COMISSÃO
EUROPEIA

Bruxelas, 27.11.2013
COM(2013) 842 final

COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO

Sistema europeu de deteção do financiamento do terrorismo (TFTS-UE)

{SWD(2013) 488 final}
{SWD(2013) 489 final}

COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO

Sistema europeu de deteção do financiamento do terrorismo (TFTS-UE)

Na sequência da Comunicação de 13 de julho de 2011 [COM (2011) 429], a presente comunicação tem por objetivo informar o Parlamento Europeu e o Conselho dos resultados da análise feita no que diz respeito à viabilidade de estabelecer um sistema europeu de deteção do financiamento (TFTS-UE).

1. CONTEXTO

1.1. Origem da questão e definição

Durante as negociações que antecederam a conclusão do Acordo TFTP entre a UE e os EUA[1], foi debatida a questão de saber qual a melhor forma de proteger os dados pessoais e respeitar os direitos fundamentais no âmbito desse acordo. Algumas partes interessadas argumentaram que extrair dados em território europeu limitaria o volume de dados transferidos para os EUA e, por conseguinte, asseguraria um nível mais elevado de garantias em matéria de proteção de dados. Alguns Estados-Membros consideraram que seria uma mais-valia a longo prazo desenvolver um sistema europeu de deteção do financiamento do terrorismo. O Parlamento Europeu solicitou ao Conselho e à Comissão que tomassem todas as medidas necessárias para elaborar, a nível europeu, uma solução duradoura e juridicamente sólida para o problema da extração dos dados solicitados no território europeu. O Conselho e o Parlamento Europeu, ao darem o seu acordo ao TFTP UE-EUA, convidaram a Comissão a apresentar, no prazo de um ano a contar da data de entrada em vigor desse acordo, um quadro jurídico e técnico para a extração de dados no território da UE e, no prazo de três anos a contar da data de entrada em vigor do mesmo acordo, um relatório sobre o desenvolvimento de um sistema equivalente na UE[2]. Além disso, o artigo 11.º do Acordo TFTP UE-EUA estabelece que, durante a vigência do acordo, a Comissão Europeia realizará um estudo sobre a eventual introdução de um sistema equivalente da UE que permita transferências de dados melhor direcionadas.

Para efeitos da presente comunicação, um sistema equivalente da UE deve ser dissociado de um quadro relativo à extração de dados no território da UE. Um *quadro relativo à extração de dados no território da UE* deve ser entendido como um sistema que autorize as pesquisas de dados atualmente transmitidos pela UE aos Estados Unidos, mas a realizar no território da UE. Em contrapartida, um *sistema equivalente da UE* seria um sistema europeu independente para a deteção do financiamento do terrorismo através do acesso a dados, bem como de pesquisas e análises de dados do ou dos fornecedores designados. O estabelecimento de um sistema da UE exigiria a alteração do Acordo TFTP UE-EUA.

1.2. Medidas adotadas

Em dezembro de 2010, a Comissão encomendou um estudo que foi alargado em julho de 2011, de forma a abranger a opção suplementar de contemplar um regime de conservação e de

[1] JO L 195 de 27.7.2010, p. 5.
[2] Decisão do Conselho de 13 de julho de 2010, JO L 195 de 27.7.2010, p. 3.

extração de dados. Enquanto decorria esse estudo, a Comissão realizou quatro reuniões de peritos, em que participaram partes interessadas, como a Europol, a Autoridade Europeia para a Proteção de Dados, o fornecedor designado para o TFTP[3] e muitos peritos dos Estados-Membros em representação de ministérios, agências com funções coercivas e serviços de informações e autoridades responsáveis pela proteção de dados.

Em 13 de julho de 2011, a Comissão, na sua Comunicação ao Parlamento Europeu e ao Conselho (a seguir designada «Comunicação de 2011»), apresentou cinco possíveis opções que tinha identificado em relação a um sistema europeu de deteção do financiamento do terrorismo (a seguir designado «TFTS-UE»). Entre essas opções, três foram consideradas viáveis. A Comunicação de 2011 teve por objetivo promover o debate sobre a via a seguir e integrar os seus resultados na avaliação de impacto a realizar.

A questão foi apresentada em outubro de 2011 ao Conselho JAI e à Comissão das Liberdades Cívicas do Parlamento Europeu.

Como os Estados-Membros e o Parlamento Europeu não manifestaram uma preferência clara por qualquer das opções propostas, foi decidido analisá-las na totalidade na avaliação de impacto da Comissão, descrevendo-as mais pormenorizadamente através de diferentes subopções. A presente comunicação tem por base a referida avaliação de impacto[4].

2. PRINCÍPIOS FUNDAMENTAIS E OPÇÕES IDENTIFICADAS PELA COMISSÃO

2.1. Princípios da Estratégia de Gestão da Informação adotada sob a Presidência sueca

Na sua análise sobre a proposta de rumo a seguir, a Comissão tem em consideração os princípios fundamentais estabelecidos na Estratégia de Gestão da Informação de 2009[5], mais tarde integrada e aprofundada na Comunicação da Comissão intitulada «Apresentação geral da gestão da informação no domínio da liberdade, segurança e justiça» de 2010[6] e na Comunicação sobre o modelo europeu de intercâmbio de informações de 2012[7].

Muito importante neste contexto são os princípios que garantem os direitos fundamentais, bem como os princípios da necessidade, da proporcionalidade e da boa relação custo/eficácia.

Proteger os *direitos fundamentais* consagrados na Carta dos Direitos Fundamentais da União Europeia, em especial o direito à privacidade e à proteção dos dados pessoais, é uma preocupação prioritária da Comissão quando elabora novas propostas que impliquem o tratamento de dados pessoais no domínio da segurança interna. Os artigos 7.° e 8.° da Carta estabelecem que «todas as pessoas têm direito ao respeito pela sua vida privada e familiar» e «à proteção dos dados de caráter pessoal que lhes digam respeito» O artigo 16.° do Tratado sobre o Funcionamento da União Europeia (TFUE), que é vinculativo para as atividades dos Estados-Membros e das instituições, órgãos e organismos da União, reafirma o direito de todas as pessoas «à proteção dos dados de caráter pessoal que lhes digam respeito». Nos

[3] Society for Worldwide Interbank Financial Telecommunication (SWIFT).
[4] Documento de trabalho dos serviços da Comissão, SWD 2013 (xx) de .
[5] Conclusões do Conselho de 30 de novembro de 2009 sobre uma Estratégia de Gestão da Informação para a segurança interna da UE, documento 16637/09.
[6] COM(2010) 385 de 20 de julho de 2010.
[7] COM(2012) 735 de 7 de dezembro de 2012.

termos do artigo 52.º da Carta, sob reserva do princípio da proporcionalidade, essas restrições ao exercício dos direitos e liberdades reconhecidos pela Carta só podem ser introduzidas se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros.

A ingerência no direito ao respeito da vida privada é considerada *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.

Embora seja difícil avaliar a totalidade dos custos do terrorismo em termos financeiros, continua a ser pertinente ter em conta uma boa relação custo-eficácia. Esta abordagem irá basear-se nas soluções preexistentes, a fim de reduzir as sobreposições ao mínimo e maximizar as eventuais sinergias. É necessária uma avaliação visando saber se é possível alcançar os objetivos da proposta através de uma melhor utilização dos instrumentos existentes.

2.2. Abordagem

À luz dos princípios acima referidos, a Comissão examinou se um TFTS-UE seria necessário e proporcional, tendo em conta os seus custos, benefícios e impacto sobre os direitos fundamentais comparativamente à situação atual.

Em termos de *benefícios*, o sistema da UE poderia reforçar as capacidades da União e dos seus Estados-Membros para aceder a dados pertinentes e melhorar as respetivas capacidades analíticas visando localizar e identificar os terroristas através de operações financeiras. Uma vez que as operações financeiras podem fornecer informações valiosas que outras fontes não conseguem disponibilizar, esta ferramenta seria particularmente importante para a deteção de atividades terroristas e das pessoas envolvidas. Por conseguinte, um TFTS-UE poderia representar uma ferramenta adicional de obtenção de informações e de investigação no domínio da luta contra o terrorismo, reforçando igualmente a segurança na União, em especial se fosse aplicável a vários fornecedores de dados financeiros e tipos de operações. Os benefícios de um TFTS-UE têm de ser ponderados em relação aos custos estimados da sua entrada em funcionamento e manutenção, incluindo o ónus financeiro a cargo da União Europeia, dos Estados-Membros e dos fornecedores designados dos dados.

2.3. Apresentação das opções

Foram tidas em conta várias opções quer para o *quadro relativo à extração de* dados no território da UE quer para o *sistema equivalente da UE*.

2.3.1. Um quadro relativo à extração de dados no território da UE

Um quadro relativo à extração de dados no território da UE poderia ser implementado através de um sistema de conservação e de extração de dados armazenados pelo fornecedor designado, permitindo o acesso direto aos dados, e que são atualmente fornecidos aos EUA ao abrigo do TFTP. Este acesso direto seria autorizado aos analistas ou peritos americanos mandatados para o efeito.

Segundo esta opção, haveria a possibilidade de conservar os dados no servidor do fornecedor designado durante um determinado período de tempo, e pesquisar diretamente neste servidor. No entanto, o atual fornecedor designado ao abrigo do TFTP UE-EUA instaurou medidas

sólidas de proteção e de segurança dos dados que não permitem a identificação das pessoas mencionadas nos dados da mensagem e, portanto, a sua base de dados atual não permite pesquisas baseadas em dados pessoais. Seria necessário, portanto, criar uma base de dados separada.

Em alternativa, os dados poderiam ser extraídos e conservados num local seguro diferente no território da UE. Os analistas ou peritos americanos autorizados a efetuar pesquisas poderiam estar fisicamente presentes nas instalações do fornecedor designado ou ter acesso remoto aos dados. Em todo o caso, e independentemente da localização dos dados, garantias bastante estritas e sólidas teriam de ser instauradas e adaptadas à criação desse tipo de sistema.

2.3.2. Um sistema equivalente da UE

Foi avaliado um conjunto de opções no que diz respeito a um sistema equivalente da UE (como indicado na Comunicação de 2011), incluindo um sistema totalmente centralizado a nível da UE, um sistema descentralizado a nível dos Estados-Membros e três sistemas híbridos em que tanto a UE como os Estados-Membros participariam.

Para cada opção, há diferentes possibilidades relativamente ao âmbito do sistema europeu. Existem escolhas a fazer quanto aos tipos de mensagens e fornecedores designados que seriam incluídos no sistema. Um sistema equivalente da UE poderia limitar-se às mensagens financeiras ou ir além delas e do fornecedor designado atualmente abrangido pelo Acordo TFTP UE-EUA.

- A opção por um sistema totalmente centralizado a nível da União significa que um único organismo da UE desempenharia todas as principais funções do sistema, ou seja, solicitar a extração de dados, armazenar dados, pesquisar, realizar a análise de informações de segurança, salvaguardar e controlar o sistema e difundir indícios aos Estados-Membros. Esta opção é juridicamente inadequada por não respeitar o artigo 72.º do TFUE, que estabelece que a responsabilidade pela manutenção da ordem pública e de garantia da segurança interna incumbe principalmente aos Estados-Membros. Um sistema desse tipo não seria viável nem aceitável para os Estados-Membros, na medida em que exigiria a criação de uma forma de estrutura de informação centralizada a nível da UE.
- Um sistema completamente descentralizado a nível dos Estados-Membros, significa que a sua gestão incumbiria às autoridades competentes nacionais, não sendo desempenhada qualquer função a nível da UE. Os dados poderiam ser transferidos e pesquisados por todos os 28 Estados-Membros em paralelo. Esta opção multiplica os fluxos de dados e teria importantes implicações a nível dos custos. Implicaria igualmente um risco acrescido de tratamento incoerente dos dados e a criação de mecanismos desiguais de proteção de dados. Esta opção não é, por conseguinte, considerada viável.

As duas opções referidas foram, portanto, excluídas de uma avaliação mais aprofundada.

As restantes três opções relativas a um sistema equivalente da UE implicam a repartição de diferentes funções entre organizações diferentes a nível nacional e da UE («sistemas híbridos»).

Em todos estes sistemas híbridos, os dados devem ser solicitados de forma contínua e interativa ao ou aos fornecedores designados, bem como extraídos e armazenados numa base de dados num local seguro na UE. As pesquisas seriam efetuadas nesta base de dados central. Do mesmo modo para todas as opções, devem ser criadas garantias adequadas de proteção dos dados.

- A) No primeiro sistema híbrido, ou seja, o serviço de coordenação e de análise do TFTS-UE, teria de ser criada uma unidade central da UE. As suas atribuições consistiriam em solicitar dados ao ou aos fornecedores designados, efetuar pesquisas, analisar informações de segurança e comunicar os resultados. A diferença em relação a um sistema totalmente centralizado seria que os Estados-Membros teriam acesso direto ao sistema e poderiam solicitar que as pesquisas fossem efetuadas em seu nome pela unidade central ou pelos seus próprios analistas.
- B) O segundo sistema híbrido, ou seja o serviço de extração do TFTS-UE, envolveria igualmente a criação de uma unidade central. Contudo, no âmbito desta opção, o organismo da UE efetuaria as pesquisas a pedido dos Estados-Membros e comunicar-lhes-ia os resultados sem analisar as informações de segurança. O organismo da UE, contudo, poderia realizar as suas próprias pesquisas e analisar o resultado das mesmas.
- C) No último sistema híbrido ou seja, o serviço de coordenação das unidades de informação financeira[8] (UIF), seria criada uma plataforma *ad hoc* europeia. Não seria um organismo permanente, mas um grupo de peritos sobre informações financeiras que participariam em reuniões. A plataforma UIF poderia ser eventualmente adaptada para este efeito. Cada Estado-Membro designaria um representante que atuaria em seu nome. Esta autoridade *ad hoc* compilaria os pedidos das UIF de cada Estado-Membro e apresentá-los-ia ao ou aos fornecedores designados com base nesses pedidos dos Estados-Membros. O representante de cada Estado-Membro seria encarregado de efetuar pesquisas, realizar análises e gerir os resultados em nome do respetivo Estado-Membro. Caberia depois às autoridades competentes dos Estados-Membros utilizar os indícios e difundi-los subsequentemente a nível nacional.

2.3.3. Status quo: Acordo TFTP UE-EUA

Atualmente, a UE e os Estados-Membros podem solicitar que as pesquisas sejam efetuadas pelos EUA ao abrigo do Acordo TFTP UE-EUA que regula o tratamento de mensagens de pagamentos financeiros e a sua transferência da União Europeia para os Estados Unidos para efeitos do Programa de Deteção do Financiamento do Terrorismo («TFTP»).

O TFTP é uma ferramenta de luta contra o terrorismo desenvolvida pelos EUA na sequência dos atentados terroristas de 11 de setembro de 2001. Baseia-se na consulta dos dados transmitidos pelo fornecedor designado, incluindo os dados transferidos a partir da União Europeia.

O Acordo TFTP UE-EUA regula exaustivamente o processo de pedido dos dados pelas autoridades americanas. A Europol verifica se os pedidos de dados recebidos dos Estados Unidos são conformes com o Acordo e, em especial, se são limitados ao mínimo possível de modo a reduzir o volume de dados transferidos. Numerosas disposições cobrem o tratamento

[8] Decisão 2000/642/JAI do Conselho, de 17 de outubro de 2000, relativa a disposições de cooperação entre as unidades de informação financeira dos Estados-Membros em matéria de troca de informações.

seguro, a conservação e a supressão dos dados. Os dados fornecidos são guardados num ambiente físico seguro e conservados separadamente de outros dados. O Acordo prevê um período de conservação de cinco anos e a obrigação de avaliar regularmente a necessidade de conservar os dados. Os supervisores independentes estabelecidos nos EUA incluem dois supervisores escolhidos pela União. Exercem um controlo contínuo sobre a forma como o sistema funciona e têm a possibilidade de verificar cada pesquisa efetuada pelo Departamento do Tesouro dos Estados Unidos, a fim de assegurar que o conteúdo de uma pesquisa está relacionado com o terrorismo ou o seu financiamento.

O Acordo inclui igualmente disposições relativas aos direitos de acesso e de retificação de dados pessoais, bem como sobre as vias de recurso disponíveis. Prevê ainda que qualquer pessoa que considere que os seus dados pessoais foram tratados em violação do Acordo tem o direito de interpor recurso administrativo e judicial nos termos da legislação da União Europeia, dos seus Estados-Membros e dos Estados Unidos, respetivamente. Ao abrigo da legislação americana, as pessoas, independentemente da nacionalidade ou do país de residência, dispõem de vias de recurso judiciais contra uma medida administrativa negativa.

A legislação aplicável relativamente a vias de recurso contra uma medida administrativa negativa do Departamento do Tesouro relacionada com dados pessoais recebidos ao abrigo do Acordo inclui a *Administrative Procedure Act* (Lei relativa ao procedimento administrativo) e a *Freedom of Information Act* (Lei relativa à liberdade de informação). A *Administrative Procedure Act* permite que as pessoas que foram lesadas em resultado de uma ação do Governo americano tenham direito a recurso judicial contra essa ação. A *Freedom of Information Act* permite que as pessoas recorram às vias administrativas e judiciais para consultar os registos governamentais. Os atuais procedimentos uniformes para o acesso e/ou a retificação, o apagamento ou o bloqueio de dados pessoais, acordados entre a Comissão, os EUA e o Grupo de Trabalho do artigo 29.º, têm por objetivo facilitar o exercício desses direitos pelos cidadãos da União. A aplicação do Acordo e as respetivas garantias e controlos são sujeitos a reexames periódicos, ao abrigo do artigo 13.º do Acordo. Foram realizados dois reexames desta natureza em 2011[9] e 2012[10], que concluiram que o Acordo estava a ser corretamente aplicado. Um terceiro reexame está previsto para a primavera de 2014. O relatório conjunto respeitante ao valor dos dados fornecidos, elaborado em conformidade com o artigo 6.º do Acordo, demonstra os benefícios do TFTP em matéria de prevenção e luta contra o terrorismo e o seu financiamento, bem como da sua utilização por vários Estados-Membros. As informações obtidas ao abrigo do TFTP e a sua exatidão permitem a identificação e a localização de terroristas e das suas redes de apoio em todo o mundo. Contribui para revelar as atuais estruturas financeiras das organizações terroristas e a identificação de novos fluxos de apoio financeiro e intervenientes envolvidos.

3. AVALIAÇÃO

Ao avaliar se deve ou não ser proposta a criação de um TFTS-UE, a Comissão tem de conciliar as diferentes opiniões e expectativas em relação ao nível de ambição de um sistema da União Europeia. Os objetivos do TFTS-UE são considerados de forma diferente pelos vários decisores políticos e partes interessadas. A Comissão examinou as possibilidades e implicações de ambos os cenários, comparando-as com os princípios de elaboração e

[9] SEC(2011) 438 de 30 de março de 2011.
[10] SWD(2012) 454 de 14 de dezembro de 2012.

aplicação de novas iniciativas, acima referidos em pormenor. Em especial, cada opção foi ponderada em termos da necessidade, da proporcionalidade e da relação custo-eficácia.

3.1. Um quadro relativo à extração de dados no território da UE

Tal como descrito no ponto 2.3.1, a opção por um regime de conservação e extração, no território da UE, serviria para recolher, armazenar e pesquisar dados, que são atualmente transferidos para os EUA ao abrigo do Acordo TFTP UE-EUA. Portanto, não geraria benefícios adicionais em termos de informações de segurança para a UE ou os seus Estados-Membros em comparação com a situação atual. Pelo contrário, com os dados TFTP armazenados nos EUA e na UE, a fragmentação das pesquisas, que atualmente são efetuadas num conjunto de dados TFTP, poderia ter um impacto negativo sobre a qualidade e a quantidade dos indícios e agravar a eficiência global do TFTP. Também poderia retardar significativamente o processo de análise, uma vez que poderiam ser necessárias diferentes pesquisas consecutivas sobre dados TFTP armazenados nas duas localizações para seguir de forma mais aprofundada um determinado indício. A rapidez é frequentemente essencial nas investigações de âmbito terrorista.

A extração dos dados em território europeu em vez do território americano não constitui por si só uma garantia de melhor proteção dos dados pessoais. A proteção do acesso aos dados é fundamental para assegurar o tratamento adequado dos dados, independentemente da sua localização. Para este efeito, deveria ser criado um conjunto de garantias sólidas para assegurar a conformidade do tratamento e processamento dos dados com os requisitos necessários. O sistema teria de ser equipado com uma função de controlo direcionada para a verificação dos pedidos de pesquisas e a sua justificação. O papel dos supervisores independentes seria crucial para assegurar a utilização dos dados para os fins definidos num acordo específico. Deveriam ser adotadas medidas para impedir o acesso não autorizado aos dados ou a sua divulgação, designadamente conservar os dados num ambiente físico seguro. Teriam de ser instaurados procedimentos relativos ao acesso e à retificação de dados pessoais e às vias de recurso, devendo ser igualmente encomendada uma auditoria externa para assegurar o correto funcionamento do sistema.

Ao abrigo do Acordo TFTP UE-EUA, as autoridades americanas não têm acesso a todos os dados do fornecedor designado, mas apenas a conjuntos de dados que os EUA solicita e que a Europol aprova com base em análises de risco de terrorismo anteriores e atuais. A menos que seja criado um mecanismo semelhante de limitação inicial dos pedidos de dados, permitir que sejam efetuadas pesquisas de todos os dados na posse do fornecedor designado aumentaria ainda mais o risco e o impacto sobre os direitos de proteção de dados. Esta situação exigiria uma reformulação significativa da forma como o fornecedor designado trabalha e armazena os seus dados. Atualmente, os dados de mensagens de pagamentos financeiros objeto do Acordo são conservados de forma a não permitir a identificação das pessoas mencionadas no respetivo conteúdo. Cada mensagem financeira é cifrada e só pode ser consultada através de metadados, ou seja, a data em que a mensagem foi enviada, o tipo de mensagem, e os bancos envolvidos que enviaram e receberam a mensagem. O fornecedor designado instaurou medidas muito sólidas de proteção e segurança dos dados, a fim de proteger os dados dos seus clientes em todo mundo. Por conseguinte, para permitir que as pesquisas sejam efetuadas diretamente no servidor do atual fornecedor designado, todas essas mensagens devem, em primeiro lugar, ser descodificadas. Fazê-lo seria excessivo e desproporcionado, uma vez que o servidor do fornecedor designado contém mais mensagens do que as exigidas para efeitos da

luta contra o financiamento do terrorismo. Além disso, um acesso direto para efeitos de pesquisa seria tremendamente invasivo em termos de operações diárias do fornecedor designado e criaria riscos operacionais, de segurança e sistémicos significativos. Por conseguinte, tal sistema exigiria a criação de uma base de dados separada no território da UE para armazenar os dados necessários do fornecedor designado.

Seria necessário um importante investimento para colocar o sistema em funcionamento e assegurar a sua plena conformidade com os requisitos de segurança. As instalações do fornecedor designado ou outro local seguro teriam de ser adaptados às necessidades específicas, teriam de ser desenvolvidas e mantidas soluções informáticas e técnicas, e teria de ser contratado e formado pessoal bastante qualificado para gerir e supervisionar o sistema.

No âmbito desta opção, a UE e os Estados-Membros suportariam todos os inconvenientes e custos de um mecanismo criado unicamente para servir o TFTP, um instrumento pertencente a um país terceiro. Atualmente, esta opção não parece ser necessária ou proporcional nem ter uma boa relação custo-eficácia, uma vez que não permitiria obter benefícios adicionais em termos de informações de segurança, a sua criação seria dispendiosa e exigiria muito do ponto de vista técnico, podendo ainda gerar riscos para a proteção dos dados pessoais.

3.2. Um sistema equivalente da UE

Um TFTS-UE totalmente centralizado foi excluído da avaliação pormenorizada devido à falta de uma base jurídica e à possibilidade remota de que os Estados-Membros aceitassem um papel centralizador da UE num domínio que é da sua competência. Um sistema completamente descentralizado foi excluído por vir a ter um impacto considerável em termos de custos e um impacto multiplicado sobre os direitos de proteção de dados. Os três sistemas híbridos avaliados permitiriam graus variáveis de controlo de cada Estado-Membro sobre as pesquisas por eles efetuadas e pelo organismo centralizado a nível da UE.

Alargar o âmbito de um sistema equivalente da UE para cobrir as câmaras de compensação automatizadas (*Automated Clearance Houses*), o dinheiro eletrónico e outros dados não financeiros, implicaria benefícios a nível de informações de segurança através do aumento da capacidade da UE para detetar pagamentos dentro da UE, e poderia criar um sistema mais à prova do tempo do que um sistema que trata apenas da transmissão de mensagens financeiras. No entanto, cada novo fornecedor designado aumentaria o risco de violação dos direitos de proteção de dados e, por isso, seria necessário um conjunto estrito de condições, garantias e outras medidas de controlo. Este aspeto também aumentaria os encargos administrativos impostos aos fornecedores designados. Introduzir múltiplos fornecedores de dados e mensagens para criar um sistema de tal forma complexo, em termos técnicos e de organização, também aumentaria consideravelmente os custos.

Em consequência desta análise, um eventual TFTS-UE apenas utilizaria dados das mensagens financeiras, uma vez que a Comissão considera que os benefícios adicionais da utilização de múltiplos tipos de dados e fornecedores não compensariam os custos significativos para as empresas privadas e os danos causados à privacidade e aos direitos de proteção de dados que tal sistema implicaria. Assim, uma vez que um sistema europeu apenas abrangeria o mesmo fornecedor designado e o mesmo tipo de mensagem que o TFTP, a qualidade e a quantidade de indícios recebidos, bem como o risco para os dados, seriam comparáveis ao TFTP UE-EUA.

Tal como acima referido, existem três opções para este sistema equivalente da UE: A) o serviço de coordenação e de análise do TFTS-UE, B) o serviço de extração do TFTS-UE, e C) o serviço de coordenação das unidades de informação financeira.

A opção A seria suscetível de ter efeitos positivos sobre a prevenção do terrorismo e o reforço da segurança na UE. Tendo duas equipas, da UE e dos Estados-Membros, a efetuarem pesquisas e a analisarem os resultados, contribuiria em certa medida para assegurar que os requisitos específicos das informações de segurança da UE e dos Estados-Membros são plenamente tidos em conta e que o sistema é direcionado em especial para a «ameaça contra a UE». Contudo, esta melhoria estaria dependente da vontade e capacidade dos Estados-Membros para partilharem informações e análises a médio e longo prazo. Não é claro em que medida se pode confiar neste maior fluxo de informações. Além disso, uma vez que os Estados-Membros poderiam continuar a solicitar pesquisas dos EUA no âmbito do TFTP, o sistema em análise necessitaria de uma maior adesão e cooperação dos Estados-Membros, caso se pretenda que o mesmo fornecesse uma panorâmica mais coerente da UE.

A opção B poderia ter algum impacto positivo na prevenção do terrorismo e no reforço da segurança na UE. O sistema seria mais reativo às análises de ameaça contra a UE, uma vez que as pesquisas seriam realizadas em conformidade com os requisitos específicos das informações de segurança dos Estados-Membros. Todavia, o papel do organismo centralizado a nível da UE seria limitado às pesquisas e transferência das respostas sobre os dados ao Estado-Membro requerente; agiria sobretudo como guardião do sistema. Em seu resultado, não haveria análise a nível da UE e o sistema estaria inteiramente dependente dos Estados-Membros que partilham análises entre si, fora do sistema, caso se pretendesse obter uma perspetiva coerente das informações de segurança viesse a ser estabelecida. A incapacidade do sistema para assegurar uma abordagem uniforme das definições das pesquisas aumentaria o risco de falsos positivos, interferindo assim com os direitos de proteção de dados e a privacidade.

A opção C seria capaz de dar resposta às necessidades específicas de informações de segurança dos Estados-Membros e, por conseguinte, teria algum impacto positivo na prevenção do terrorismo e no reforço da segurança. Contudo, como as unidades nacionais de informação financeira seriam responsáveis pelas pesquisas e análises dos respetivos Estados-Membros, esta opção apresenta o mesmo tipo de inconvenientes que a opção B, ou seja, uma panorâmica clara só poderia ser alcançada com a cooperação reforçada dos Estados-Membros, fora do sistema. Além disso, as unidades de informação financeira centrariam a sua atenção apenas em informações financeiras e o fosso entre estas informações e as informações de segurança em geral tornaria mais difícil estabelecer ligações e detetar o financiamento do terrorismo. Existe igualmente um nível muito baixo de participação da UE nesta opção, e a capacidade seria reforçada principalmente a nível nacional.

Todas estas opções implicariam custos significativos para a UE, os Estados-Membros e o fornecedor designado, incluindo, nomeadamente, o custo de desenvolvimento da infraestrutura informática, de instalações seguras e o custo de dezenas, ou mesmo centenas, de técnicos responsáveis pela gestão do sistema e execução das garantias e controlos. Cada um destes eventuais sistemas, porém, pode contribuir para uma melhoria da situação em matéria de segurança na Europa, pois utilizariam avaliações de ameaças específicas às necessidades europeias.

Um instrumento independente vocacionado para as informações de segurança e a investigação no território europeu eliminaria o requisito de transferência de dados para os EUA. No entanto, um TFTS-UE continuaria a exigir garantias estritas em matéria de proteção de dados e controlos análogos aos que já vigoram ao abrigo do Acordo TFTP UE-EUA e, em todo o caso, conformes com o direito da UE e o acervo em matéria de proteção de dados dos Estados-Membros. Qualquer pedido de pesquisa de dados nos sistemas da UE necessitaria de ser verificado em conformidade com a rigorosa limitação da finalidade à luta contra o terrorismo e ao seu financiamento, incluindo sobre a questão de saber se a transferência de dados seria justificada. Em especial, os supervisores independentes qualificados seriam obrigados a verificar que cada pesquisa da UE ou de um Estado-Membro foi devidamente autorizada e se seria necessária para efeitos da luta contra o terrorismo e o seu financiamento. O processamento e o armazenamento seguros dos dados teriam de ser assegurados e impedido o acesso não autorizado aos mesmos. Seria necessária uma auditoria externa ao funcionamento correto do sistema e de todas as suas garantias. Todos os procedimentos necessários ao acesso e à retificação de dados pessoais e as vias de recurso teriam de ser integrados no sistema.

Em conclusão, em consonância com os pedidos do Parlamento Europeu e do Conselho, a Comissão avaliou as eventuais opções de um TFTS-UE, incluindo um regime para a extração e conservação dos dados.

Esta avaliação tem em conta os princípios consagrados na Estratégia de Gestão da Informação que foi aprovada sob a égide da Presidência sueca. Qualquer sistema criado deve ser necessário, proporcional e ter uma boa relação custo-eficácia, devendo respeitar os direitos fundamentais. A análise da Comissão, tal como acima pormenorizada e na avaliação de impacto, revela que cada uma das opções viáveis apresenta vantagens e desvantagens. A Comissão, contudo, não teve em conta as opções consideradas não viáveis, como atrás indicado.

Tendo em conta as informações reunidas, a necessidade de apresentar uma proposta relativa a um TFTS europeu não está claramente demonstrada na fase atual.

A Comissão aguarda com interesse os pontos de vista do Parlamento Europeu e do Conselho sobre a presente comunicação.