos à Europol e à Eurojust). Outras medidas tratam dados pessoais altamente especializados e relevantes para os seus objectivos específicos: os sistemas de PNR tratam as informações relativas às reservas de avião dos passageiros; o FIDE, dados relevantes para a investigação de fraudes aduaneiras; a Directiva relativa à conservação de dados, endereços IP e identificadores de equipamentos móveis; o ECRIS, os registos criminais; os AROs, os bens privados e as informações relativas às empresas; as plataformas de alerta da cibercriminalidade, os crimes praticados com recurso à Internet; a Europol, ligações a redes criminosas; e o TFTP, os dados de mensagens de pagamentos financeiros. Só o intercâmbio transfronteiras de dados e de informações criminais para efeitos de investigações apresenta importantes sobreposições entre as funções dos diferentes instrumentos. Do ponto de vista jurídico, a Iniciativa sueca seria suficiente para proceder ao intercâmbio de *todos* os tipos de informações que têm interesse para tais investigações (desde que o intercâmbio desses dados pessoais seja permitido ao abrigo da legislação nacional). Todavia, numa perspectiva operacional, pode ser preferível utilizar a Decisão Prüm para partilhar dados relativos a perfis de ADN e a impressões digitais, na medida em que o seu sistema de acerto/não acerto (*hit/no hit*) assegura respostas imediatas e o seu método de partilha automatizada de dados garante um elevado nível de segurança dos dados[82]. Da mesma forma, pode revelar-se mais eficiente para as UIF, os ARO e as plataformas de alerta da cibercriminalidade estabelecerem ligações directas com os seus homólogos da UE, sem terem de preencher os formulários exigidos pela Iniciativa sueca para solicitar pedidos de informações.

Direitos de acesso controlado

Os direitos de acesso aos instrumentos criados na lógica da luta contra o terrorismo e formas graves de criminalidade são normalmente concedidos apenas a uma parte restrita dos serviços repressivos, designadamente os serviços policiais, as autoridades de controlo das fronteiras e as autoridades aduaneiras. Os direitos de acesso às medidas que correspondem à lógica «Schengen» são em princípio concedidos aos serviços de imigração e, sob certas condições, aos serviços policiais, às autoridades de controlo das fronteiras e às autoridades aduaneiras. O fluxo de informação é controlado pelas interfaces nacionais no caso dos sistemas centralizados SIS e VIS e através dos pontos de contacto nacionais ou unidades centrais de coordenação no caso dos instrumentos descentralizados, tais como a Decisão Prüm, a Iniciativa sueca, a Convenção Nápoles II, a ECRIS, o TFTP, os acordos PNR, as UIF, os ARO e as plataformas de alerta da cibercriminalidade.

Disparidade das normas em matéria de conservação de dados

Os períodos de conservação dos dados variam muito em função dos objectivos dos diversos instrumentos. O acordo PNR com os EUA prevê o período mais longo de conservação dos

---

82 A Decisão Prüm (Decisão 2008/615/JAI do Conselho, JO L 210 de 6.8.2008, p. 1) é acompanhada de uma decisão de execução (Decisão 2008/616/JAI do Conselho, JO L 210 de 6.8.2008, p. 12), que visa garantir a utilização de medidas que correspondem às técnicas mais recentes para assegurar a protecção e segurança dos dados, bem como procedimentos de cifragem e de autorização de acesso aos dados, incluindo regras específicas que regulam a admissibilidade das consultas.

dados — 15 anos, enquanto a API prevê o período mais curto — 24 horas. Os acordos PNR introduzem uma distinção interessante entre dados em utilização activa e passiva: após um certo tempo, as informações devem ser arquivadas e só podem ser «desbloqueadas» mediante autorização especial. A utilização feita pelo Canadá dos dados PNR originários da UE ilustra bem esta abordagem: as informações devem ser tornadas anónimas após 72 horas, mas permanecem disponíveis para os agentes autorizados durante três anos e meio.

Gestão eficaz da identidade

Diversas medidas acima analisadas, incluindo o futuro SIS II e o VIS, destinam-se a permitir a verificação de identidade através do uso de dados biométricos. Espera-se que a aplicação do SIS II venha reforçar a segurança no domínio da liberdade, da segurança e da justiça, ao facilitar, por exemplo, a identificação de indivíduos relativamente aos quais foi emitido um mandado de detenção europeu, das pessoas a quem foi recusada a entrada no espaço Schengen e daqueles que estão a ser procurados por outras razões ligadas a investigações específicas (como pessoas desaparecidas ou testemunhas em processos judiciais), independentemente da disponibilidade ou autenticidade dos documentos de identificação. A aplicação VIS deverá facilitar o processo de emissão e de gestão dos vistos.

Soluções da UE para garantir a segurança dos dados

Para o intercâmbio de informações «sensíveis» através das fronteiras europeias, os Estados-Membros preferem soluções da UE. Diversos instrumentos de diferentes dimensões, estruturas e finalidades recorrem à rede de comunicação de dados s-TESTA, financiada pela Comissão, para efeitos da partilha de informações sensíveis. Entre eles contam-se os sistemas centralizados SIS II, VIS e EURODAC, o sistema Prüm descentralizado, os instrumentos ECRIS e UIF, bem como a Europol e a Eurojust. O SIA e o FIDE utilizam a rede de comunicação comum, o sistema de interface comum ou o acesso seguro à Internet facultado pela Comissão. Entretanto, a aplicação de intercâmbio seguro de informações SIENA da Europol parece ter-se tornado a aplicação preferida para algumas iniciativas recentes relativas a uma transferência de dados segura: está a ser debatida a possibilidade de a FIU.net, os ARO e as plataformas de alerta da cibercriminalidade passarem a operar com base nesta aplicação.

Disparidade dos mecanismos de reexame

Os instrumentos acima analisados incluem um amplo conjunto de diferentes mecanismos de reexame. No caso de sistemas de informação complexos, como o SIS II, o VIS e o EURODAC, a Comissão tem de apresentar ao Parlamento Europeu e ao Conselho relatórios anuais ou bienais sobre o funcionamento ou estado de avanço destes sistemas. Os instrumentos descentralizados de intercâmbio de informações exigem que a Comissão apresente às outras instituições um único relatório de avaliação poucos anos depois da aplicação: a Directiva relativa à conservação de dados, a Iniciativa sueca e as medidas ARO deverão ser avaliadas em 2010; a Decisão Prüm em 2012; e o ECRIS em 2016. Os três acordos PNR prevêem reexames periódicos e *ad hoc*, e dois deles também incluem cláusulas de caducidade. A Europol e a Eurojust apresentam relatórios anuais ao Conselho, que os transmite para informação ao Parlamento Europeu. Estas considerações sugerem que a estrutura actual de gestão da informação na UE não é conducente à adopção de um mecanismo de avaliação único para o conjunto dos instrumentos. Tendo em conta esta diversidade, é essencial que qualquer futura alteração de um instrumento no domínio da gestão da informação tenha em conta o seu potencial impacto em todas as outras medidas que

regem a recolha, conservação ou o intercâmbio de dados pessoais no domínio da liberdade, da segurança e da justiça.

4. PRINCÍPIOS DE ELABORAÇÃO DE POLÍTICAS

A secção 2 descreve várias iniciativas que a Comissão Europeia tem aplicado, apresentou ou estudou nos últimos anos. Devido ao grande número de ideias novas e a um *corpus* de legislação cada vez mais relevante no domínio da gestão da segurança interna e da gestão da migração, é conveniente definir um conjunto de princípios fundamentais para guiar o lançamento e a avaliação de propostas de acções nos próximos anos. Estes princípios baseiam-se e devem completar princípios gerais, consagrados pelos Tratados da UE, a jurisprudência do Tribunal de Justiça Europeu e do Tribunal Europeu dos Direitos do Homem e os acordos interinstitucionais pertinentes entre o Parlamento Europeu, o Conselho e Comissão Europeia. A Comissão propõe elaborar e aplicar novas iniciativas e avaliar os instrumentos existentes com base nas duas categorias de princípios seguintes:

Princípios substantivos

Proteger os direitos fundamentais, em especial o direito à privacidade e à protecção dos dados

A protecção dos direitos fundamentais das pessoas, tal como consagrada na Carta dos Direitos Fundamentais da União Europeia, particularmente o direito à privacidade e à protecção dos dados pessoais, constituirá uma prioridade para a Comissão aquando da elaboração de novas propostas que impliquem o tratamento de dados pessoais no domínio da segurança interna e da gestão dos fluxos migratórios. Os artigos 7.° e 8.° da Carta estabelecem que «todas as pessoas têm direito ao respeito pela sua vida privada e familiar» e «à protecção dos dados de carácter pessoal que lhes digam respeito»[83]. O artigo 16.° do Tratado sobre o Funcionamento da União Europeia (TFUE), que é vinculativo para as actividades dos Estados-Membros e das instituições, órgãos e organismos da União, reafirma o direito de todas as pessoas «à protecção dos dados de carácter pessoal que lhes digam respeito»[84]. Quando elaborar novos instrumentos baseados na utilização das tecnologias da informação, a Comissão deverá seguir uma abordagem baseada na tomada em conta do respeito da vida privada desde a sua concepção (*privacy by design*). Para este efeito, integrará a protecção dos dados pessoais na base tecnológica dos instrumentos propostos, limitando o tratamento dos dados ao estritamente necessário tendo em conta a finalidade preconizada e só autorizando o acesso aos dados às entidades que tenham necessidade de os conhecer[85].

Necessidade

A ingerência de uma autoridade pública no exercício pelas pessoas do direito ao respeito da sua vida privada pode ser necessária no interesse da segurança nacional, da segurança pública

---

83 Carta dos Direitos Fundamentais da União Europeia, JO C 83 de 30.3.2010, p. 389.

84 Versões consolidadas do Tratado da União Europeia e do Tratado sobre o Funcionamento da União Europeia, JO C 83 de 30.3.2010.2008, p. 1.

85 Para uma descrição completa do princípio *privacy by design*, ver o parecer da Autoridade Europeia de Protecção de Dados sobre a promoção da confiança na sociedade da informação graças ao reforço da protecção dos dados e da vida privada (Promoting Trust in the Information Society by Fostering Data Protection and Privacy) de 18.3.2010.

ou da prevenção da criminalidade[86]. A jurisprudência do Tribunal Europeu dos Direitos do Homem estabelece três condições em que tais restrições se podem justificar: se estiverem legalmente previstas, se prosseguirem um fim legítimo e se forem necessárias numa sociedade democrática. A ingerência no direito ao respeito da vida privada é considerada como necessária se corresponder a uma necessidade social imperiosa, se for proporcionada ao fim preconizado e se os motivos invocados pelas autoridades públicas para a justificar forem pertinentes e suficientes[87]. A Comissão, em todas as suas futuras propostas, avaliará a incidência da iniciativa em causa sobre o direito das pessoas ao respeito da vida privada e à protecção dos dados pessoais e referirá em que medida tal incidência é necessária, e de que forma a solução proposta é proporcionada à finalidade legítima que constituem a manutenção da segurança interna na União Europeia, a prevenção da criminalidade ou a gestão dos fluxos migratórios. O respeito das normas relativas à protecção dos dados pessoais será em todas as circunstâncias objecto de um controlo por uma autoridade independente a nível nacional ou da UE.

Subsidiariedade

A Comissão procurará justificar as suas novas propostas em função dos princípios da subsidiariedade e da proporcionalidade, em conformidade com o artigo 5.° do Protocolo (n.° 2) anexo ao Tratado da União Europeia. Qualquer nova proposta legislativa incluirá uma ficha com elementos que permitirão avaliar o respeito do princípio da subsidiariedade, tal como enunciado no artigo 5.° do Tratado da União Europeia. Essa ficha incluirá elementos que permitirão avaliar o impacto financeiro e socioeconómico da proposta e, quando se trate de uma directiva, as suas implicações para a regulamentação a aplicar pelos Estados-Membros[88]. As razões que permitem concluir que um objectivo da UE pode ser melhor alcançado a nível da UE terão por base indicadors qualitativos. As propostas legislativas deverão assegurar que qualquer encargo para a UE, bem como para os governos nacionais, as autoridades regionais, os operadores económicos e os cidadãos seja reduzido ao mínimo e proporcionado ao objectivo alcançar. No caso de propostas visando concluir novos acordos internacionais, essa ficha mencionará os efeitos previstos da proposta a nível das relações com os países terceiros em causa.

Gestão rigorosa dos riscos

Os intercâmbios de informações no domínio da liberdade, da segurança e da justiça visam normalmente analisar as ameaças que pesam sobre a segurança, destacar as tendências das actividades criminosas ou avaliar os riscos associados a determinados domínios da acção[89]. Os riscos estão muitas vezes, mas não necessariamente, associados a pessoas cujo comportamento anterior ou padrão de comportamento indica a persistência de um risco no futuro. Todavia, os riscos devem ser avaliados com base em provas e não em hipóteses. É essencial para qualquer medida de gestão da informação prever uma verificação da

---

86 Ver artigo 8.° da Convenção Europeia para a Protecção dos Direitos do Homem e das Liberdades Fundamentais (STE n.° 5), Conselho da Europa de 4.11.1950.

87 Ver *Marper/ the United Kingdom*, acórdão do Tribunal Europeu dos Direitos do Homem, Estrasburgo de 4.12.2008.

88 Os princípios de base das avaliações de impacto são estabelecidos nas directrizes da Comissão Europeia sobre as avaliações de impacto (SEC(2009)92 de 15.1.2009).

89 Entre alguns exemplos práticos da gestão eficaz dos riscos inclui-se impedir uma pessoa expulsa após ter praticado um crime grave num Estado-Membro de voltar a entrar no espaço Schengen através de outro Estado-Membro (SIS), ou impedir uma pessoa de requerer o asilo em vários Estados-Membros (EURODAC).

necessidade e respeitar o princípio da limitação das finalidades. A elaboração de perfis de risco — não confundir com perfis raciais ou outros perfis discriminatórios, que são incompatíveis com os direitos fundamentais — apresenta um interesse evidente. Com efeito, tais perfis podem contribuir para centrar os recursos em determinados indivíduos para fins de identificação de ameaças para a segurança e a protecção das vítimas da criminalidade.

Princípios orientados para o processo[90]

Custo-eficácia

Os serviços públicos baseados nas tecnologias da informação deviam fornecer aos contribuintes um melhor serviço e uma melhor relação custo-eficácia. Tendo em conta a situação económica actual, todas as novas propostas e, em especial, as que dizem respeito à criação ou modernização dos sistemas de informação, deverão apresentar a melhor relação custo-eficácia possível. Esta abordagem irá basear-se nas soluções pré-existentes, a fim de reduzir as sobreposições ao mínimo e maximizar as eventuais sinergias. A Comissão avaliará igualmente se uma melhor utilização dos instrumentos existentes permitiria alcançar os objectivos das propostas. A Comissão também examinará, antes de propor a criação de novos sistemas, a hipótese de dotar os sistemas de informação existentes de funções auxiliares suplementares.

Elaborar políticas partindo da base

É essencial que os contributos de todas as partes interessadas, nomeadamente os das autoridades nacionais responsáveis pela implementação, actores económicos e da sociedade civil, sejam tidos em conta o mais cedo possível no âmbito de novas iniciativas. A elaboração de políticas que tenham em conta os interesses dos utilizadores finais requer uma reflexão horizontal e uma ampla consulta[91]. Esta é a razão pela qual a Comissão procurará estabelecer relações permanentes com os funcionários nacionais e os profissionais através das estruturas do Conselho, dos comités de gestão e de formações *ad hoc*.

Repartição clara das responsabilidades

Tendo em conta a complexidade técnica dos projectos de recolha e de intercâmbio de informações no domínio da liberdade, da segurança e da justiça, deve ser conferida especial atenção à concepção inicial das estruturas de governação. A experiência do projecto SIS II demonstrou que se não forem definidos desde o início os objectivos, as atribuições e as responsabilidades de forma clara e estável, podem surgir derrapagens orçamentais consideráveis e importantes atrasos na implementação. Segundo uma primeira avaliação da aplicação da Decisão Prüm, uma estrutura de governação descentralizada também não seria a solução, uma vez que os Estados-Membros não têm qualquer líder a quem se dirigir para obter aconselhamento sobre os aspectos financeiros ou técnicos da implementação. Talvez a futura agência TI possa fornecer este tipo de aconselhamento técnico aos responsáveis dos sistemas de informação no domínio da liberdade, da segurança e da justiça. Poderia igualmente proporcionar uma plataforma com vista a uma ampla participação das partes interessadas na gestão operacional e no desenvolvimento dos sistemas informáticos. A fim de

---

90 Estes princípios inspiram-se nas conclusões do Conselho sobre uma Estratégia de gestão da informação para a segurança interna da UE, Conselho «Justiça e Assuntos Internos» de 30.11.2009.

91 Os princípios gerais das normas mínimas de consulta pública são definidos no documento COM(2002)704 de 11.12.2002.

evitar o mais possível derrapagens orçamentais e atrasos devidos à alteração das exigências, qualquer novo sistema de informação no domínio da liberdade, da segurança da justiça, em especial quando se trate de um sistema informático de grande escala, só será desenvolvido uma vez definitivamente adoptados os instrumentos jurídicos de base relativos à definição do seu objecto, alcance, funções e características técnicas.

Cláusulas de reexame e de caducidade

A Comissão avaliará cada instrumento descrito na presente comunicação. Essa avaliação diz respeito ao conjunto dos instrumentos que existem no domínio da gestão da informação, e deverá permitir ter uma ideia correcta da forma como os diferentes instrumentos se inserem no quadro mais amplo da segurança interna e da gestão dos fluxos migratórios. As propostas que serão apresentadas no futuro irão prever, se for caso disso, relatórios anuais obrigatórios, reexames periódicos e *ad hoc*, bem como a uma cláusula de caducidade. Os instrumentos existentes só serão mantidos se continuarem a servir o objectivo legítimo para o qual foram concebidos. O Anexo II fixa a data e um mecanismo de reexame para cada instrumento objecto da presente comunicação.

5. PERSPECTIVAS FUTURAS

A presente comunicação fornece, pela primeira vez, uma apresentação geral clara e completa das medidas em vigor, em implementação ou em estudo que regulam, a nível da UE, a recolha, a conservação ou o intercâmbio transfronteiras de dados pessoais para fins repressivos ou de gestão dos fluxos migratórios.

Faz uma apresentação geral aos cidadãos sobre os tipos de informações que são recolhidas, conservadas ou trocadas a seu respeito, qual a sua finalidade e por quem tais operações são efectuadas. Trata-se de um instrumento de referência, transparente para todas as partes interessadas, que desejem reflectir sobre o rumo futuro a seguir pela política da UE neste domínio. Paralelamente, fornece uma primeira resposta ao pedido do Conselho Europeu no sentido de serem elaborados instrumentos de gestão da informação a nível da UE em conformidade com a Estratégia relativa à gestão da informação da UE[92] e de reflectir sobre a necessidade de adoptar um modelo europeu de intercâmbio de informações[93].

A Comissão tenciona dar seguimento à presente comunicação através da apresentação de uma comunicação sobre o modelo europeu de intercâmbio de informações em 2012[94]. Para este efeito, a Comissão lançou um exercício de cartografia dos dados em Janeiro de 2010 tendo por fundamento as bases jurídicas e o funcionamento prático dos intercâmbios de dados e informações criminais entre Estados-Membros, cujos resultados tenciona apresentar ao Conselho e ao Parlamento Europeu em 2011[95].

---

92 Conclusões do Conselho sobre uma Estratégia de gestão da informação para a segurança interna da UE, Conselho «Justiça e Assuntos Internos» de 30.11.2009 (Estratégia de gestão da informação da UE).

93 Programa de Estocolomo — Uma Europa aberta e segura que sirva e proteja os cidadãos, Documento do Conselho 5731/10 de 3.3.2010, Secção 4.2.2.

94 Como indica o Plano de Acção da Comissão de aplicação do Programa de Estocolmo [COM(2010)171 de 20.4.2010].

95 Este exercício é realizado em estreita colaboração com uma equipa *ad hoc* composta por representantes dos Estados-Membros da UE e da EFTA, da Europol, da Eurojust, da Frontex e da Autoridade Europeia para a Protecção de Dados.

Por último, a presente comunicação expõe, pela primeira vez, a óptica da Comissão relativamente aos princípios gerais que tenciona seguir no futuro no quadro da elaboração de instrumentos de recolha, conservação ou intercâmbio dados. Tais princípios serão igualmente aplicados para avaliar os instrumentos existentes. A adopção de uma abordagem sobre a elaboração e a avaliação das políticas fundada num conjunto de princípios igualmente definidos de forma clara, deverá reforçar a coerência e eficácia dos instrumentos actuais e futuros de forma a garantir o pleno respeito dos direitos fundamentais dos cidadãos.

ANEXO I

Os dados e exemplos seguintes visam ilustrar a aplicação prática das medidas de gestão da informação que são actualmente utilizadas.

Sistema de Informação de Schengen (SIS)

Número total de indicações no SIS registadas na base de dados central do SIS (C.SIS)[96]

Categorias de indicações	**2007**	**2008**	**2009**
Notas de banco	177 327	168 982	134 255
Documentos em branco	390 306	360 349	341 675
Armas de fogo	314 897	332 028	348 353
Documentos emitidos	17 876 227	22 216 158	25 685 572
Veículos	3 012 856	3 618 199	3 889 098
Pessoas procuradas (pseudónimo)	299 473	296 815	290 452
Pessoas procuradas (nome)	859 300	927 318	929 546
Entre os quais:			
Pessoas procuradas para detenção para efeitos de extradição	19 119	24 560	28 666
Nacionais de países terceiros que figuram na lista de proibição de entrada	696 419	746 994	736 868
Adultos desaparecidos	24 594	23 931	26 707
Menores desaparecidos	22 907	24 628	25 612
Testemunhas ou pessoas objecto de uma citação judicial	64 684	72 958	78 869
Pessoas objecto de vigilância excepcional visando prevenir as ameaças contra a segurança pública	31 568	34 149	32 571
Pessoas objecto de vigilância excepcional visando prevenir as ameaças contra a segurança nacional	9	98	253
Total	**22 933 370**	**27 919 849**	**31 618 951**

[96] Documento 6162/10 do Conselho de 5.2.2010; Documento do Conselho 5764/09 de 28.1.2009; Documento do Conselho 5441/08 de 30.1.2008.

EURODAC - Movimentos de requerentes de asilo que apresentaram novos pedidos no mesmo ou noutro Estado-Membro (2008)

Envios pelos Estados-Membros de impressões digitais para fins de comparação e de obtenção de «acertos» nos Estados-Membros (colunas) onde uma pessoa apresentou anteriormente um pedido de asilo	Estado-Membro onde foi apresentado o primeiro pedido de asilo[97]																													Total de 2.os pedidos	
	AT	BE	BG	CH	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IS	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK	UK	Acertos nacionais	Total de acertos
AT	1 725	74	2	0	1	87	274	5	2	31	12	25	115	212	5	0	134	3	14	0	9	52	49	1 371	1	42	111	17	260	61	**1 725**	**4 694**
BE	180	5 450	4	0	3	38	408	17	0	41	17	28	378	67	28	0	69	3	37	0	2	180	73	625	6	3	192	17	58	205	**5 450**	**8 129**
BG	5	2	116	0	1	1	5	1	0	7	0	0	0	1	0	0	1	0	2	0	0	1	3	0	0	6	8	0	0	4	**116**	**164**
CH	32	52	1	4	3	5	35	0	0	17	17	8	39	19	1	0	355	0	1	0	13	15	37	3	1	0	41	4	4	25	**4**	**732**
CY	1	0	0	0	68	0	1	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	**68**	**73**
CZ	55	12	0	0	0	637	48	4	0	0	3	4	13	0	1	0	8	2	1	0	0	7	6	17	1	0	13	0	1	6	**637**	**839**
DE	260	268	12	0	4	79	1 852	42	0	174	39	56	256	106	9	2	200	5	26	2	5	174	137	149	4	43	567	30	89	128	**1 852**	**4 718**
DK	44	43	3	0	0	13	126	119	0	27	13	44	36	13	4	0	47	0	7	0	0	30	225	55	2	4	436	2	7	41	**119**	**1 341**
EE	0	0	0	0	0	0	1	1	0	0	0	8	0	0	0	0	0	0	0	0	0	0	1	0	0	0	3	0	0	9	**0**	**23**
EL	66	88	27	0	12	9	131	10	0	766	8	8	35	3	9	0	48	0	1	0	0	33	24	3	0	13	141	0	8	316	**766**	**1 759**
ES	16	18	2	0	1	3	37	1	0	11	108	0	29	4	5	0	35	0	0	0	0	9	9	4	6	0	21	5	1	16	**108**	**341**
FI	37	44	1	0	1	10	115	25	0	48	5	229	14	30	10	1	194	0	3	0	90	49	107	44	2	4	362	3	3	81	**229**	**1512**
FR	365	339	0	0	8	97	502	29	0	92	78	31	860	161	8	0	336	11	26	1	29	106	74	1 739	8	9	286	37	75	190	**860**	**5 497**
HU	297	53	4	0	1	3	169	4	0	2	3	19	70	791	1	0	27	1	10	0	0	28	32	0	0	76	79	19	14	14	**791**	**1 717**
IE	20	21	0	0	4	2	24	1	0	9	8	0	23	4	309	0	35	0	4	0	4	16	7	0	0	0	22	2	2	187	**309**	**704**
IS	4	3	0	0	0	0	3	0	0	3	1	1	6	2	1	0	3	0	1	0	1	3	10	1	0	0	11	1	0	3	**0**	**58**
IT	390	111	5	0	6	33	349	11	0	270	47	27	192	60	23	5	3 290	0	11	0	58	78	116	9	2	6	201	59	224	680	**3 290**	**6 263**
LT	3	1	0	0	1	3	0	0	0	0	1	0	1	0	0	0	0	5	0	0	0	0	4	14	0	0	5	0	2	0	**5**	**40**
LU	7	21	4	0	0	0	12	2	0	0	0	1	9	6	0	1	8	0	2	0	1	6	4	0	0	0	10	3	1	3	**2**	**101**
LV	3	1	0	0	0	0	1	0	1	0	0	0	1	0	0	0	0	5	0	0	0	0	0	0	0	0	1	0	2	0	**0**	**15**
MT	1	0	0	0	0	0	0	0	0	0	0	5	1	0	0	0	6	0	0	0	16	0	1	0	0	0	1	1	0	0	**16**	**32**
NL	109	223	16	0	1	27	198	21	0	113	16	29	109	33	7	1	226	0	14	0	58	1 240	95	16	8	9	289	8	22	129	**1 240**	**3 017**
NO	84	103	6	0	2	13	256	76	0	199	55	57	78	23	8	0	524	8	13	1	83	86	276	164	1	9	826	10	21	96	**276**	**3 078**
PL	188	65	0	0	0	30	68	15	0	0	2	4	75	1	1	0	0	3	3	0	0	7	27	1 208	1	1	43	1	13	4	**1 208**	**1 760**
PT	1	10	0	0	0	0	4	1	0	0	11	0	9	0	0	0	2	0	2	0	0	2	2	0	3	0	2	0	1	2	**3**	**52**
RO	43	2	5	0	1	9	33	0	0	3	0	5	14	11	0	0	0	0	1	0	0	9	1	1	0	64	17	0	4	4	**64**	**227**
SE	243	133	30	0	4	36	516	173	0	143	29	143	145	80	16	3	276	0	16	0	130	98	430	147	5	13	1 914	11	26	122	**1 914**	**4 882**
SI	14	4	0	0	0	1	10	1	0	1	1	2	15	6	0	0	5	0	1	0	0	2	3	0	0	0	5	45	3	2	**45**	**121**
SK	105	4	0	0	0	7	33	0	1	0	0	1	2	12	0	0	3	0	0	1	0	4	4	4	0	0	9	2	195	6	**195**	**393**
UK	109	153	7	0	3	12	276	30	0	108	6	38	209	25	217	2	768	0	8	0	43	128	76	7	4	11	174	6	46	3 141	**3 141**	**5 607**
Total de 1.os pedidos	**4 407**	**7 298**	**245**	**4**	**125**	**1 155**	**5 487**	**589**	**4**	**2 067**	**480**	**773**	**2 734**	**1 670**	**663**	**15**	**6 600**	**46**	**204**	**5**	**542**	**2 363**	**1 833**	**5 581**	**55**	**313**	**5 791**	**283**	**1 082**	**5 475**	**24 433**	**57 889**

[97] COM(2009) 494 de 25.9.2009. A expressão «acertos nacionais» refer-se à apresentação de um novo pedido de asilo no Estado-Membro onde já foi apresentado o pedido anterior.

Sistema de informações antecipadas sobre os passageiros (API)

Utilização pelo Reino Unido do Sistema de informações avançadas sobre os passageiros para melhorar os controlos nas fronteiras e lutar contra a imigração irregular[98]	
Número de acções desenvolvidas em 2009	
Antecedentes desfavoráveis (entrada recusada à pessoa)	379
Passaportes perdidos roubados ou anulados (documento confiscado)	56

[98] A Border Agency do Reino Unido (agência britânica para a gestão das fronteiras) forneceu estas informações à Comissão para efeitos da presente comunicação.

Sistema de Informação Aduaneira (SIA)

Número total de dossiês registados na base de dados SIA (2009)[99]	
Acção	**SIA (com base na convenção SIA)**
Dossiês criados	2 007
Dossiês activos	274
Dossiês consultados	11 920
Dossiês suprimidos	1 355

[99] Estas informações foram fornecidas pela Comissão.

Iniciativa sueca

Exemplos de utilização da Iniciativa sueca para investigar crimes[100]	
Homicídio	Em 2009 teve lugar uma tentativa de homicídio na capital de um Estado-Membro. A polícia recolheu uma amostra biológica de um copo que tinha sido utilizado pelo suspeito. Os agentes da polícia científica extraíram ADN dessa amostra e estabeleceram um perfil de ADN. Uma comparação deste perfil com outros perfis de referência conservados na base de dados ADN nacional não produziu qualquer resultado positivo. As forças policiais encarregadas do inquérito decidiram então enviar por intermédio do seu ponto de contacto Prüm um pedido de comparação com os perfis ADN de referência conservados por outros Estados-Membros que tinham sido autorizados a trocar tais dados com base na Decisão Prüm ou no Acordo Prüm. Esta comparação transfronteiras permitiu obter um acerto. Com base na Iniciativa sueca as forças policiais solicitaram informações adicionais sobre o suspeito. O seu ponto de contacto nacional recebeu uma resposta de outros Estados-Membros no prazo de 36 horas o que permitiu à polícia identificar o suspeito.
Violação	Em 2003 um suspeito não identificado violou uma mulher. A polícia recolheu amostras da vítima mas o perfil de ADN obtido inicialmente a partir dessas mostras não correspondia a qualquer perfil de referência conservado na base de dados ADN nacional. Um pedido de comparação de ADN enviado pelo ponto de contacto Prüm aos outros Estados-Membros que tinham sido autorizados a trocar os perfis de ADN de referência com base na Decisão Prüm ou no Acordo Prüm permitiu obter um acerto. As forças policiais solicitaram então informações adicionais sobre o suspeito no quadro da Iniciativa sueca. O seu ponto de contacto nacional recebeu uma resposta no prazo de 8 horas o que permitiu à polícia identificar o suspeito.

[100] As autoridades policiais de um Estado-Membro forneceram estes exemplos à Comissão para efeitos da presente comunicação.

Obtenção pela Alemanha de «acertos» no quadro da comparação transfronteiras de perfis de ADN em função do tipo de crime (2009)[101]

Acertos por tipo de crime	**Áustria**	**Espanha**	**Luxemburgo**	**Países Baixos**	**Eslovénia**
Crimes contra interesses públicos	32	4	0	5	2
Crimes contra a liberdade das pessoas	9	3	5	2	0
Crimes sexuais	40	22	0	31	4
Crimes contra as pessoas	49	24	0	15	2
Outros crimes	3 005	712	18	1 105	71

[101] Resposta do Governo alemão a uma pergunta parlamentar de Ulla Jelpke, Inge Höger e Jan Korte (referência n.° 16/14120), Bundestag, 16.ª sessão, referência n.° 16/14150 de 22.10.2009. Estes números referem-se ao período que tem início na data em que um Estado-Membro começou a trocar dados como a Alemanha e que termina em 30 de Setembro de 2009.

Exemplos de Estados-Membros que detectaram casos de crimes graves a partir de dados conservados[102]	
Assassinato	Os serviços policiais de um Estado-Membro conseguiram encontrar um grupo de assassinos responsáveis pela morte de seis pessoas por motivos raciais. Os autores tentaram fugir da polícia através da troca de cartões SIM mas as listas das ligações efectuadas e os identificadores dos seus telefones portáteis traíram-nos.
Homicídio	Uma autoridade policial conseguiu provar o envolvimento de dois suspeitos num caso de homicídio analisando os dados de tráfego do telefone portátil da vítima. Tal análise permitiu aos investigadores reconstituir o itinerário percorrido em conjunto pela vítima e os dois suspeitos.
Roubo	As autoridades encontraram o paradeiro de um assaltante responsável por 17 roubos analisando os dados de tráfego do seu cartão anónimo pré-pago SIM. Ao identificar a sua namorada conseguiram igualmente localizar o autor dos roubos.
Fraude	Os investigadores resolveram um caso de fraude em que um grupo de indivíduos que propunha a venda na Internet de automóveis de luxo em troca de dinheiro em espécie roubava sistematicamente os compradores que vinham tomar posse dos seus veículos. Um endereço IP permitiu à polícia encontrar o seu assinante e prender os infractores.

[102] Estes exemplos anónimos baseiam-se nas respostas dos Estados-Membros a um questionário de 2009 da Comissão relativo à transposição da Directiva 2006/24/CE (Directiva relativa à conservação de dados).

Cooperação entre as unidades de informação financeira (UIF)

Número total de pedidos de informações apresentados pelas UIF nacionais através da FIU.net[103]		
Ano	**Pedidos de informações**	**Utilizadores activos**
2007	3 133	12 Estados-Membros
2008	3 084	13 Estados-Membros
2009	3 520	18 Estados-Membros

[103] O serviço FIU.net forneceu estas informações à Comissão para efeitos da presente comunicação.

Cooperação entre os gabinetes de recuperação de bens (ARO)

Pedidos de detecção de bens apresentados pelos Estados-Membros e tratados pela Europol[104]

Ano	**2004**	**2005**	**2006**	**2007**
Pedidos de informações	5	57	53	133
Entre os quais:				
Casos de fraude				29
Casos de branqueamento de capitais				26
Casos de droga				25
Casos relacionados com outros crimes				18
Casos de droga e de branqueamento de capitais				19
Casos de fraude e de branqueamento de capitais				7
Casos relacionados com vários crimes				9

Casos de confisco de bens tratados pela Eurojust (2006-2007)[105]

Tipos de casos		**Dossiês iniciados por**	
Casos de criminalidade ambiental	1	Alemanha	27 %
Casos de participação numa organização criminosa	5	Países Baixos	21 %
Casos de tráfico de droga	15	Reino Unido	15 %
Casos de fraude fiscal	8	Finlândia	13 %
Casos de fraude	8	França	8 %
Casos de fraude ao IVA	1	Espanha	6 %
Casos de branqueamento de capitais	9	Portugal	4 %
Casos de corrupção	1	Suécia	2 %
Casos de crimes contra a propriedade	2	Dinamarca	2 %
Casos de tráfico de armas	1	Letónia	2 %
Casos de contrafacção e de piratagem de produtos	2		
Casos de fraude sobre pagamentos antecipados	2		
Casos de falsificação de documentos administrativos	1		
Casos de crimes associados a veículos	1		
Casos de terrorismo	1		
Casos de falsificação	2		
Casos de tráfico de seres humanos	1		

104 «Assessing the effectiveness of EU Member States' practices in the identification, tracing, freezing and confiscation of criminal assets – Final Report» (para a Comissão Europeia, DG JLS), Matrix Insight, Junho de 2009.

105 Ibidem.

Plataformas de alerta da cibercriminalidade

Exemplos da plataforma francesa de alerta da cibercriminalidade Pharos que investiga casos de cibercriminalidade[106]	
Pornografia infantil	Um internauta informou a Pharos da existência de um blogue com fotografias e imagens de tipo desenho animado de abuso sexual de crianças. O autor do blogue que aparecia numa foto tentava igualmente seduzir crianças através do seu blogue. Os investigadores identificaram um professor de matemática como principal suspeito. A busca realizada no seu domicílio permitiu encontrar 49 vídeos com imagens de pornografia infantil. O inquérito revelou igualmente que se preparava para organizar cursos particulares no seu domicílio. O arguido foi posteriormente condenado e punido com uma pena de prisão suspensa.
Abuso sexual de crianças	A polícia francesa teve conhecimento do facto de um indivíduo oferecer dinheiro na Internet em troca de relações sexuais com crianças. Um detective da Pharos fazendo-se passar por um menor estabeleceu contacto com o suspeito que lhe ofereceu dinheiro em troca de relações sexuais. A conversa entretanto mantida na Internet permitiu à Pharos identificar o endereço do protocolo Internet do suspeito e descobrir o seu paradeiro numa cidade conhecida por registar um número elevado de casos de exploração sexual de crianças. O arguido foi posteriormente condenado e punido com uma pena de prisão suspensa.

[106] Pharos é a abreviação de «*plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements*».

Exemplos da contribuição da Europol para a luta contra formas graves de criminalidade transfronteiras[107]	
Operação Andromeda	Em Dezembro de 2009 a Europol participou numa vasta operação policial transfronteiriça contra uma rede de tráfico de droga com contactos em 42 países. Esta rede baseada na Bélgica e na Noruega organizava o tráfico de droga a partir do Peru através dos Países Baixos com destino à Bélgica Reino Unido Itália e outros Estados-Membros. A cooperação policial foi coordenada pela Europol e a cooperação judiciária pela Eurojust. As autoridades participantes instalaram um gabinete móvel em Pisa e a Europol um centro operacional na cidade da Haia. A Europol procedeu a uma comparação cruzada das informações sobre os suspeitos e elaborou um relatório com a descrição da rede criminosa.
Participantes	Itália Países Baixos Alemanha Bélgica Reino Unido Lituânia Noruega e Eurojust.
Resultados	As forças policiais participantes apreenderam 49 kg de cocaína, 10 kg de heroína, 6000 comprimidos de ecstasy, duas armas de fogo, cinco documentos de identidade falsos e 43 000 EUR em numerário e detiveram 15 pessoas.
Operação Typhon	Entre Abril de 2008 e Fevereiro de 2010 a Europol forneceu apoio analítico às forças policiais dos 20 países envolvidos na Operação Typhon. Por ocasião desta vasta operação contra uma rede de pedofilia que distribuía imagens de pornografia infantil através de um sítio Web austríaco a Europol prestou apoio técnico e análise de informações criminais com base nas imagens comunicadas pela Áustria. Avaliou seguidamente a fiabilidade dos dados e procedeu à sua reestruturação antes de preparar as suas próprias informações. Ao proceder a uma comparação cruzada dos dados com as informações constantes do seu ficheiro de análise produziu 30 relatórios de informações com base nos quais foram iniciadas investigações em vários países.
Participantes	Áustria Bélgica Bulgária Canadá Dinamarca França Alemanha Hungria Itália Lituânia Luxemburgo Malta Países Baixos Polónia Roménia Eslováquia Eslovénia Espanha Suíça e Reino Unido.
Resultados	As forças participantes identificaram 286 suspeitos tendo procedido à detenção de 118 de entre eles e salvaram no âmbito deste caso cinco vítimas de abuso em quatro países.

[107] A Europol forneceu estas informações à Comissão para efeitos da presente comunicação. Informações adicionais sobre a operação Andromeda estão disponíveis no endereço http://www.eurojust.europa.eu/.

Exemplos de coordenação pela Eurojust de vastas operações judiciárias transfronteiras de luta contra formas graves de criminalidade[108]

Tráfico de seres humanos e financiamento do terrorismo	Em Maio de 2010 a Eurojust coordenou uma operação transfronteiras de que resultou a detenção de cinco membros de uma rede de criminalidade organizada activa no Afeganistão Paquistão Roménia Albânia e Itália. O grupo fornecia documentos falsos a nacionais afegãos e paquistaneses e organizava o seu tráfico para Itália através do Irão Turquia e Grécia. Quando chegavam a Itália os migrantes eram enviados para a Alemanha Suécia Bélgica Reino Unido e Noruega. As receitas do tráfico destinavam-se a financiar o terrorismo.
Fraude de cartões bancários	Ao coordenar a cooperação policial e judiciária transfronteiras a Europol e a Eurojust ajudaram a desmantelar uma rede de fraude de cartões bancários activa na Irlanda em Itália nos Países Baixos na Bélgica e na Roménia. Esta rede roubou os dados de identificação de cerca de 15 000 cartões de pagamento causando um prejuízo de 6 5 milhões de EUR. Em antecipação a esta operação de que resultaram 24 detenções em Julho de 2009 magistrados belgas irlandeses italianos neerlandeses e romenos facilitaram a emissão de mandados de detenção europeus e a autorização de escutas aos suspeitos.
Tráfico de seres humanos e tráfico de droga	Na sequência de uma reunião de coordenação organizada pela Eurojust em Março de 2009 as autoridades italianas neerlandesas e colombianas procederam à detenção de 62 indivíduos suspeitos de tráfico de seres humanos e de tráfico de droga. Esta rede era especializada no tráfico de mulheres vulneráveis originárias da Nigéria com destino aos Países Baixos obrigando-as a prostituírem-se em Itália França e Espanha. Os lucros da prostituição financiavam as compras de cocaína da rede na Colômbia sendo a droga seguidamente encaminhada para a UE para fins de consumo.

[108] Estes exemplos têm origem no endereço: http://www.eurojust.europa.eu/

Exemplos de análise PNR que permitem recolher informações no quadro de investigações de formas graves de criminalidade transfronteiras[109]	
Tráfico de crianças	A análise PNR revelou que três menores não acompanhados viajavam de um Estado-Membro da UE para um país terceiro sem indicação de quem os deveria esperar à chegada. Alertadas pela polícia do Estado-Membro após a partida as autoridades do país terceiro detiveram a pessoa que se encontrava à espera das crianças que se revelou ser um delinquente sexual registado no Estado-Membro.
Tráfico de seres humanos	A análise PNR permitiu desmascarar um grupo de traficantes de seres humanos que viajavam sempre segundo o mesmo itinerário. Utilizavam documentos falsos para procederem às formalidades de registo num voo interno da UE e utilizavam documentos autênticos para proceder simultaneamente às formalidades de registo noutro voo com destino a um país terceiro. Quando se encontravam na sala de espera do aeroporto embarcavam no voo interno da UE.
Fraude de cartões bancários	Várias famílias viajaram para um Estado-Membro com bilhetes comprados graças a cartões de crédito roubados. A investigação revelou que um grupo criminoso utilizava esses cartões para adquirir os bilhetes que revendiam seguidamente através de centros de atendimento telefónico à distância. Foram os dados PNR que permitiram estabelecer a ligação entre os viajantes por um lado e os cartões de crédito e os vendedores por outro.
Tráfico de droga	A autoridade policial de um Estado-Membro dispunha de informações que indiciavam o envolvimento de um homem no tráfico de droga a partir de um país terceiro mas os guardas de fronteira nunca encontraram qualquer substância suspeita à sua chegada à UE. A análise PNR revelou que esta pessoa viajava sempre em companhia de um associado. A inspecção deste associado permitiu apreender grandes quantidades de droga.

[109] Estes exemplos foram tornados anónimos para proteger as fontes das informações.

Programa de Detecção do Financiamento do Terrorismo (TFTP)

Exemplos de informações recolhidas no quadro do TFTP para fins de investigação de planos terroristas[110]	
Plano terrorista de Barcelona de 2008	Em Janeiro de 2008 foram detidos em Barcelona dez suspeitos no âmbito de uma tentativa falhada de atentado nos transportes públicos da cidade. Os dados TFTP foram utilizados para identificar as ligações dos suspeitos com a Ásia a África e a América do Norte.
Tentativa de atentado com explosivos líquidos num voo transatlântico em 2006	Foram utilizadas informações TFTP para investigar e proceder à acusação de indivíduos associados a uma tentativa falhada de atentado que visava em Agosto de 2006 fazer explodir dez aviões transatlânticos com destino aos EUA e ao Canadá a partir do Reino Unido.
Atentados à bomba de Londres de 2005	Foram utilizados dados TFTP para fornecer novas pistas aos investigadores confirmar a identidade dos suspeitos e revelar as relações entre os indivíduos responsáveis por esses atentados.
Atentados à bomba de Madrid de 2004	Foram fornecidos dados TFTP a vários Estados-Membros da UE para os ajudar nas investigações iniciadas na sequência destes atentados.

110 Segundo relatório do juiz Jean-Louis Bruguière sobre o tratamento de dados pessoais provenientes da UE pelo Departamento do Tesouro dos Estados Unidos para fins de luta contra o terrorismo, Janeiro de 2010.

ANEXO II

Quadro de apresentação geral dos instrumentos em vigor em implementação ou em estudo

Instrumento	Antecedentes	Finalidade(s)	Estrutura	Dados pessoais abrangidos	Acesso aos dados	Protecção dos dados	Conservação dos dados	Estado de implementação	Reexame
Sistema de Informação de Schengen (SIS)	Iniciativa dos Estados-Membros	Manter a segurança pública incluindo a segurança nacional no espaço Schengen e facilitar a circulação das pessoas através da utilização de informações comunicadas através deste sistema.	Centralizada: N.SIS (partes nacionais) ligados através de interface ao C.SIS (parte central).	Nomes e pseudónimos características físicas local e data de nascimento nacionalidade e indicações de pessoas armadas ou violentas. As indicações no SIS referem-se a vários grupos de pessoas diferentes.	A polícia a polícia de fronteiras alfândegas autoridades judiciais têm acesso a todos os dados; autoridades de imigração e consulares têm acesso à lista de proibição de entrada e à lista dos documentos perdidos ou roubados. A Europol e a Eurojust podem aceder a determinados dados.	Convenção 108 do Conselho da Europa (CdE) e Recomendação das Polícias R (87) 15 do CdE.	Os dados pessoais inseridos no SIS para efeitos de procura de pessoas só podem ser conservados durante o período necessário para cumprir os fins para os quais tiverem sido fornecidos e nunca mais de três anos após a data de inserção. Os dados sobre as pessoas sujeitas a controlos excepcionais devido à ameaça que representam para a segurança pública ou nacional devem ser apagados após um ano.	O SIS é plenamente aplicável em 22 Estados-Membros e também na Suíça na Noruega e na Islândia. O Reino Unido e a Irlanda participam no SIS à excepção das indicações sobre nacionais de países terceiros que constem da lista de proibição de entrada. Prevê-se que a Bulgária a Roménia e o Liechtenstein apliquem esta medida proximamente.	Os signatários podem propor alterações à Convenção de Schengen. O texto alterado terá de ser adoptado por unanimidade e ratificado pelos parlamentos.

Quadro de apresentação geral dos instrumentos em vigor em implementação ou em estudo

Instrumento	Antecedentes	Finalidade(s)	Estrutura	Dados pessoais abrangidos	Acesso aos dados	Protecção dos dados	Conservação dos dados	Estado de implementação	Reexame
Sistema de Informação de Schengen de segunda geração (SIS II)	Iniciativa da Comissão.	Assegurar um elevado nível de segurança no espaço de liberdade de segurança e de justiça e facilitar a circulação de pessoas através da comunicação de informações por intermédio deste sistema.	Centralizada: N.SIS II (partes nacionais) ligados através de interface ao CS-SIS (parte central). O SIS II utilizará a rede segura de comunicação de dados s-TESTA.	As categorias de dados do SIS bem como impressões digitais fotografias cópias de mandados de detenção europeus indicações sobre a usurpação de identidades e ligações entre diversas indicações. As indicações no SIS II referem-se a vários grupos de pessoas diferentes.	A polícia a polícia de fronteiras alfândegas autoridades judiciais terão acesso a todos os dados; autoridades de imigração e consulares têm acesso à lista de proibição de entrada e à lista dos documentos perdidos ou roubados. A Europol e a Eurojust poderão aceder a determinados dados.	Disposições específicas previstas nos instrumentos legislativos de base que regulam o SIS II e a Directiva 95/46/CE Regulamento (CE) n.º 45/2001 Decisão-Quadro 2008/977/JAI Convenção 108 do CdE e Recomendação das Polícias R (87) 15 do CdE.	Os dados pessoais inseridos no SIS para efeitos de procura de pessoas só podem ser conservados durante o período necessário para cumprir os fins para os quais tiverem sido fornecidos e nunca mais de três anos após a data de inserção. Os dados sobre as pessoas sujeitas a controlos excepcionais devido à ameaça que representam para a segurança pública ou nacional devem ser apagados após um ano.	O SIS II está a ser implementado. Quando estiver pronto a funcionar será aplicável na UE-27 Suíça Liechtenstein Noruega e Islândia. O Reino Unido e a Irlanda participarão no SIS II à excepção das indicações sobre nacionais de países terceiros que constem da lista de proibição de entrada.	A Comissão deve transmitir relatórios intercalares todos os dois anos ao Parlamento Europeu (PE) e ao Conselho sobre o desenvolvimento do SIS II e possível migração do SIS.

Quadro de apresentação geral dos instrumentos em vigor em implementação ou em estudo

Instrumento	Antecedentes	Finalidade(s)	Estrutura	Dados pessoais abrangidos	Acesso aos dados	Protecção dos dados	Conservação dos dados	Estado de implementação	Reexame
EURODAC	Iniciativa da Comissão.	Ajudar a determinar qual o Estado-Membro responsável pela análise de um pedido de asilo.	Centralizada composto por pontos nacionais de acesso ligados por uma interface à unidade central do EURODAC. O EURODAC utiliza a rede s-TESTA.	Dados das impressões digitais sexo local e data do pedido de asilo o número de referência utilizado pelo Estado-Membro de origem e a data em que as impressões digitais foram recolhidas transmitidas e inseridas no sistema.	Os Estados-Membros devem fornecer a lista de autoridades que têm acesso aos dados que inclui geralmente autoridades responsáveis pelo asilo e imigração guardas de fronteira e polícia.	Directiva 95/46/CE.	10 anos para as impressões digitais dos requerentes de asilo; 2 anos para as impressões digitais de nacionais de países terceiros detidos no âmbito da passagem irregular de uma fronteira externa.	O EURODAC é plenamente aplicável em cada Estado-Membro e na Noruega na Islândia e na Suíça. Está em vias de conclusão um acordo que permite a ligação do Liechtenstein.	A Comissão deve apresentar ao Parlamento Europeu e ao Conselho um relatório anual sobre o funcionamento da unidade central do EURODAC.
Sistema de Informação sobre Vistos (VIS)	Iniciativa da Comissão.	Ajudar a aplicar uma política comum em matéria de asilo e contribuir para a prevenção de ameaças à segurança interna.	Centralizada composto por partes nacionais ligadas por uma interface à parte central. O VIS utilizará a rede s-TESTA.	Pedidos de visto impressões digitais fotografias decisões relacionadas com vistos e ligações entre pedidos.	As autoridades em matéria de vistos asilo imigração e controlo no fronteiriço terão acesso a todos os dados. A polícia e a Europol podem consultar o VIS para efeitos de prevenção detecção e investigação de crimes graves.	Disposições específicas previstas nos instrumentos legislativos de base que regulam o VIS e a Directiva 95/46/CE Regulamento (CE) n.º 45/2001 Decisão-Quadro 2008/977/JAI Convenção 108 do CdE e Recomendação das Polícias R (87) 15 do CdE.	5 anos.	O VIS está a ser implementado e será aplicável em cada Estado-Membro (com excepção do Reino Unido e da Irlanda) bem como na Noruega Islândia e Suíça.	A Comissão deve apresentar um relatório ao Parlamento Europeu e ao Conselho sobre o funcionamento do VIS três anos após o seu lançamento e seguidamente de quatro em quatro anos.

Quadro de apresentação geral dos instrumentos em vigor em implementação ou em estudo

Instrumento	Antecedentes	Finalidade(s)	Estrutura	Dados pessoais abrangidos	Acesso aos dados	Protecção dos dados	Conservação dos dados	Estado de implementação	Reexame
Sistema de informações antecipadas sobre os passageiros (API)	Iniciativa lançada por Espanha.	Melhorar os controlos nas fronteiras e combater a imigração ilegal.	Descentralizada.	Dados pessoais extraídos dos passaportes ponto de embarque e ponto de entrada na UE.	Autoridades responsáveis pelo controlo nas fronteiras e a pedido as autoridades responsáveis pela aplicação da lei.	Directiva 95/46/CE.	Os dados devem ser suprimidos 24 horas após a chegada de um voo à UE.	O sistema API está em vigor em todos os Estados-Membros mas só é utilizado por alguns deles.	A Comissão avaliará o sistema API em 2011.
Convenção Nápoles II	Iniciativa dos Estados-Membros	Ajudar as administrações aduaneiras nacionais a prevenir e detectar as infracções às regulamentaçõe s aduaneiras nacionais e ajudá-las a reprimir e punir as violações das normas aduaneiras da UE e nacionais.	Descentralizada funcionando através de uma série de unidades centrais de coordenação.	Todas as informações relativas a uma pessoa identificada ou identificável.	As unidades centrais de coordenação transmitem as informações às autoridades aduaneiras nacionais organismos de investigação e judiciais e com o consentimento prévio do Estado-Membro que tiver fornecido os dados a outras entidades.	Directiva 95/46/CE e a Convenção 108 do CdE. Os dados devem no Estado-Membro que os recebe beneficiar de um nível de protecção pelo menos equivalente ao nível de protecção garantido no Estado-Membro que os forneceu.	Os dados podem ser conservados por um período que não exceda o necessário relativamente aos efeitos para os quais tiverem sido fornecidos.	A Convenção Nápoles II foi ratificada por todos os Estados-Membros.	Os signatários podem propor alterações à Convenção Nápoles II. O texto alterado terá de ser adoptado pelo Conselho e ratificado pelos Estados-Membros.

Quadro de apresentação geral dos instrumentos em vigor em implementação ou em estudo

Instrumento	Antecedentes	Finalidade(s)	Estrutura	Dados pessoais abrangidos	Acesso aos dados	Protecção dos dados	Conservação dos dados	Estado de implementação	Reexame
Sistema de Informação Aduaneira (SIA)	Iniciativa dos Estados-Membros	Ajudar as autoridades competentes a prevenir investigar e reprimir as infracções graves às regulamentaçõe s aduaneiras nacionais.	Centralizada acessível através de terminais em cada Estado-Membro e na Comissão. O SIA e o FIDE funcionam com base na AFIS que utiliza a rede de comunicação comum o sistema de interface comum ou o acesso seguro à Web facultado pela Comissão.	Nomes e pseudónimos data e lugar de nascimento nacionalidade sexo características físicas documentos de identidade morada eventuais registos de violência motivo de inserção dos dados no SIA acção proposta e número de registo do meio de transporte.	As autoridades aduaneiras nacionais a Europol e a Eurojust podem aceder aos dados do SIA.	Disposições específicas que figuram na convenção SAI e a Directiva 95/46/CE Regulamento (CE) n.º 45/2001 Convenção 108 do CdE e Recomendação das Polícias R (87) 15 do CdE.	Os dados pessoais copiados do SIA para outros sistemas para fins de gestão dos riscos ou de análise operacional só podem ser conservados durante o tempo necessário para cumprir o objectivo para o qual tiverem sido copiados e nunca por mais de 10 anos.	Em vigor em todos os Estados-Membros.	A Comissão em cooperação com os Estados-Membros apresenta anualmente ao PE e ao Conselho um relatório sobre o funcionamento do SIA.
Iniciativa sueca	Iniciativa da Suécia.	Racionalizar os intercâmbios de informações para efeitos de investigação penal e operações de informações criminais.	Descentralizada os Estados-Membros devem designar os pontos de contacto nacionais competentes para receber os pedidos urgentes de informação.	Quaisquer informações existentes ou informações criminais de que dispõem as autoridades responsáveis pela aplicação da lei.	As autoridades policiais e aduaneiras e qualquer outra autoridade com competência para investigar crimes (com excepção dos serviços de informação).	Normas nacionais em matéria de protecção de dados bem como a Convenção 108 do CdE e Recomendação das Polícias R (87) 15 do CdE.	Os dados e a informação criminal fornecidos a título deste instrumento só podem ser utilizados para os fins para que foram fornecidos e sob determinadas condições definidas pelo Estado-Membro que fornece esses dados.	12 dos 31 signatários (Estados da UE e da EFTA) adoptaram leis nacionais que aplicam este instrumento; cinco países preenchem o formulário de pedido de informações; e dois utilizam frequentemente o formulário no seu intercâmbio de informações.	A Comissão deve apresentar um relatório de avaliação ao Conselho em 2010.

Quadro de apresentação geral dos instrumentos em vigor em implementação ou em estudo

Instrumento	Antecedentes	Finalidade(s)	Estrutura	Dados pessoais abrangidos	Acesso aos dados	Protecção dos dados	Conservação dos dados	Estado de implementação	Reexame
Decisão Prüm	Iniciativa dos Estados-Membros	Reforçar a prevenção do crime em particular o terrorismo e manter a ordem pública.	Descentralizada interconexão através da rede s-TESTA. Os pontos de contacto coordenam a recepção e o envio de pedidos de comparação de dados.	Perfis de ADN e impressões digitais anónimos dados de registo de veículos e informações acerca de pessoas suspeitas de ligações ao terrorismo.	Os pontos de contacto transmitem os pedidos; o acesso nacional é regulado pelo direito interno.	Normas específicas estabelecidas pela Decisão Prüm e a Convenção 108 do CdE Protocolo Adicional 181 e Recomendação das Polícias R (87) 15 do CdE. As pessoas podem dirigir-se às respectivas autoridades nacionais de protecção de dados para exercerem os seus direitos relativamente ao tratamento dos dados pessoais.	Os dados pessoais devem ser apagados logo que deixem de ser necessários para os fins para que foram fornecidos. O período máximo de conservação dos dados aplicável a nível nacional no Estado que fornece os dados é obrigatório para o Estado que os recebe.	A Decisão Prüm está a ser implementada. Dez Estados-Membros foram autorizados a trocar dados de ADN cinco a trocar impressões digitais e sete a trocar dados relativos a veículos. A Noruega e Islândia terão brevemente acesso a este instrumento.	A Comissão deve apresentar um relatório de avaliação ao Conselho em 2012.

Quadro de apresentação geral dos instrumentos em vigor em implementação ou em estudo

Instrumento	Antecedentes	Finalidade(s)	Estrutura	Dados pessoais abrangidos	Acesso aos dados	Protecção dos dados	Conservação dos dados	Estado de implementação	Reexame
Directiva relativa à conservação de dados	Iniciativa dos Estados-Membros	Reforçar a investigação detecção e repressão de formas graves de criminalidade através da conservação de dados de tráfego das telecomunicaçõ es e de dados de localização.	Descentralizada este instrumento impõe obrigações aos fornecedores de serviços de telecomunicações em matéria de conservação de dados.	Números de telefone endereços IP e identificadores de equipamentos móveis.	As autoridades com direitos de acesso são definidas a nível nacional.	Directivas 95/46/CE e 2002/58/CE.	De 6 a 24 meses.	Seis Estados-Membros ainda não transpuseram esta directiva e os tribunais constitucionais alemão e romeno declararam as leis de execução inconstitucionais.	A Comissão deve apresentar um relatório de avaliação ao PE e ao Conselho em 2010.
Sistema europeu de informação sobre os registos criminais (ECRIS)	Iniciativa da Bélgica e proposta pela Comissão.	Melhorar a partilha transfronteiras de dados relativos aos registos criminais dos cidadãos da UE.	Descentralizada interconexão através de um conjunto de autoridades centrais que trocarão informações extraídas dos registos criminais através da rede s-TESTA.	Dados pessoais; condenações penas e crimes; dados adicionais incluindo impressões digitais (se disponíveis).	Autoridades judiciárias e autoridades administrativas competentes.	Normas específicas estabelecidas pela Decisão 2009 /315/JAI do Conselho que integra as disposições da Decisão 2005/876/JAI do Conselho e Decisão-Quadro 2008/977/JAI do Conselho Convenção 108 do CdE e Regulamento (CE) n.° 45/ 2001.	Aplicam-se as disposições nacionais em matéria de conservação de dados pois este instrumento só regula o intercâmbio de dados.	O ECRIS está a ser implementado. Nove Estados-Membros começaram o intercâmbio de dados por via electrónica.	A Comissão deve apresentar dois relatórios de avaliação ao PE e ao Conselho: sobre a Decisão-Quadro 2008/675/JHA em 2011; sobre a Decisão-Quadro 2009/315/JAI em 2015. A partir de 2016 a Comissão tem de publicar relatórios periódicos sobre o funcionamento da Decisão 2009/316/JAI do Conselho (ECRIS).

Quadro de apresentação geral dos instrumentos em vigor em implementação ou em estudo

Instrumento	Antecedentes	Finalidade(s)	Estrutura	Dados pessoais abrangidos	Acesso aos dados	Protecção dos dados	Conservação dos dados	Estado de implementação	Reexame
Unidades de informação financeira (FIU.net)	Iniciativa dos Países Baixos.	Trocar as informações necessárias para analisar e investigar actividades de branqueamento capitais e de financiamento do terrorismo.	Descentralizada as UIF procedem ao intercâmbio de dados através da FIU.net que utiliza a rede s-TESTA. A aplicação SIENA da Europol poderá brevemente reforçar a rede FIU.net.	Todos os dados com relevância para a análise e investigação de actividades de branqueamento capitais e de financiamento do terrorismo.	Unidades de informação financeira (criadas a nível dos serviços policiais das autoridades judiciárias ou das autoridades administrativas que dependem de autoridades financeiras.	Decisão-Quadro 2008/977/JAI do Conselho e Convenção 108 do CdE e Recomendação das Polícias R (87) 15 do CdE.	Aplicam-se as disposições nacionais em matéria de conservação de dados pois este instrumento só regula o intercâmbio de dados.	Vinte Estados-Membros participam na FIU.net uma aplicação de partilha de dados em linha utilizando a rede s-TESTA.	No quadro do seu Plano de acção para os serviços financeiros a Comissão reexamina a aplicação da Directiva 2005/60/CE desde 2009.
Cooperação entre os gabinetes de recuperação de bens (ARO)	Iniciativa dos Estados-Membros	Trocar as informações necessárias para detectar e identificar os produtos do crime	Descentralizada os ARO devem trocar informações utilizando a Iniciativa sueca. A aplicação SIENA da Europol poderá brevemente reforçar a cooperação entre os ARO.	Informações relativas a bens nomeadamente contas bancárias bens imóveis e veículos bem como informações sobre pessoas procuradas incluindo nomes e moradas e informações sobre accionistas ou empresas.	Gabinetes de recuperação de bens (ARO).	Convenção 108 do CdE Protocolo Adicional 181 e Recomendação das Polícias R (87) 15 do CdE.	Aplicam-se as disposições nacionais em matéria de conservação de dados pois este instrumento só regula o intercâmbio de dados.	Mais de vinte Estados-Membros criaram gabinetes ARO; doze participam num projecto-piloto que desenvolve a aplicação SIENA da Europol para o intercâmbio de informações relevantes para a detecção de bens.	A Comissão deve apresentar um relatório de avaliação ao Conselho em 2010.

Quadro de apresentação geral dos instrumentos em vigor em implementação ou em estudo

Instrumento	Antecedentes	Finalidade(s)	Estrutura	Dados pessoais abrangidos	Acesso aos dados	Protecção dos dados	Conservação dos dados	Estado de implementação	Reexame
Plataformas nacionais e da UE de luta contra a cibercriminalidade	Iniciativa da França.	Recolher analisar e trocar informações sobre crimes cometidos na Internet.	Descentralizada reúne as plataformas nacionais de alerta e a plataforma da UE de luta contra a cibercriminalidade da Europol. A aplicação SIENA da Europol poderá brevemente reforçar os intercâmbios de dados entre as plataformas de alerta.	Conteúdo ou comportamento ilícito detectado na Internet.	As plataformas nacionais recebem as informações dos cidadãos; a plataforma da UE de luta contra a cibercriminalidade da Europol recebe as informações sobre formas graves de cibercriminalidade transfronteiras da parte das autoridades responsáveis pela aplicação da lei.	Disposições específicas estabelecidas pela Decisão Europol e pela Decisão-Quadro 2008/977/JAI do Conselho Convenção 108 do CdE Protocolo Adicional 181 do CdE Recomendação das Polícias R (87) 15 do CdE e Regulamento (CE) n.° 45/2001.	Aplicam-se as disposições nacionais em matéria de conservação de dados pois esta medida só regula o intercâmbio de dados.	Quase todos os Estados-Membros criaram plataformas nacionais de alerta; A Europol trabalha na sua plataforma europeia de luta contra a cibercriminalidade.	As actividades da Europol cobrem a cibercriminalidade e no futuro dará conta das actividades da plataforma europeia de luta contra a cibercriminalidade no seu relatório anual apresentado ao Conselho para aprovação e ao Parlamento Europeu para informação.

Quadro de apresentação geral dos instrumentos em vigor em implementação ou em estudo

Instrumento	Antecedentes	Finalidade(s)	Estrutura	Dados pessoais abrangidos	Acesso aos dados	Protecção dos dados	Conservação dos dados	Estado de implementação	Reexame
Europol	Iniciativa dos Estados-Membros	Ajudar os Estados-Membros a prevenir e combater o crime organizado o terrorismo e outras formas graves de criminalidade que afectem dois ou mais Estados-Membros.	A Europol é uma agência da UE com base na Haia. A Europol está a desenvolver a rede SIENA a sua própria aplicação de intercâmbio seguro de informações.	O sistema de informação da Europol (SIE) contém dados pessoais nomeadamente identificadores biométricos condenações penais e ligações ao crime organizado suspeitos de crimes abrangidos pelo âmbito de competências da Europol. Os ficheiros de análise (AWF) contêm todos os dados pessoais pertinentes.	O SIE é acessível às unidades nacionais da Europol aos agentes de ligação ao pessoal e ao director da Europol. O acesso aos AWF é permitido aos agentes de ligação. Os dados pessoais podem ser trocados com os países terceiros que tenham concluído um acordo com a Europa.	Disposições específicas estabelecidas pela Decisão Europol e pela Decisão-Quadro 2008/977/JAI do Conselho Convenção 108 do CdE Protocolo Adicional 181 do CdE Recomendação das Polícias R (87) 15 do CdE e Regulamento (CE) n.° 45/2001.	Os AWF podem ser conservados por um período máximo de três anos com possibilidade de prorrogação por mais três anos.	A Europol é activamente utilizada por todos os Estados-Membros bem como pelos países terceiros com os quais concluiu um acordo operacional. A nova base jurídica da Europol foi transposta por todos os Estados-Membros.	Uma instância comum de controlo supervisiona as actividades da Europol em matéria de tratamento de dados pessoais e de transmissão destes dados a outras partes. A Europol apresenta relatórios periódicos ao PE e ao Conselho. A Europol apresenta igualmente um relatório anual sobre as suas actividades ao Conselho para aprovação e ao Parlamento Europeu para informação.

Quadro de apresentação geral dos instrumentos em vigor em implementação ou em estudo

Instrumento	Antecedentes	Finalidade(s)	Estrutura	Dados pessoais abrangidos	Acesso aos dados	Protecção dos dados	Conservação dos dados	Estado de implementação	Reexame
Eurojust	Iniciativa dos Estados-Membros	Melhorar a coordenação das investigações e dos procedimentos penais nos Estados-Membros e a reforçar a cooperação entre as autoridades relevantes.	A Eurojust é um órgão da UE com base na Haia que utiliza a rede s-TESTA para o intercâmbio de dados.	Dados pessoais de suspeitos e autores de crimes que afectem dois ou mais Estados-Membros incluindo dados biográficos contactos perfis de ADN fotografias impressões digitais bem como dados de tráfego de telecomunicações e dados de localização.	Os vinte sete membros nacionais da Europol que podem partilhar dados com as autoridades nacionais e de países terceiros mediante o consentimento da fonte de informações.	Normas específicas estabelecidas pela Decisão Eurojust e Decisão-Quadro 2008/977/JAI do Conselho Convenção 108 do CdE Protocolo Adicional 181 e Recomendação das Polícias R (87) 15 do CdE.	As informações devem ser suprimidas quando tiverem preenchido a finalidade para que foram fornecidas e logo que um caso esteja concluído.	A base jurídica alterada da Eurojust está actualmente a ser transposta pelos Estados-Membros.	A Comissão deve reexaminar os intercâmbios de informações entre os membros nacionais da Eurojust até Junho de 2014. Até Junho de 2013 a Eurojust deve apresentar ao Conselho e à Comissão um relatório sobre a concessão de acesso ao seu sistema de gestão de processos. Uma instância comum de controlo supervisiona as actividades da Eurojust em matéria de tratamento de dados pessoais e apresenta anualmente um relatório ao Conselho. O Presidente do colégio da Eurojust apresenta ao Conselho um relatório anual sobre as actividades da Eurojust que o Conselho transmite ao PE.

Quadro de apresentação geral dos instrumentos em vigor em implementação ou em estudo

Instrumento	Antecedentes	Finalidade(s)	Estrutura	Dados pessoais abrangidos	Acesso aos dados	Protecção dos dados	Conservação dos dados	Estado de implementação	Reexame
Acordos PNR com os EUA e a Austrália; Acordo API/PNR com o Canadá	Iniciativa da Comissão.	Prevenir e combater o terrorismo e outras formas graves de criminalidade transfronteiras.	Acordos internacionais.	Os acordos com os EUA e a Austrália dizem respeito a 19 categorias de dados incluindo dados biográficos informações relativas às reservas e aos pagamentos e informações suplementares; o acordo canadiano prevê 25 tipos de dados semelhantes.	O Ministério da Segurança Interna (Department of Homeland Security) americano o Serviço de Fronteiras canadiano (Canada Border Services Agency) e os Serviço Aduaneiro australiano podem partilhar dados com os serviços nacionais responsáveis pela repressão e luta contra o terrorismo.	As normas em matéria de protecção de dados são definidas nos acordos internacionais específicos.	EUA: sete anos de utilização activa oito anos de utilização passiva; Austrália: três anos e meio de utilização activa dois anos de utilização passiva; Canadá: 72 horas de utilização activa três anos e meio de utilização passiva.	Os acordos concluídos com os EUA e a Austrália são provisoriamente aplicáveis; o acordo com o Canadá entrou em vigor. A Comissão renegociará estes acordos. Seis Estados-Membros da UE adoptaram legislação que permite a utilização dos dados PNR para fins repressivos.	Cada acordo prevê um reexame periódico e os acordos canadiano e australiano incluem igualmente uma cláusula de denúncia.

Quadro de apresentação geral dos instrumentos em vigor em implementação ou em estudo

Instrumento	Antecedentes	Finalidade(s)	Estrutura	Dados pessoais abrangidos	Acesso aos dados	Protecção dos dados	Conservação dos dados	Estado de implementação	Reexame
Acordo TFTP UE-EUA	Iniciativa da Comissão.	Prevenir investigar detectar ou reprimir o terrorismo ou o seu financiamento.	Acordo internacional.	Dados de mensagens de pagamentos financeiros que incluem nomeadamente nome número de conta morada e número de identificação da pessoa de origem e do destinatário das transacções financeiras.	O Departamento do Tesouro pode partilhar os dados pessoais extraídos das mensagens de pagamentos financeiros com os serviços repressivos organismos responsáveis pela segurança pública ou autoridades responsáveis pela luta contra o terrorismo dos EUA dos Estados-Membros da UE e a Europol ou a Eurojust. A transferência ulterior de dados para países terceiros está sujeita à autorização dos Estados-Membros.	O acordo prevê cláusulas estritas de limitação das finalidades e de proporcionalidade.	Os dados pessoais extraídos das mensagens de pagamentos financeiros só podem ser conservados durante o tempo necessário para efeitos de investigações ou acções repressivas individuais. Os dados não extraídos só podem ser conservados durante cinco anos.	Em 8 de Julho de 2010, o PE autorizou a celebração do Acordo TFTP UE-EUA. O Conselho deve agora adoptar uma decisão do Conselho relativa à celebração deste Acordo, na sequência da qual o Acordo entrará em vigor, através de uma troca de cartas entre as duas Partes.	A Comissão deve reexaminar este acordo de seis meses após a sua entrada em vigor. O seu relatório de avaliação deve ser apresentado ao PE e ao Conselho.