

(Tradução)

**Tratamento de dados pessoais originários da UE pelo Departamento do Tesouro dos Estados Unidos para fins de combate ao terrorismo — «SWIFT»**

(2007/C 166/09)

**Programa de Detecção do Financiamento do Terrorismo — Exposição de Motivos do Departamento do Tesouro dos Estados Unidos**

A presente Exposição de Motivos faz uma descrição do Programa de Detecção do Financiamento do Terrorismo (*Terrorist Finance Tracking Program* — TFTP) do Departamento do Tesouro dos Estados Unidos e, em especial, dos controlos rigorosos e garantias que regem o tratamento, utilização e difusão dos dados recebidos da SWIFT por força de intimações administrativas. Tais controlos e garantias aplicam-se a todas as pessoas com acesso aos dados SWIFT, excepto quando indicado em contrário em exemplos específicos, tais como os que descrevem a partilha de informação indiciária derivada de dados SWIFT com governos estrangeiros.

O TFTP é um programa com fundamento na lei, cuidadosamente orientado, eficaz e com bons resultados, e está sujeito a garantias de privacidade. Representa exactamente aquilo que os cidadãos esperam que os seus governos façam para os proteger de ameaças terroristas.

**O Programa de Detecção do Financiamento do Terrorismo do Departamento do Tesouro**

Pouco depois dos ataques de 11 de Setembro de 2001, o Departamento do Tesouro deu início ao programa TFTP, como parte de um esforço mais amplo para utilizar todos os meios disponíveis com o fim de detectar terroristas e as suas redes. Ao abrigo do programa TFTP, o Departamento do Tesouro emitiu intimações administrativas com o fim de obter dados relacionados com terroristas do centro de operações nos Estados Unidos da Sociedade de Telecomunicações Financeiras Interbancárias Mundiais (*Society for Worldwide Interbank Financial Telecommunication* — SWIFT), uma cooperativa sediada na Bélgica que opera um sistema mundial de mensagens utilizado para transmitir informações sobre transacções financeiras. Essas intimações requerem que a SWIFT forneça ao Departamento do Tesouro certos registos de transacções financeiras — mantidos pelo centro de operações da SWIFT nos Estados Unidos no decurso das suas actividades normais — a fim de serem utilizados exclusivamente para fins de luta anti-terrorismo, tal como é especificado nos capítulos seguintes.

**Princípios fundamentais subjacentes ao TFTP**

Desde o seu início, o programa TFTP foi concebido e implementado de forma a dar cumprimento aos imperativos legais aplicáveis, contribuir de modo significativo para o combate ao terrorismo mundial, bem como respeitar e proteger a natureza comercial potencialmente sensível e a privacidade dos dados SWIFT armazenados nos Estados Unidos. O programa TFTP tem em consideração a natureza comercial potencialmente sensível e a privacidade pessoal da informação que abrange, e as garantias especificadas na presente Exposição de Motivos aplicam-se independentemente da nacionalidade ou local de residência das pessoas em causa. O programa contém vários níveis de controlo governamental e independente, parcialmente sobrepostos, para assegurar que os dados, de natureza limitada, apenas sejam pesquisados para fins de luta anti-terrorismo, mantidos na sua totalidade em ambiente seguro e devidamente tratados.

Todos os actos do Departamento do Tesouro destinados a obter informação específica do centro de operações SWIFT nos Estados Unidos e utilizar essa informação apenas para a investigação, detecção, prevenção e/ou processamento do terrorismo ou do seu financiamento, ou as investigações e acções judiciais subsequentes correlatas, são conformes com a legislação dos Estados Unidos. Além disso, os dados fornecidos pela SWIFT não são pesquisados para recolher provas ou detectar actividades não relacionadas com o terrorismo ou seu financiamento, mesmo que essas actividades sejam por si próprias ilícitas. O Departamento do Tesouro não efectua pesquisas nos dados SWIFT, nem a respectiva informação pode ser utilizada, no âmbito de investigações gerais de evasão fiscal, branqueamento de capitais, espionagem económica, tráfico de estupefacientes ou outras actividades criminosas, a menos que em casos específicos essas actividades estejam relacionadas com o terrorismo e o seu financiamento.

Os dados recebidos da SWIFT por força de intimação consistem em cópias de mensagens de transacções financeiras efectuadas, isto é, cópias electrónicas de registos de transacções mantidos pelo centro de operações SWIFT nos Estados Unidos no decurso das suas actividades normais. Embora tais dados possam sofrer um certo tratamento, no sentido da capacidade muito restrita, a que se refere a presente, de busca e consulta no âmbito da luta anti-terrorismo, não há alteração, manipulação, aditamento ou apagamento de dados em cada uma das mensagens de transacção na base de dados pesquisável.

O programa TFTP demonstrou ser um potente instrumento de investigação, que tem dado um importante contributo para a protecção dos cidadãos dos Estados Unidos e outras pessoas em todo o mundo e para proteger a segurança nacional da América e de outros países. O programa tem sido instrumental para identificar e capturar terroristas e os seus financiadores, e tem sido útil na obtenção de muitos indícios, que foram difundidos a peritos anti-terrorismo de vários serviços de informações e de polícia em todo o mundo.

### **Preocupações surgidas na União Europeia**

Depois de os órgãos de comunicação social terem divulgado publicamente em Junho de 2006 a existência do TFTP, surgiram na UE preocupações acerca do programa TFTP e, em especial, da possibilidade de o Departamento do Tesouro ter acesso a dados pessoais relativos a pessoas singulares identificadas ou identificáveis, contidos nas transacções financeiras tratadas pela SWIFT. Em particular, foram levantadas questões quanto à compatibilidade do TFTP com as obrigações decorrentes da Directiva « Protecção de Dados » (Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados), bem como da legislação dos Estados-Membros que implementa essa directiva.

### **Natureza dos dados SWIFT**

Os registos de transacções financeiras fornecidos pela SWIFT sob intimação podem incluir informação identificadora do ordenante e/ou recipiente da transacção, incluindo o nome, número de conta, endereço, número nacional de identificação e outros dados pessoais. Seria verdadeiramente excepcional que os registos financeiros SWIFT incluíssem dados « sensíveis » como os referidos no artigo 8.º da Directiva 65/46/CE (a saber, dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual).

### **Princípios internacionais de luta contra o financiamento do terrorismo**

Os dados financeiros SWIFT utilizados no programa TFTP são extraordinariamente úteis no combate ao terrorismo mundial e seu financiamento, bem como no cumprimento da responsabilidade governamental de defender a população, preservar a segurança nacional e detectar, prevenir, investigar e processar os crimes terroristas.

A comunidade internacional e as autoridades nacionais reconhecem que o dinheiro constitui o sustento vital do terrorismo. Isso mesmo se reflecte na Convenção Internacional de 1999 das Nações Unidas para a Eliminação do Financiamento do Terrorismo e em numerosas resoluções das Nações Unidas relativas à prevenção e supressão do financiamento de actos terroristas, em especial a Resolução n.º 1373 do Conselho de Segurança das Nações Unidas. Nos Estados Unidos, o Departamento do Tesouro e o Congresso criaram em 2004 o Serviço de Informações Financeiras e do Terrorismo (*Office of Terrorism and Financial Intelligence* — OFAC) para concatenar as funções do Departamento em matéria de execução da lei e de informações, com o duplo objectivo de proteger o sistema financeiro contra usos ilícitos e de combater, nomeadamente, o terrorismo e outras ameaças à segurança nacional. As várias componentes deste Serviço recolhem e analisam informação proveniente dos serviços de polícia e de informações, bem como do sector financeiro, sobre a forma como os terroristas (e outros criminosos) obtêm, transferem e depositam dinheiro. Estas actividades permitem a este Serviço congelar activos de terroristas, combater o terrorismo em geral e desenvolver e promover normas de luta contra o financiamento do terrorismo, tanto nos Estados Unidos como no estrangeiro.

Estas e outras iniciativas reflectem a realidade de todos os dias, ou seja, o facto de os terroristas dependerem de um fluxo regular de dinheiro para pagar os operacionais, organizar deslocações, treinar novos membros, falsificar documentos, pagar subornos, adquirir armas e realizar ataques. Ao enviar dinheiro através do sistema bancário, fornecem muitas vezes dados que produzem o tipo de indícios concretos susceptíveis de fazer avançar investigações sobre o terrorismo. É por esta razão que os profissionais da luta anti-terrorismo dão tanta importância às informações financeiras, incluindo as derivadas de programas como o TFTP, que provou ter um valor inestimável no combate ao terrorismo mundial.

É também por essa razão que o sector financeiro está sujeito a extensos requisitos de registo e informação, destinados a apoiar os esforços governamentais de luta anti-terrorismo. Em todo o mundo, numerosos países adoptaram legislação que a tal obriga, na linha das recomendações do Grupo de Acção Financeira Internacional. Por exemplo, nos Estados Unidos a legislação primária para o efeito é a Lei do Segredo Bancário (*Bank Secrecy Act*). Na Europa, foram adoptadas disposições similares na legislação nacional em transposição da Terceira Directiva sobre Branqueamento de Capitais e, mais recentemente, o Regulamento (CE) n.º 1781/2006 do Parlamento Europeu e do Conselho, de 15 de Novembro de 2006, relativo às informações sobre o ordenante que acompanham as transferências de fundos.

### **Fundamento jurídico para a obtenção e utilização dos dados SWIFT**

As intimações notificadas à SWIFT baseiam-se em legislação existente de longa data e num Decreto Presidencial (*Executive Order*) conexo, relativo à luta contra o terrorismo e o seu financiamento. A Lei sobre os Poderes Económicos em caso de Emergência Internacional (*International Emergency Economic Powers Act — IEEPA*) de 1997 autoriza o Presidente dos Estados Unidos, em caso de emergência nacional declarada, a investigar transferências bancárias e outras transacções em que possa estar envolvida uma pessoa estrangeira. De modo semelhante, a Lei sobre a Participação nas Nações Unidas (*United Nations Participation Act — UNPA*) de 1945 autoriza o Presidente, ao implementar as Resoluções do Conselho de Segurança das Nações Unidas, a investigar as relações económicas ou meios de comunicação entre quaisquer pessoas estrangeiras e os Estados Unidos.

Em 23 de Setembro de 2001, o Presidente, fundamentando-se em parte na IEEPA e na UNPA e fazendo referência às Resoluções do Conselho de Segurança das Nações Unidas relativas aos Talibã e à Al Qaida, promulgou o Decreto Presidencial n.º 13224. Nesse decreto, o Presidente declarou uma emergência nacional para fazer face aos ataques terroristas de 11 de Setembro e à ameaça contínua e imediata de novos ataques, tendo congelado os activos de pessoas que cometem, ameaçam cometer ou apoiam o terrorismo e proibido transacções com essas pessoas.

Para efeitos do Decreto Presidencial n.º 13224, a respectiva secção 3 contém a seguinte definição:

o termo «terrorismo» significa uma actividade que

- i) implica um acto violento ou acto perigoso para a vida humana, bens ou infra-estruturas, e
- ii) se afigura intencional para
  - A) para intimidar ou coagir uma população civil;
  - B) influenciar a política de um governo por intimidação ou coacção, ou
  - C) afectar a conduta de um governo por destruição maciça, assassinio, rapto ou tomada de reféns.

Na secção 7 desse decreto, o Presidente autorizou o Secretário do Departamento do Tesouro a utilizar todos os poderes atribuídos ao Presidente pela IEEPA e pela UNPA que possam ser necessários para cumprir os objectivos do dito decreto. O Presidente autorizou ainda o Secretário do Tesouro a delegar quaisquer destas funções a outros funcionários e agências do Governo dos Estados Unidos, e instruiu todas as agências do Governo dos Estados Unidos a tomar todas as medidas apropriadas no âmbito da sua autoridade para dar cumprimento ao disposto no dito decreto. A IEEPA e o Decreto Presidencial, tal como aplicados através da Regulamentação de Sanções contra o Terrorismo Mundial (*Global Terrorism Sanctions Regulations*), autorizam o Director do Serviço de Controlo dos Activos Estrangeiros (OFAC) do Departamento do Tesouro a requerer que qualquer pessoa forneça dados sobre transacções financeiras ou outros dados, no âmbito de uma investigação económica conducente a sanções. São estes os fundamentos jurídicos ao abrigo dos quais o OFAC notifica intimações à SWIFT para obter dados financeiros relacionados com investigações sobre o terrorismo.

### **Controlo do acesso e segurança do sistema informático**

Em conformidade com os procedimentos do Governo dos Estados Unidos para tratamento da informação relacionada com a investigação do terrorismo e, de uma forma mais geral, do seu financiamento, os dados obtidos da SWIFT estão sujeitos a estritas medidas técnicas e organizativas a fim de proteger a informação contra a destruição, perda, alteração ou acesso, tanto accidentais como ilícitos. Todas as medidas de segurança a seguir indicadas estão sujeitas a auditoria independente.

Os dados SWIFT são mantidos em ambiente físico seguro e armazenados separadamente de outros dados, e os sistemas informáticos estão equipados de controlos de alto nível contra a intrusão e outras protecções para limitar o acesso apenas aos dados descritos na presente. Não são feitas cópias dos dados SWIFT, excepto como reserva para efeitos de recuperação em caso de calamidade. O acesso aos dados e ao equipamento informático é limitado às pessoas com a adequada habilitação de segurança. Mesmo para essas pessoas, o acesso aos dados SWIFT é possível apenas para leitura e é limitado por força do programa TFTP, estritamente com base na necessidade de conhecer, aos analistas dedicados à investigação do terrorismo e às pessoas participantes no apoio técnico, gestão e fiscalização do programa TFTP.

### **Exploração e utilização dos dados apenas para investigação do terrorismo**

O programa TFTP não implica a prospecção de dados, nem qualquer outro tipo de caracterização algorítmica ou automatizada, nem a filtragem informática. O programa TFTP apresenta múltiplos níveis de controlo rigoroso, a fim de limitar o volume de informação recolhida, assegurar que a informação apenas é explorada e utilizada para efeitos de luta anti-terrorismo, e proteger a privacidade das pessoas não relacionadas com o terrorismo ou o seu financiamento. Esta sobreposição de garantias constitui uma restrição contínua e importante do acesso e utilização dos dados financeiros tratados pela SWIFT na sua actividade diária.

Liminarmente, as intimações notificadas à SWIFT são cuidadosa e estritamente orientadas de molde a limitar o volume de dados fornecido ao Departamento do Tesouro. São requeridos da SWIFT apenas os dados que o Departamento do Tesouro entende serem necessários para combater o financiamento do terrorismo, com base em anteriores análises centradas nos tipos de mensagens e sua distribuição geográfica, bem como em ameaças e vulnerabilidades apercebidas. Além disso, as pesquisas são estritamente orientadas de forma a minimizar a exploração de mensagens que não são pertinentes para uma investigação sobre terrorismo. Os dados fornecidos pela SWIFT são objecto de pesquisa apenas para extrair informação relacionada com uma determinada investigação pré-existente sobre terrorismo. Isso significa que toda e qualquer pesquisa efectuada tem de se referir e apoiar em provas documentais que sustentem a suposição de que o alvo está relacionado com o terrorismo e o seu financiamento. Ao mesmo tempo, toda e qualquer pesquisa de dados SWIFT no âmbito do programa TFTP é também objecto de registo cronológico, incluindo o vínculo com o terrorismo necessário para desencadear uma investigação.

Em virtude das garantias atrás referidas, de facto apenas houve acesso a uma parte mínima (isto é, substancialmente menos de 1 %) do conjunto de mensagens SWIFT fornecidas ao Departamento do Tesouro, e apenas porque tais mensagens constituíam uma resposta directa a uma pesquisa focalizada, relacionada com o terrorismo.

### **Fiscalização independente**

Para além dos controlos exercidos em permanência pelo Departamento do Tesouro, descritos na presente, o programa TFTP inclui vários níveis complementares de fiscalização independente: por representantes da própria SWIFT, por uma empresa independente de auditoria e por outras autoridades federais dos Estados Unidos, incluindo o Congresso.

A SWIFT e os seus auditores externos exercem o seu direito de fiscalização independente do programa TFTP de várias formas mutuamente complementares. Em primeiro lugar, certos representantes da SWIFT receberam habilitações de segurança apropriadas para terem acesso 24 horas por dia ao equipamento e aos dados e a capacidade de controlar a utilização dos dados, em tempo real e retrospectivamente, para assegurar que são consultados apenas para fins de luta anti-terrorismo. Acresce que esses representantes da SWIFT podem fazer parar imediatamente qualquer pesquisa específica e têm mesmo a capacidade de fazer parar todo o sistema caso tenham qualquer apreensão.

No que respeita aos auditores externos independentes, a manutenção, acesso e utilização dos dados SWIFT são sujeitos a uma auditoria independente, regular e periódica, em conformidade com protocolos cuidadosamente elaborados e compatíveis com as normas internacionais de auditoria. Estas auditorias abrangem o controlo de acesso e as salvaguardas de segurança do sistema informático, assim como a utilização dos dados limitada à investigação do terrorismo, tal como acima descrito. Os auditores independentes comunicam as suas conclusões ao comité de auditoria e finanças do Conselho de Administração da SWIFT.

Além disso, em conformidade com a legislação dos Estados Unidos, vários Comités do Congresso têm sido informados repetidas vezes acerca do programa TFTP e do seu funcionamento, informação essa que tem continuado a ser prestada com regularidade. O programa TFTP também tem sido objecto de audiências do Congresso.

Finalmente, a Comissão de Controlo da Privacidade e das Liberdades Cívicas (*Privacy and Civil Liberties Oversight Board*), estabelecida pela Lei de Prevenção do Terrorismo e Reforma dos Serviços de Informações (*Intelligence Reform and Terrorism Prevention Act*) de 2004, exerce também uma fiscalização do programa TFTP. Esta Comissão tem por mandato assegurar que as preocupações em matéria de privacidade e liberdades cívicas são devidamente tidas em conta na implementação de toda a legislação, regulamentação e políticas do ramo executivo dos Estados Unidos, relacionadas com os esforços destinados a proteger os Estados Unidos contra o terrorismo. Essa Comissão é ainda responsável por monitorizar as práticas dos departamentos e agências do ramo executivo em matéria de partilha de informação sobre terrorismo, a fim de determinar se são cumpridas as directrizes destinadas a proteger de forma apropriada a privacidade e as liberdades cívicas.

Tal como se refere adiante, esta extensa fiscalização independente funciona a par de controlos restritivos de difusão que também resultam num acesso restrito à informação derivada dos registos financeiros da SWIFT e também servem para proteger os interesses de privacidade.

### Difusão e partilha da informação

A comunidade internacional reconheceu a importância de partilhar a informação sobre o terrorismo. Por exemplo, a RCSNU n.º 1373 exorta todos os Estados a encontrar formas de intensificar e acelerar o intercâmbio de informação operacional sobre o terrorismo e a trocar informações com vista a prevenir o cometimento de actos terroristas. Também a secção 6 do Decreto Presidencial n.º 13224 requer que o Secretário do Tesouro (e outros funcionários) desenvolvam todos os esforços pertinentes de cooperação e coordenação com outros países afim de alcançar os objectivos do dito decreto, incluindo a prevenção e o impedimento de actos terroristas, a recusa de financiamento e de serviços financeiros a terroristas, bem como a partilha de informações sobre as actividades de financiamento em apoio do terrorismo. É neste contexto que deve ser considerada apropriada a partilha da informação derivada dos dados SWIFT com os parceiros nacionais e internacionais. Tal como sucede com todas as outras facetas do programa TFTP, esta partilha de informação é conforme com a legislação dos Estados Unidos e sujeita a uma série de garantias destinadas a proteger os dados SWIFT e a privacidade das pessoas a quem digam respeito.

Os analistas em matéria de luta anti-terrorismo que efectuem as pesquisas TFTP verificam a pertinência de qualquer informação produzida em resposta a uma consulta antes de essa informação ser preparada para difusão através de canais seguros. O Departamento do Tesouro também efectua controlos do emitente para qualquer difusão subsequente da informação, no sentido de que nenhum receptor é autorizado a redifundir a informação sem autorização expressa do Departamento do Tesouro. A este respeito, tal como sucede para qualquer acesso não autorizado aos dados SWIFT, qualquer divulgação não autorizada da informação derivada do programa TFTP pode resultar numa estrita acção disciplinar ou na imposição de sanções cíveis ou penais.

A informação derivada dos dados SWIFT é partilhada sob estrito controlo com outras agências dos Estados Unidos nos sectores da polícia ou das informações, a fim de serem exclusivamente utilizadas para efeitos de investigação, detecção, prevenção e/ou processamento do terrorismo ou do seu financiamento, ou ainda para as investigações e acções judiciais subsequentes e correlatas. Esta partilha é feita ao abrigo da Lei de Segurança Nacional (*National Security Act*), da Lei de Prevenção do Terrorismo e Reforma dos Serviços de Informações de 2004 e de uma série de memorandos de acordo e correspondentes decretos presidenciais. As agências receptoras têm as mesmas obrigações, segundo a legislação dos Estados Unidos, que o Departamento do Tesouro em matéria de protecção da informação derivada do programa TFTP. Importa igualmente notar que a informação derivada do programa TFTP é partilhada com outras agências dos Estados Unidos apenas para efeitos de indícios, o que restringe a sua utilização como prova material em acções judiciais. As agências receptoras utilizam o seu próprio mandato legislativo para prosseguir as suas investigações, incluindo para obter documentação de outras fontes que possa ser posteriormente usada como prova em acções judiciais.

Essas outras agências governamentais partilham ainda a informação indicial derivada dos dados SWIFT com as suas homólogas estrangeiras para as mesmas finalidades, com aprovação caso a caso pelo Departamento do Tesouro, quando tal se justifica por razões de segurança nacional e de execução da lei. Muitos indícios derivados do programa TFTP têm sido partilhados com autoridades estrangeiras, regra geral sem revelar que a fonte foi o programa TFTP.

Quanto à eventual difusão pública dos dados SWIFT, o Departamento do Tesouro trata esses dados como informação classificada, sensível em termos policiais e confidencial em termos comerciais. Por conseguinte, o Departamento do Tesouro não divulga nem tenciona divulgar publicamente tais dados, excepto se a isso for obrigado por lei. A esse respeito, o Departamento do Tesouro assumirá a posição, relativamente a qualquer acção administrativa ou judiciária decorrente de um pedido de dados TFTP feito por terceiros ao abrigo da Lei da Liberdade de Informação (*Freedom of Information Act* — FOIA), de que tais registos estão isentos da divulgação por força da FOIA.

### Recurso

A natureza confinada dos dados em cada uma das mensagens de transacção SWIFT, a forma restrita como certos dados SWIFT podem ser consultados no âmbito do programa TFTP como parte de uma investigação pré-existente sobre terrorismo e os limites à sua difusão como indícios reduzem de forma significativa a pertinência de um mecanismo de recurso no âmbito do próprio programa TFTP. Não obstante, a legislação dos Estados Unidos prevê formas adequadas de recurso contra uma eventual utilização abusiva por parte das autoridades governamentais dos Estados Unidos.

No que respeita ao interesse de uma determinada pessoa singular quanto à utilização dos dados e à sua capacidade de obter recurso contra uma eventual utilização abusiva, há que fazer uma distinção entre os dados pesquisáveis fornecidos pela SWIFT e as mensagens exploradas no âmbito de uma determinada investigação sobre terrorismo, que podem servir de base para uma decisão administrativa ou outra acção governamental. Os dados recebidos da SWIFT por força de intimações do OFAC consistem em cópias de mensagens de transacções financeiras efectuadas, isto é, cópias electrónicas de registos de transacções mantidos pelo centro de operações SWIFT nos Estados Unidos, no decurso das suas actividades normais. Embora tais dados possam sofrer um certo tratamento, no sentido da capacidade muito restrita, a que se refere a presente, de busca e consulta no âmbito da luta anti-terrorismo, não há alteração, manipulação, aditamento ou apagamento de dados em cada uma das mensagens de transacção na base de dados pesquisável.

Por outro lado, importa salientar de novo que a vasta maioria das mensagens de transacção fornecidas pela SWIFT nunca serão vistas mesmo pelos analistas em matéria de luta anti-terrorismo, e portanto não são conhecidas. Em consequência, responder a um pedido de uma pessoa singular, por questão de privacidade, no sentido de saber se existe informação sobre essa pessoa na base de dados, exigiria em quase todos os casos o acesso a dados que nunca seriam consultados no decurso do funcionamento normal do programa TFTP. Tal acesso não seria compatível com o requisito próprio ao TFTP de que cada pesquisa pressupõe uma conexão prévia com o terrorismo. Finalmente, dado que não há alteração, manipulação, apagamento ou aditamento de dados na base de dados pesquisável, não existe fundamento para «rectificar» qualquer informação. Acresce que isso faria alterar os registos de transacções efectuadas requeridos pela intimação do OFAC.

O posterior tratamento dos dados de uma determinada mensagem de transacção só ocorre no caso das relativamente poucas mensagens de transacção exploradas a partir da base de dados pesquisável e que constituem uma resposta directa a uma pesquisa focalizada no terrorismo. Uma vez os dados explorados e sujeitos aos múltiplos controlos que limitam a sua difusão para efeitos de luta anti-terrorismo, o recurso contra uma alegada utilização abusiva pode ser introduzido segundo os adequados procedimentos administrativos e judiciários para os actos governamentais relativos a essa informação difundida.

A possibilidade de recurso pode ser ilustrada pelo seguinte exemplo relativo a um acção administrativa do OFAC no sentido de congelar activos ao abrigo da Regulamentação de Sanções contra o Terrorismo Mundial que implementa o Decreto Presidencial n.º 13224. Uma pessoa pode requerer ao OFAC a revisão administrativa da sua designação especial como terrorista mundial, sendo-lhe dada nesse âmbito a oportunidade de demonstrar que «deixaram de ser aplicáveis as circunstâncias conducentes a essa designação» e de «apresentar argumentos ou provas que, segundo essa pessoa, demonstram que não existe uma base suficiente para essa designação». Uma pessoa especialmente designada como terrorista mundial também pode requerer revisão judicial da decisão de uma agência, ao abrigo das disposições pertinentes da Lei dos Procedimentos Administrativos (*Administrative Procedures Act*). Estas vias administrativas e judiciárias de recurso são aplicáveis a qualquer pessoa que é objecto da decisão governamental, independentemente da sua nacionalidade.

### Período de conservação

O período de conservação da informação para efeitos de luta anti-terrorismo (ou quaisquer outros) varia em função de numerosos factores bem estabelecidos, incluindo requisitos de investigação, legislação restritiva aplicável e prazos legais de reclamação ou acção judiciária. A aplicabilidade e o *modus operandi* destes e de outros factores variam conforme as agências, dependendo da natureza das funções e missões específicas de cada agência. Por conseguinte, os períodos de conservação de certos tipos de informação relacionada com o terrorismo compilados pelas diversas agências depende da natureza da informação e da investigação a que diz respeito.

No quadro do Governo dos Estados Unidos, os prazos de conservação e disponibilidade dos registos das agências são aprovados pela Administração dos Arquivos e Registos Nacionais (*National Archives and Records Administration* — NARA), nos termos de diversa legislação e regulamentação. Para todos os registos não considerados como tendo valor permanente, tem de estar prevista a sua destruição após um determinado período de tempo, com base em princípios administrativos, fiscais e jurídicos explicitados. Os factores tidos em consideração pela NARA ao aprovar os períodos de conservação para os registos de uma agência incluem a legislação restritiva aplicável, os prazos legais de reclamação ou acção judiciária, o potencial de fraude, os riscos de litígio e os direitos substantivos, bem como a legislação ou regulamentação que concede ou restringe um direito específico.

No que respeita ao período de conservação da informação relacionada com o TFTP, mais uma vez há que fazer uma distinção entre os dados requeridos da SWIFT por intimação e os dados explorados que servem de base para uma decisão administrativa ou um acto governamental.

O Departamento do Tesouro diligenciará, com regularidade e pelo menos anualmente, no sentido de identificar e suprimir todos os dados não extraídos que não sejam necessários para os efeitos referidos na presente Exposição de Motivos. Sob reserva dos resultados da análise acima referida e determinada pela necessidade, todos os dados não explorados recebidos da SWIFT pelo Departamento do Tesouro após a data de publicação da presente Exposição de Motivos serão apagados pelo Departamento do Tesouro o mais tardar cinco anos após a sua recepção pelo Departamento do Tesouro. Sob reserva dos resultados da análise acima referida e determinada pela necessidade, todos os outros dados não explorados serão apagados o mais tardar cinco anos após a data de publicação da presente Exposição de Motivos.

Os dados explorados que constituem resposta directa a uma pesquisa focalizada no terrorismo e que foram subordinados aos múltiplos controlos de difusão atrás referidos para efeitos de luta anti-terrorismo ficam sujeitos ao período de conservação aplicável aos dossiers de investigação da autoridade governamental em questão.

Por exemplo, os dados SWIFT explorados no âmbito do programa TFTP poderão ser utilizados na investigação de uma pessoa para efeitos da sua eventual designação ao abrigo da Regulamentação de Sanções contra o Terrorismo Mundial do OFAC. Segundo o calendário de conservação de registos do OFAC, aprovado pela NARA, se for tomada uma decisão administrativa final no sentido de designar uma pessoa (decisão essa que é tornada pública), a informação em que tal decisão se baseou será conservada em permanência como registo escrito da prova que fundamenta a acção da agência. O dossier comprovativo é conservado para efeitos de revisão administrativa ou judicial, no caso de a designação ser contestada, bem como em apoio de posteriores investigações sobre terrorismo. Em contrapartida, se uma investigação for terminada sem haver designação, os dossiers de investigação são destruídos *in loco* o mais tardar um ano após a investigação ter sido terminada.

Finalmente, em coerência com o quadro legislativo dos Estados Unidos acima descrito, o período de conservação para a informação indicial derivada do TFTP que tiver sido difundida rege-se pela regulamentação e prazos da agência ou governo receptores. Por exemplo, qualquer informação derivada que é utilizada numa acção judiciária do Departamento do Tesouro está sujeita aos períodos de conservação aplicáveis pelo Departamento do Tesouro.

### Futura cooperação no domínio da luta anti-terrorismo

O programa TFTP tem sido um instrumento de grande valor na luta contra o terrorismo a nível mundial, inclusive na Europa. O Governo dos Estados Unidos continuará a avaliar judiciosamente se qualquer informação obtida por meio do programa TFTP pode ou não contribuir para a investigação, prevenção, combate ou perseguição judicial do terrorismo ou do seu financiamento num ou mais Estados-Membros da União Europeia e, em todos os caso apropriados, porá essa informação à disposição das autoridades competentes na forma mais expediente.

Como mostra do nosso empenho e parceria na luta contra o terrorismo mundial, será nomeada uma eminente personalidade europeia com a missão de confirmar que o programa é aplicado de forma coerente com a presente Exposição de Motivos, para efeitos de verificar a protecção dos dados pessoais originários da UE. Em especial, essa personalidade eminente fiscalizará a execução dos procedimentos de apagamento dos dados não explorados.

Essa personalidade eminente deverá ter experiência adequada e habilitação de segurança e será nomeada por um período renovável de dois anos pela Comissão Europeia, em consulta com o Departamento do Tesouro. No cumprimento das suas funções, deverá agir com total independência e não solicitar nem aceitar instruções de quem quer que seja. No âmbito da sua nomeação, deverá também abstrair-se de qualquer acção incompatível com as suas funções.

Essa personalidade eminente apresentará anualmente à Comissão Europeia as suas observações e conclusões em relatório escrito. A Comissão, por seu turno, apresentará relatório ao Parlamento Europeu e o Conselho, se for caso disso.

O Departamento do Tesouro disponibilizará a essa personalidade eminente o acesso, a informação e os dados necessários para o exercício das suas funções. A personalidade eminente agirá a todo o momento em cumprimento dos requisitos de segurança e confidencialidade impostos por lei. As modalidades práticas serão acordadas com o Departamento do Tesouro.

O Departamento do Tesouro informará igualmente a União Europeia de quaisquer alterações materiais das garantias contidas na presente Exposição de Motivos e da adopção de qualquer legislação dos Estados Unidos que afecte materialmente o conteúdo da presente Exposição de Motivos.

O Departamento do Tesouro fará publicar a presente Exposição de Motivos no Registo Federal e consente na sua publicação no *Jornal Oficial da União Europeia*.

---