

(Übersetzung)

Verarbeitung personenbezogener Daten aus der EU durch das Finanzministerium der Vereinigten Staaten zu Zwecken der Terrorismusbekämpfung — SWIFT

(2007/C 166/09)

Programm zum Aufspüren der Finanzierung des Terrorismus — Zusicherungen des Finanzministeriums der Vereinigten Staaten

In diesen Zusicherungen werden das Programm des US-Finanzministeriums zum Aufspüren der Finanzierung des Terrorismus (*Terrorist Financing Tracking Program*, TFTP) und insbesondere die strengen Kontrollen und Garantien in Bezug auf den Umgang mit den von SWIFT aufgrund administrativer Beschlagnahmeanordnungen übermittelten Daten und deren Verwendung und Verbreitung dargelegt. Diese Kontrollen und Garantien gelten in Bezug auf alle Personen mit Zugang zu SWIFT-Daten, sofern in spezifischen, beispielhaft angeführten Fällen, wie etwa dem Austausch von wichtigen, aus SWIFT-Daten gewonnenen Informationen mit ausländischen Regierungen, nichts anderes vorgesehen ist.

Das TFTP ist ein auf einer gesetzlichen Grundlage beruhendes, zielgerichtetes schlagkräftiges und erfolgreiches Instrument, das angemessenen Datenschutzgarantien unterliegt. Das TFTP entspricht genau den von den Bürgerinnen und Bürgern an ihre Regierungen gerichteten Erwartungen und Hoffnungen hinsichtlich des Schutzes vor terroristischen Bedrohungen.

Das Programm des Finanzministeriums zum Aufspüren der Finanzierung des Terrorismus

Das TFTP ist vom Finanzministerium kurz nach den Terroranschlägen des 11. September 2001 im Rahmen der Bemühungen, alle verfügbaren Mittel zum Aufspüren von Terroristen und deren Netzwerken aufzubieten, eingerichtet worden. Im Rahmen des TFTP erließ das Finanzministerium administrative Anordnungen auf Herausgabe von Daten, die einen Zusammenhang mit Terrorismus aufweisen, gegen das amerikanische Rechenzentrum (*Operations Center*) der Society for Worldwide Interbank Financial Telecommunication (SWIFT), einer in Belgien ansässigen Genossenschaft, die ein weltweites Nachrichtensystem für die Übermittlung von Informationen über Finanztransaktionen betreibt. Aufgrund dieser Anordnungen muss SWIFT dem Finanzministerium bestimmte Aufzeichnungen über Finanztransaktionen — die vom amerikanischen Rechenzentrum von SWIFT im Rahmen der normalen Geschäftsvorgänge aufbewahrt werden — zur Verfügung stellen; diese werden ausschließlich zu den in den folgenden Abschnitten beschriebenen Zwecken der Terrorismusbekämpfung verwendet.

Dem TFTP zugrunde liegende Grundsätze

Die Ausgestaltung und Umsetzung des TFTP waren von Anfang an darauf angelegt, die geltenden gesetzlichen Anforderungen in den Vereinigten Staaten zu erfüllen, einen wirkungsvollen Beitrag zur Bekämpfung des weltweiten Terrorismus zu leisten und die möglicherweise geschäftlich sensiblen SWIFT-Daten, die in den Vereinigten Staaten gespeichert werden, und damit verbundene Interessen des Schutzes der Privatsphäre zu schützen. Das TFTP trägt dem möglicherweise geschäftlich sensiblen Charakter der Daten und dem individuellen Interesse am Schutz der Privatsphäre in Bezug auf die von ihm erfassten Informationen Rechnung; die in diesen Zusicherungen im Einzelnen beschriebenen Garantien gelten unabhängig von Staatsangehörigkeit oder Wohnort der Betroffenen. Das Programm sieht mehrfach abgestufte staatliche und unabhängige Kontrollen vor, die sicherstellen sollen, dass die der Art nach begrenzten Daten ausschließlich für Zwecke der Terrorismusbekämpfung abgefragt werden und alle Daten in gesicherter Umgebung aufbewahrt und ordnungsgemäß gehandhabt werden.

Sämtliche Maßnahmen des Finanzministeriums zur Erlangung spezifischer Informationen aus dem Rechenzentrum von SWIFT in den USA und zur ausschließlichen Nutzung dieser Informationen für die Zwecke der Ermittlung, Feststellung, Verhütung und/oder Verfolgung des Terrorismus oder der Finanzierung des Terrorismus sowie die damit zusammenhängenden weiterführenden Ermittlungs- und Verfolgungsmaßnahmen stehen mit amerikanischem Recht im Einklang. Außerdem werden die von SWIFT übermittelten Daten nicht zur Erhebung von Beweismitteln oder zur Feststellung von Tätigkeiten ausgewertet, die nicht mit dem Terrorismus oder seiner Finanzierung in Zusammenhang stehen, auch wenn es sich um möglicherweise unrechtmäßige Tätigkeiten handelt. Das Finanzministerium führt keine Abfrage von SWIFT-Daten im Zusammenhang mit allgemeinen Ermittlungen in den Bereichen Steuerhinterziehung, Geldwäsche, Wirtschaftsspionage, illegaler Drogenhandel oder bei sonstigen strafbaren Handlungen durch und kann die Informationen hierzu auch nicht verwenden, es sei denn, in einem konkreten Fall wird ein Bezug zum Terrorismus oder zur Finanzierung des Terrorismus festgestellt.

Die von SWIFT aufgrund von Beschlagnahmeanordnungen übermittelten Daten bestehen aus Kopien von Nachrichten über abgewickelte Finanztransaktionen, d.h. elektronischen Kopien von Geschäftsunterlagen, die im Rechenzentrum von SWIFT in den USA im Rahmen der normalen Geschäftsvorgänge aufbewahrt werden. Zwar erfolgt möglicherweise eine Verarbeitung dieser Daten im Rahmen der hier beschriebenen sehr eingeschränkten Such- und Abfrage-Funktion für Zwecke der Terrorismusbekämpfung, jedoch werden die Daten in den einzelnen Nachrichten über Transaktionen innerhalb der abfragbaren Datenbank weder verändert, bearbeitet, ergänzt noch gelöscht.

Das TFTP hat sich als ein schlagkräftiges Ermittlungsinstrument erwiesen und wesentlich dazu beigetragen, amerikanische Staatsbürger und andere Personen auf der ganzen Welt zu schützen und die nationale Sicherheit der Vereinigten Staaten und anderer Staaten zu garantieren. Durch das Programm war es möglich, Terroristen und deren Geldgeber zu ermitteln und festzunehmen; ferner konnten viele wichtige Informationen gewonnen werden, die an Terrorabwehr-Experten von Nachrichtendiensten und Strafverfolgungsbehörden in der ganzen Welt weitergegeben wurden.

Bedenken innerhalb der Europäischen Union

Nach Offenlegung des TFTP durch die öffentlichen Medien im Juni 2006 wurden in der EU Bedenken gegen das Programm und insbesondere in Bezug darauf vorgebracht, dass das Finanzministerium möglicherweise Zugang zu personenbezogenen Daten über bestimmte oder bestimmbar natürliche Personen in den von SWIFT verarbeiteten Finanztransaktionen erhalten könne. Insbesondere wurde die Frage aufgeworfen, ob das TFTP mit den Verpflichtungen nach der Datenschutzrichtlinie (Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr) sowie mit den von den Mitgliedstaaten in Umsetzung der Richtlinie erlassenen Rechtsvorschriften in Einklang steht.

Art der SWIFT-Daten

Die von SWIFT aufgrund von Beschlagnahmeanordnungen zur Verfügung gestellten Daten über Finanztransaktionen können Informationen zur Identifizierung des Auftraggebers und/oder des Empfängers einer Zahlung, einschließlich Name, Kontonummer, Anschrift, nationaler Identifikationsnummer und sonstiger personenbezogener Daten enthalten. Es ist äußerst unwahrscheinlich, dass SWIFT-Finanzunterlagen „sensible“ Daten im Sinne des Artikels 8 der Richtlinie 95/46/EG (d.h. personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben) enthalten.

Internationale Grundsätze für die Bekämpfung der Finanzierung des Terrorismus

Die im Rahmen des TFTP genutzten Finanzdaten von SWIFT erweisen sich als außerordentlich wertvoll bei der Bekämpfung des weltweiten Terrorismus und seiner Finanzierung sowie bei der Wahrnehmung der staatlichen Aufgabe, die Allgemeinheit zu schützen, die nationale Sicherheit zu garantieren und terroristische Straftaten festzustellen, zu verhüten, zu ermitteln und zu verfolgen.

Die internationale Gemeinschaft und die nationalen Behörden sind sich bewusst, dass Geld eine absolute Notwendigkeit für den Terrorismus darstellt. Dies spiegelt sich in dem Internationalen Übereinkommen der Vereinten Nationen von 1999 zur Bekämpfung der Finanzierung des Terrorismus und in den zahlreichen Resolutionen der Vereinten Nationen zur Verhütung und Bekämpfung der Finanzierung terroristischer Handlungen, insbesondere der Resolution 1373 des Sicherheitsrats der Vereinten Nationen. In den Vereinigten Staaten richteten das Finanzministerium und der Kongress im Jahre 2004 das Amt für Terrorismus- und Finanzinformationen (*Office of Terrorism and Financial Intelligence*) ein, das die dem Ministerium obliegenden Aufgaben der Gesetzesdurchsetzung und Erkenntnisgewinnung ausführt und dabei zwei Ziele verfolgt, nämlich das Finanzsystem vor einer Nutzung zu unrechtmäßigen Zwecken zu schützen und gegen unter anderem Terroristen und andere Bedrohungen der nationalen Sicherheit vorzugehen. Die einzelnen Abteilungen des Amtes sammeln und analysieren Informationen aus Strafverfolgungsbehörden, Nachrichtendiensten und der Finanzwelt über die Geldbeschaffung, den Geldverkehr und die Geldaufbewahrung durch Terroristen (und andere Straftäter). Dadurch wird es dem Amt möglich, Vermögenswerte von Terroristen einzufrieren, den Terrorismus allgemein zu bekämpfen und Standards für die Bekämpfung der Finanzierung des Terrorismus in den Vereinigten Staaten und im Ausland zu entwickeln und zu fördern.

Diese und andere Initiativen spiegeln die Tatsache wider, dass Terroristen auf regelmäßige Geldströme angewiesen sind, um Helfer zu bezahlen, Reisevorkerkungen zu treffen, neue Mitglieder auszubilden, Dokumente zu fälschen, Bestechungsgelder zu zahlen, Waffen zu erwerben und Anschläge auszuführen. Im Rahmen der von ihnen getätigten Geldüberweisungen über das Bankensystem fallen oft Informationen an, die zu den Arten von konkreten Hinweisen führen, die eine Terrorismusermittlung voranbringen können. Finanzinformationen, auch solche, die im Rahmen von Programmen wie dem TFTP gewonnen werden, werden daher von für die Terrorismusbekämpfung zuständigen Beamten für äußerst wichtig gehalten; sie haben sich bei der Bekämpfung des weltweiten Terrorismus als von unschätzbarem Wert erwiesen.

Aus diesem Grund ist das Finanzgewerbe auch umfassenden Anforderungen in Bezug auf die Aktenführung und das Berichtswesen unterworfen; damit sollen die staatlichen Anstrengungen zur Bekämpfung des Terrorismus unterstützt werden. Im Einklang mit den Empfehlungen der Financial Action Task Force haben Staaten in der ganzen Welt entsprechende gesetzliche Vorschriften erlassen. In den Vereinigten Staaten beispielsweise ist das Gesetz über das Bankgeheimnis (*Bank Secrecy Act*) die vorrangige rechtliche Grundlage. Ähnliche Bestimmungen wurden in Europa gemäß der Dritten Geldwäscherichtlinie in nationales Recht umgesetzt und erst unlängst mit der Verordnung (EG) Nr. 1781/2006 des Europäischen Parlaments und des Rates vom 15. November 2006 über die Übermittlung von Angaben zum Auftraggeber bei Geldtransfers erlassen.

Gesetzliche Grundlage für die Erlangung und Nutzung von SWIFT-Daten

Die gegen SWIFT erlassenen Beschlagnahmeanordnungen beruhen auf seit langem in Kraft befindlichen Gesetzen und einem damit in Zusammenhang stehenden Exekutiverlass (*Executive Order*) zur Bekämpfung des Terrorismus und der Finanzierung des Terrorismus. Das Gesetz über wirtschaftliche Befugnisse bei einer internationalen Notlage (*International Emergency Economic Powers Act, IEEPA*) von 1977 ermächtigt den Präsidenten der Vereinigten Staaten, bei einem festgestellten nationalen Notstand Ermittlungen in Bezug auf Banküberweisungen und andere Transaktionen durchzuführen, an denen Ausländer ein Interesse haben. Desgleichen ermächtigt das Gesetz über die Teilnahme an den Vereinten Nationen (*United Nations Participation Act, UNPA*) von 1945 den Präsidenten, bei der Umsetzung von Resolutionen des Sicherheitsrats der Vereinten Nationen Ermittlungen in Bezug auf die Wirtschaftsbeziehungen oder die Kommunikationsmittel zwischen Ausländern und den Vereinigten Staaten zu führen.

Am 23. September 2001 erließ der Präsident den Exekutiverlass (*Executive Order*) 13224, wobei er sich zum Teil auf das IEEPA und das UNPA sowie auf die auf die Taliban und Al Qaida abhebenden Resolutionen des Sicherheitsrats der Vereinten Nationen stützte. Darin stellte der Präsident fest, dass ein nationaler Notstand in Bezug auf die Bewältigung der Terroranschläge vom 9.11. vorliegt und dass eine fortwährende und unmittelbare Bedrohung durch weitere Anschläge gegeben ist; er ordnete die Einfrierung der Vermögenswerte von Personen, die terroristische Handlungen begehen, zu begehen drohen oder diese unterstützen, an und untersagte Transaktionen mit solchen Personen.

In Artikel 3 des Exekutiverlasses 13224 ist für die Zwecke dieses Erlasses folgende Definition vorgesehen:

der Ausdruck „Terrorismus“ bezeichnet Aktivitäten, die

- i) gewalttätige Handlungen oder Handlungen, die Menschenleben, Vermögenswerte oder Infrastrukturen gefährden, umfassen und
- ii) offenbar darauf ausgerichtet sind,
 - A. die Zivilbevölkerung einzuschüchtern oder zu nötigen,
 - B. die Maßnahmen einer Regierung durch Einschüchterung oder Nötigung zu beeinflussen, oder
 - C. die Regierungsgeschäfte durch massenhafte Zerstörung, Ermordung, Entführung oder Geiselnahme zu beeinträchtigen.

In Artikel 7 des Erlasses ermächtigte der Präsident den Finanzminister, soweit erforderlich alle dem Präsidenten durch das IEEPA und das UNPA verliehenen Befugnisse zur Verwirklichung der Ziele des Erlasses zu nutzen. Er ermächtigte den Finanzminister ferner, die betreffenden Aufgaben an andere Beamte oder Stellen der amerikanischen Regierung weiter zu delegieren, und wies alle Stellen der amerikanischen Regierung an, in ihrem Zuständigkeitsbereich alle geeigneten Maßnahmen zur Ausführung der Bestimmungen des Erlasses zu treffen. Das IEEPA und der Erlass, die im Wege der Regelungen über Sanktionen gegen den weltweiten Terrorismus (*Global Terrorism Sanctions Regulations*) umgesetzt werden, ermächtigen den Direktor des Amtes zur Kontrolle ausländischer Vermögenswerte (*Office of Foreign Assets Control, OFAC*) des Finanzministeriums, von jedermann zu verlangen, Daten über Finanztransaktionen oder andere Daten im Rahmen einer Ermittlung zu Wirtschaftssanktionen zur Verfügung zu stellen. Auf diese Rechtsgrundlagen stützte sich das OFAC, als es die Zwangsmaßnahmen gegen SWIFT zur Herausgabe von Finanzdaten, die Ermittlungen zum Terrorismus betreffen, erlassen hat.

Zugangskontrolle und Sicherheit des Computersystems

Für die von SWIFT übermittelten Daten gelten gemäß den Verfahren der amerikanischen Regierung für den Umgang mit Informationen, die Ermittlungen zum Terrorismus und zur Finanzierung des Terrorismus betreffen, strenge technische und organisatorische Maßnahmen, mit denen die Daten vor zufälliger oder unrechtmäßiger Vernichtung, zufälligem oder unrechtmäßigem Verlust, zufälliger oder unrechtmäßiger Veränderung oder zufälligem oder unrechtmäßigem Zugang geschützt werden sollen. Alle der nachstehend beschriebenen Sicherheitsmaßnahmen unterliegen einer Kontrolle durch unabhängige Prüfer.

Die SWIFT-Daten werden in einer sicheren physischen Umgebung aufbewahrt und getrennt von anderen Daten gespeichert; die Computersysteme verfügen über ausgefeilte Schutzvorkehrungen gegen unbefugtes Eindringen und andere Schutzvorrichtungen, mit denen der Datenzugriff auf die hier beschriebenen Zwecke beschränkt wird. Es werden keine Kopien von SWIFT-Daten angefertigt, außer für ein Back-up für den Fall eines Zusammenbruches des Systems. Zugriff auf die Daten und die Hardwarekomponenten haben nur Personen mit einer entsprechenden Ermächtigung zum Zugang zu Verschlusssachen. Selbst diese Personen haben nur einen Lesezugriff auf die SWIFT-Daten; über das TFTP ist der Zugang strikt nach dem Prinzip „Kenntnis nur, wenn nötig“ (Need-to-know-Prinzip) auf Analytiker, die Ermittlungen zum Terrorismus durchführen, und auf Personen, die mit der technischen Unterstützung, Verwaltung und Beaufsichtigung des TFTP befasst sind, beschränkt.

Extraktion und Nutzung nur für Ermittlungen zum Terrorismus

Das TFTP umfasst kein Data Mining oder andere Arten der algorithmisierten oder automatisierten Profilerstellung oder des elektronischen Filterns. Mehrfach abgestufte strenge Kontrollen sind in das TFTP eingebaut worden, um die erhobenen Informationen zu begrenzen, um sicherzustellen, dass Informationen nur zu Zwecken der Terrorismusbekämpfung extrahiert und genutzt werden, und um die Interessen von Personen, die keine Verbindung zum Terrorismus oder zur Finanzierung des Terrorismus haben, in Bezug auf den Schutz ihrer Privatsphäre zu schützen. Durch diese ineinander greifenden Sicherheitsvorkehrungen wird der Zugang zu den von SWIFT im alltäglichen Geschäftsbetrieb bearbeiteten Finanzdaten und die Nutzung dieser Daten beständig eingegrenzt und erheblich beschränkt.

Zunächst ist festzuhalten, dass der Gegenstand der gegen SWIFT erlassenen Anordnungen so sorgfältig und so eng eingegrenzt ist, dass dem Finanzministerium möglichst wenige Daten übermittelt werden müssen. SWIFT muss nur solche Daten zur Verfügung stellen, die aufgrund von vorher durchgeführten Analysen, die sich hauptsächlich auf Nachrichtenarten und deren geographische Herkunft konzentrieren, sowie aufgrund von festgestellten Bedrohungen und Schwachstellen nach Auffassung des Finanzministeriums für die Bekämpfung der Terrorismusfinanzierung unbedingt erforderlich sind. Außerdem werden die Suchabfragen so zielgerichtet vorgenommen, dass die Extraktion von Nachrichten ohne Belang für eine Ermittlung zum Terrorismus auf ein Mindestmaß beschränkt wird. Die von SWIFT zur Verfügung gestellten Daten werden so abgefragt, dass nur Informationen extrahiert werden, die mit einer bestimmten, schon vorher eingeleiteten Ermittlung zum Terrorismus in Zusammenhang stehen. Dies bedeutet, dass bei der Durchführung einer Suchabfrage belegte Beweise, die die Annahme stützen, dass die Zielperson mit Terrorismus oder der Finanzierung des Terrorismus in Verbindung steht, speziell angeführt und vermerkt werden müssen. Jede einzelne Abfrage von SWIFT-Daten im Rahmen des TFTP wird ferner gleichzeitig protokolliert; dies gilt auch für einen nachgewiesenen Bezug zum Terrorismus, der erforderlich ist, um eine Suchabfrage einzuleiten.

Aufgrund der vorstehend beschriebenen Garantien ist letztlich nur auf einen Bruchteil (d.h. im Wesentlichen weniger als ein Prozent) der Teilmenge von SWIFT-Nachrichten, die an das Finanzministerium übermittelt wurden, tatsächlich zugegriffen worden, und zwar ausschließlich deshalb, weil die betreffenden Nachrichten im Rahmen einer gezielten, terrorismusbezogenen Suchabfrage direkt ermittelt wurden.

Unabhängige Aufsicht

Zusätzlich zu den hier beschriebenen vom Finanzministerium laufend durchgeführten Kontrollen sieht das TFTP ergänzend eine mehrfach abgestufte unabhängige Aufsicht vor: durch eigene Vertreter von SWIFT, eine unabhängige Wirtschaftsprüfungsgesellschaft und sonstige unabhängige staatliche Stellen der Vereinigten Staaten, einschließlich des amerikanischen Kongresses.

SWIFT und die von ihr gewählten externen Prüfer nehmen eine unabhängige Aufsicht über das TFTP in unterschiedlichen, einander ergänzenden Weisen wahr. Erstens erhielten einige Vertreter von SWIFT geeignete Ermächtigungen für den Zugang zu Verschlusssachen, die ihnen rund um die Uhr Zugang zu der Hardware und den Daten ermöglichen und sie in die Lage versetzen, die Nutzung der Daten in Echtzeit und nachträglich zu überprüfen, um sicherzustellen, dass ein Datenzugriff nur für Zwecke der Terrorismusbekämpfung erfolgt. Außerdem können die betreffenden Vertreter von SWIFT die sofortige Beendigung einer spezifischen Suchabfrage veranlassen; ferner können sie die Abschaltung des gesamten Systems erwirken, wenn ihrerseits Bedenken bestehen.

Was die Kontrolle durch unabhängige externe Prüfer anbelangt, so werden die Aufbewahrung der SWIFT-Daten sowie der Zugang zu diesen und deren Nutzung einer ständigen, regelmäßig durchgeführten unabhängigen Prüfung unterzogen, die gemäß sorgfältig abgefassten Protokollen erfolgt, die im Einklang mit internationalen Prüfungsstandards stehen. Die Prüfungen erstrecken sich auf die Zugangskontrolle und die Vorkehrungen in Bezug auf die Sicherheit des Computersystems sowie darauf, dass die Daten nur für Ermittlungen zum Terrorismus genutzt werden dürfen, wie es vorstehend beschrieben wurde. Die unabhängigen Prüfer übermitteln ihre Schlussfolgerungen dem Prüf- und Finanzausschuss des Verwaltungsrats von SWIFT.

Außerdem sind im Einklang mit amerikanischem Recht mehrere Kongress-Ausschüsse wiederholt über das TFTP und dessen Durchführung unterrichtet worden und werden auch weiterhin regelmäßig darüber unterrichtet. Das TFTP war auch Gegenstand von Anhörungen im Kongress.

Schließlich ist festzuhalten, dass die Stelle zur Überwachung des Schutzes der Privatsphäre und der bürgerlichen Freiheiten (*Privacy and Civil Liberties Oversight Board*), die aufgrund des Gesetzes zur Reform der Nachrichtendienste und zur Terrorismusprävention (*Intelligence Reform and Terrorism Prevention Act*) von 2004 eingesetzt worden ist, die Durchführung des TFTP beaufsichtigt. Die Stelle hat die Aufgabe, sicherzustellen, dass Belange des Schutzes der Privatsphäre und der bürgerlichen Freiheiten bei der Umsetzung aller amerikanischen Gesetze, Verordnungen und Maßnahmen der Exekutive im Zusammenhang mit den Anstrengungen zur Terrorabwehr in den Vereinigten Staaten angemessen berücksichtigt werden. Ferner ist die Stelle dafür zuständig, die Praxis des Austauschs von Informationen über Terrorismus zwischen den Ministerien und den Stellen der Exekutive daraufhin zu überprüfen, ob die Leitlinien für einen angemessenen Schutz der Privatsphäre und der bürgerlichen Freiheiten eingehalten werden.

Wie nachstehend beschrieben, werden parallel zu dieser umfassenden, unabhängigen Aufsicht restriktive Kontrollen in Bezug auf die Verbreitung durchgeführt, mit denen der Zugang zu den aus den Finanzunterlagen von SWIFT gewonnenen Informationen weiter eingeschränkt und Interessen des Schutzes der Privatsphäre weiter geschützt werden sollen.

Verbreitung und Austausch von Informationen

Die internationale Gemeinschaft hat anerkannt, dass dem Austausch von Informationen über Terrorismus ganz entscheidende Bedeutung zukommt. In der Resolution 1373 des VN-Sicherheitsrats beispielsweise werden alle Staaten aufgefordert, Wege zur Intensivierung und Beschleunigung des Austauschs operativer Informationen über Terrorismus zu finden und Informationen auszutauschen, um die Begehung terroristischer Handlungen zu verhüten. Desgleichen ist in Artikel 6 des Exekutiverlasses (*Executive Order*) 13224 vorgesehen, dass der Finanzminister (und sonstige Beamte) alle geeigneten Anstrengungen zur Zusammenarbeit und Abstimmung mit anderen Staaten unternehmen müssen, damit die Ziele des Erlasses erreicht werden können; dazu gehören auch die Verhütung und Verfolgung von terroristischen Handlungen, die Unterbindung von Finanzierungen und Finanzdienstleistungen für Terroristen und der Austausch von Erkenntnissen über Finanzierungsaktivitäten zur Unterstützung des Terrorismus. Vor diesem Hintergrund werden denn auch die aus den SWIFT-Daten gewonnenen Informationen in angemessener Weise mit inländischen und internationalen Partnern ausgetauscht. Wie es für alle anderen Aspekte des TFTP zutrifft, so erfolgt auch dieser Informationsaustausch im Einklang mit amerikanischem Recht und unterliegt verschiedenen Sicherheitsvorkehrungen, mit denen die SWIFT-Daten und die Interessen des Schutzes der Privatsphäre von Personen, auf die sich diese Daten gegebenenfalls beziehen, geschützt werden sollen.

Die im Bereich der Terrorismusbekämpfung eingesetzten Analytiker, die Suchabfragen im Rahmen des TFTP durchführen, überprüfen die so gewonnenen Informationen auf ihre Relevanz hin, bevor sie im Hinblick auf ihre Weitergabe über gesicherte Kanäle aufbereitet werden. Das Finanzministerium unterwirft ferner alle späteren Übermittlungen dem Grundsatz der Kontrolle durch den Urheber; dies bedeutet, dass die Informationen vom Empfänger nicht ohne die ausdrückliche Zustimmung des Finanzministeriums weitergegeben dürfen. Diesbezüglich gilt, dass — wie auch bei jedem anderen unbefugten Zugang zu SWIFT-Daten — eine nicht genehmigte Offenlegung von im Rahmen des TFTP gewonnenen Informationen zur Folge haben kann, dass strenge Disziplinarmaßnahmen oder zivilrechtliche bzw. strafrechtliche Sanktionen verhängt werden.

Die aus SWIFT-Daten gewonnenen Informationen werden unter Einhaltung strenger Kontrollen mit anderen amerikanischen Stellen im Bereich der nachrichtendienstlichen Erkenntnisgewinnung und der Strafverfolgung ausgetauscht und ausschließlich zum Zwecke der Ermittlung, Feststellung, Verhütung und/oder Verfolgung des Terrorismus oder der Finanzierung des Terrorismus bzw. für damit zusammenhängende weitergehende Ermittlungen oder Verfolgungen genutzt. Dieser Informationsaustausch ist nach dem Gesetz über die nationale Sicherheit (*National Security Act*), dem Gesetz zur Reform der Nachrichtendienste und zur Terrorismusprävention (*Intelligence Reform and Terrorism Prevention Act*) von 2004 sowie nach verschiedenen Vereinbarungen (*Memoranda of Understanding*) und den zugehörigen Exekutiverlassen (*Executive Orders*) vorgeschrieben. Die empfangenden Stellen sind nach amerikanischem Recht genauso wie das Finanzministerium zum Schutz der im Rahmen des TFTP gewonnenen Informationen verpflichtet. Wichtig ist ferner der Hinweis, dass diese Informationen nur zu wichtigen Zwecken mit anderen amerikanischen Stellen ausgetauscht werden, so dass die Informationen nur in begrenztem Umfang als Beweismittel in Gerichtsverfahren Verwendung finden. Die empfangenden Stellen stützen sich auf die für sie jeweils geltenden gesetzlichen Grundlagen, um eigene Ermittlungen durchzuführen, unter anderem auch hinsichtlich der Erlangung von Unterlagen aus anderen Quellen, die später als Beweismittel vor Gericht verwendet werden könnten.

Diese anderen staatlichen Stellen tauschen ferner wichtige, aus SWIFT-Daten gewonnene Informationen mit den entsprechenden Stellen im Ausland zu denselben Zwecken aus; das Finanzministerium muss hierzu von Fall zu Fall seine Genehmigung erteilen, wenn dies aus Gründen der nationalen Sicherheit oder im Interesse der Strafverfolgung gerechtfertigt ist. Viele wichtige Informationen, die im Rahmen des TFTP gewonnen wurden, wurden mit ausländischen Behörden ausgetauscht, ohne dass dabei generell das TFTP als Quelle angegeben wurde.

Was die etwaige öffentliche Verbreitung von SWIFT-Daten anbelangt, so ist festzuhalten, dass diese Daten vom Finanzministerium als geheimhaltungsbedürftige, sicherheitsempfindliche und strafverfolgungsrelevante vertrauliche Geschäftsinformationen behandelt werden. Die Daten werden daher vom Finanzministerium nicht öffentlich zugänglich gemacht und auch in Zukunft nicht öffentlich zugänglich gemacht werden, es sei denn, das Ministerium ist hierzu gesetzlich verpflichtet. Diesbezüglich wird das Finanzministerium im Rahmen von Verwaltungs- oder Gerichtsverfahren im Zusammenhang mit Anträgen von Dritten nach dem Gesetz über die Informationsfreiheit (*Freedom of Information Act, FOIA*), in denen die Herausgabe von TFTP-Daten verlangt wird, den Standpunkt vertreten, dass diese Daten von der Offenlegung nach dem FOIA ausgenommen sind.

Rechtsschutz

Aufgrund dessen, dass die in individuellen Zahlungsverkehrsnachrichten von SWIFT enthaltenen Daten von der Art her begrenzt sind, nur ein beschränkter Zugang zu bestimmten SWIFT-Daten über das TFTP im Rahmen einer bereits laufenden Ermittlung zum Terrorismus besteht und einer Verbreitung als wichtige Information enge Grenzen gezogen sind, kann praktisch weitgehend auf einen Rechtsschutzmechanismus im TFTP selbst verzichtet werden. Hiervon abgesehen stehen im amerikanischen Recht geeignete Rechtsbehelfe gegen einen möglichen Missbrauch durch staatliche Stellen zur Verfügung.

Hinsichtlich des Interesses von betroffenen natürlichen Personen in Bezug auf die Verwendung von Daten und die Möglichkeit zur Einlegung eines Rechtsbehelfs wegen etwaigen Datenmissbrauchs ist zu unterscheiden zwischen den von SWIFT übermittelten abrufbaren Daten und den im Rahmen einer gezielten Ermittlung zum Terrorismus extrahierten Nachrichten, die als Grundlage für eine Verwaltungsentscheidung oder eine sonstige staatliche Maßnahme dienen können. Die von SWIFT aufgrund von Beschlagnahmeanordnungen des OFAC übermittelten Daten bestehen aus Kopien von Nachrichten über abgewickelte Finanztransaktionen, d.h. elektronischen Kopien von Geschäftsunterlagen, die im Rechenzentrum von SWIFT in den USA im Rahmen der normalen Geschäftsvorgänge aufbewahrt werden. Zwar ist eine Verarbeitung dieser Daten im Sinne der hier beschriebenen sehr eingeschränkten Möglichkeit der Informationssuche und -gewinnung im Rahmen der Terrorismusbekämpfung in bestimmtem Maße möglich, jedoch werden die in der abrufbaren Datenbank in den einzelnen Zahlungsverkehrsnachrichten enthaltenen Daten dabei nicht verändert, bearbeitet, ergänzt oder gelöscht.

Außerdem ist es auch hier wichtig hervorzuheben, dass die überwiegende Mehrzahl der von SWIFT zur Verfügung gestellten Zahlungsverkehrsnachrichten nie — auch nicht von Analytikern im Bereich Terrorismusbekämpfung — eingesehen und somit nicht bekannt wird. Folglich müsste bei der Beantwortung der Anfrage einer ihr Auskunftsrecht geltend machenden natürlichen Person, ob diese Person betreffende Daten in der Datenbank enthalten sind, in fast allen Fällen auf Daten zugegriffen werden, auf die im Rahmen der normalen Durchführung des TFTP nie ein Zugriff erfolgt. Ein derartiger Zugriff stünde nicht mit der Anforderung des TFTP im Einklang, dass bei jeder Abfrage ein vorher bestehender Bezug zum Terrorismus gegeben sein muss. Da die in der abfragbaren Datenbank enthaltenen Daten weder verändert, bearbeitet, gelöscht noch ergänzt werden, erübrigt sich schließlich auch eine „Berichtigung“ von Informationen. Außerdem würden dadurch die Daten über abgewickelte Geschäfte verändert, die in den Beschlagnahmeanordnungen des OFAC angefordert werden.

Eine Weiterverarbeitung der in individuellen Zahlungsverkehrsnachrichten enthaltenen Daten wird nur bei relativ wenigen, im Rahmen einer gezielten Abfrage zum Terrorismus direkt ermittelten Nachrichten erfolgen, die aus der abfragbaren Datenbank extrahiert werden. Erst nach der Extraktion der Daten und vorbehaltlich der Durchführung der mehrfachen Kontrollen, die einer Verbreitung zu Zwecken der Terrorismusbekämpfung Grenzen setzen, könnte bezüglich der von der Regierung auf die Verbreitung der Informationen hin eingeleiteten Maßnahmen entsprechend den geeigneten verwaltungsrechtlichen oder gerichtlichen Verfahren ein ordentlicher Rechtsbehelf wegen angeblichen Missbrauchs eingelegt werden.

Die Möglichkeit zur Einlegung eines Rechtsbehelfs lässt sich am Beispiel einer vom OFAC getroffenen Verwaltungsmaßnahme zum Einfrieren von Vermögenswerten nach den Regelungen für Sanktionen gegen den weltweiten Terrorismus (*Global Terrorism Sanctions Regulations*), mit denen der Exekutiverlass (*Executive Order*) 13224 umgesetzt wird, verdeutlichen. Eine Person kann das OFAC um Überprüfung einer von ihm getroffenen Entscheidung ersuchen, mit der sie auf die Liste der weltweit agierenden Terroristen gesetzt wurde; damit erhält diese Person die Möglichkeit, nachzuweisen, dass „die Umstände, die zu der Aufnahme in die Liste führten, nicht mehr gelten“, und „Argumente vorzubringen oder Beweismittel vorzulegen, die ihrer Ansicht nach belegen, dass die Einstufung als Terrorist auf einer nicht ausreichenden Grundlage“ erfolgte. Eine in der Liste weltweit agierender Terroristen namentlich aufgeführte Person kann ferner die entsprechende behördliche Entscheidung vor Gericht nach den einschlägigen Bestimmungen des Verwaltungsverfahrensgesetzes (*Administrative Procedure Act*) anfechten. Diese Möglichkeit, behördlichen oder gerichtlichen Rechtsschutz zu begehren, steht unabhängig von ihrer Staatsangehörigkeit allen Personen offen, gegen die staatliche Entscheidungen erlassen wurden.

Speicherfrist

Die Dauer des Zeitraums für die Aufbewahrung von Informationen für die Terrorismusbekämpfung (und für andere Zwecke) richtet sich nach zahlreichen, allgemein anerkannten Kriterien, wozu unter anderem Ermittlungserfordernisse, anwendbare Verjährungsfristen und gesetzliche Fristen für die Geltendmachung von Ansprüchen und für die Einleitung von Strafverfolgungsmaßnahmen gehören. Ob diese und andere Kriterien anwendbar sind und greifen, ist von Stelle zu Stelle unterschiedlich und hängt von der Art der spezifischen Aufgaben und Missionen der jeweiligen Stelle ab. Daher bestimmen sich die Fristen für die Aufbewahrung bestimmter Arten von terrorismusbezogenen Informationen, die von den verschiedenen Stellen zusammengetragen werden, nach dem Wesen der Informationen und der Ermittlung, auf die diese sich beziehen.

Innerhalb der US-amerikanischen Verwaltung werden die Regelungen für die Aufbewahrung und Vernichtung behördlicher Unterlagen werden durch die Verwaltung der nationalen Archive und Unterlagen (*National Archives and Records Administration, NARA*) nach Maßgabe verschiedener Gesetze und Verordnungen gebilligt. Alle Unterlagen ohne dauerhaften Wert müssen nach einer bestimmten Frist vernichtet werden; dabei finden administrative, fiskalische und gesetzliche Gesichtspunkte Berücksichtigung. Zu den Kriterien, die von der NARA bei der Billigung von Fristen für die Aufbewahrung von Unterlagen einer Stelle berücksichtigt werden, gehören die geltenden Verjährungsfristen, die gesetzlichen Fristen für die Geltendmachung von Ansprüchen oder für die Einleitung von Strafverfolgungsmaßnahmen, die Möglichkeit von Betrug, die Gefahr von Streitigkeiten, materielle Rechte sowie Gesetze oder Verordnungen, mit denen ein bestimmtes, gesetzlich verankertes Recht gewährt oder eingeschränkt wird.

Was den Zeitraum für die Aufbewahrung von Informationen im Zusammenhang mit dem TFTP anbelangt, so ist auch hier zu unterscheiden zwischen den von SWIFT aufgrund der Beschlagnahmeanordnungen übermittelten Daten und den extrahierten Daten, die als Grundlage für eine Verwaltungsentscheidung oder Maßnahmen der Regierung dienen.

Das Finanzministerium wird beständig, mindestens aber einmal jährlich alle nicht-extrahierten Daten, die für den Vollzug der in diesen Zusicherungen genannten Zwecke nicht notwendig sind, ermitteln und löschen. Vorbehaltlich der Ergebnisse der vorerwähnten Notwendigkeitsanalyse werden alle nicht-extrahierten Daten, die dem Finanzministerium nach dem Datum der Veröffentlichung dieser Zusicherungen von SWIFT übermittelt werden, spätestens fünf Jahre nach Erhalt vom Finanzministerium gelöscht. Vorbehaltlich der Ergebnisse der vorerwähnten Notwendigkeitsanalyse werden alle sonstigen nicht-extrahierten Daten spätestens fünf Jahre nach dem Datum der Veröffentlichung dieser Zusicherungen gelöscht.

Die bei einer gezielten terrorismusbezogenen Abfrage direkt ermittelten und extrahierten Daten, die den weiter oben beschriebenen mehrfachen Kontrollen in Bezug auf die Verbreitung für Zwecke der Terrorismusbekämpfung unterworfen wurden, unterliegen der Speicherfrist, die in der betreffenden staatlichen Stelle für deren Ermittlungsakten gilt.

Beispielsweise könnten im Rahmen des TFTP extrahierte SWIFT-Daten bei Ermittlungen gegen eine Einzelperson im Hinblick auf deren etwaige Aufnahme in die Liste von Terroristen nach den Regelungen für Sanktionen gegen den weltweiten Terrorismus (*Global Terrorism Sanctions Regulations*) der OFAC verwendet werden. Gemäß den von der NARA gebilligten Vorschriften der OFAC für die Aufbewahrung von Unterlagen sind bei rechtskräftigen Verwaltungsentscheidungen über die Aufnahme einer Person in die Liste (diese Entscheidungen werden veröffentlicht) die der Entscheidung zugrunde liegenden Informationen dauerhaft als schriftlicher Nachweis, der das Tätigwerden der Stelle rechtfertigt, aufzuwahren. Die Beweismittelakte wird im Hinblick auf eine etwaige behördliche oder gerichtliche Überprüfung — falls die Aufnahme in die Liste angefochten werden sollte — sowie zur Unterstützung weiterer Ermittlungen zum Terrorismus aufbewahrt. Dagegen werden in Fällen, in denen die Ermittlungen nicht zur Aufnahme in die Liste führen, die Ermittlungsakten spätestens ein Jahr nach dem Abschluss der Ermittlungen von der betreffenden Behörde an Ort und Stelle vernichtet.

Schließlich ist festzuhalten, dass sich die Aufbewahrungsfrist für wichtige Informationen, die im Rahmen des TFTP gewonnen und an andere Behörden oder Regierungen weitergegeben wurden, gemäß den vorstehend beschriebenen US-amerikanischen Rechtsvorschriften nach den Regelungen und Vorschriften der empfangenden Behörde oder der empfangenden Regierung richtet. Beispielsweise gelten für gewonnene Informationen, die im Rahmen einer Verfolgungsmaßnahme des Justizministeriums verwendet werden, die Aufbewahrungsfristen des Justizministeriums.

Ständige Zusammenarbeit bei der Bekämpfung des Terrorismus

Das TFTP hat sich als äußerst wertvolles Instrument bei der Bekämpfung des Terrorismus weltweit, unter anderem auch in Europa, erwiesen. Die Regierung der Vereinigten Staaten wird auch weiterhin sorgsam prüfen, ob im Rahmen des TFTP gewonnene Informationen zur Ermittlung, Verhütung, Bekämpfung oder Verfolgung von Terrorismus oder der Finanzierung des Terrorismus in einem oder mehreren Mitgliedstaaten der Europäischen Union beitragen können; sie wird diese Informationen in allen geeigneten Fällen den zuständigen Behörden so rasch wie möglich zur Verfügung stellen.

Als Zeichen unseres Engagements und unserer Partnerschaft bei der Bekämpfung des weltweiten Terrorismus wird eine renommierte europäische Persönlichkeit ernannt, die die Aufgabe hat, zum Zwecke der Überprüfung des Schutzes personenbezogener Daten aus der EU zu bestätigen, dass das Programm im Einklang mit den vorliegenden Zusicherungen durchgeführt wird. Insbesondere wird die renommierte Persönlichkeit überwachen, ob die Arbeitsschritte in Bezug auf die Löschung von nicht-extrahierten Daten durchgeführt wurden.

Die renommierte Persönlichkeit soll über angemessene Erfahrung verfügen und die geeigneten Ermächtigungen zum Zugang zu Verschlusssachen besitzen; sie wird für einen Zeitraum von zwei Jahren, der verlängert werden kann, von der Europäischen Kommission im Benehmen mit dem Finanzministerium ernannt. Die renommierte Persönlichkeit handelt bei der Wahrnehmung ihrer Aufgaben in völliger Unabhängigkeit. Sie darf bei der Wahrnehmung ihrer Aufgaben von niemandem Weisungen einholen oder entgegennehmen. Sie enthält sich jeder Handlung, die mit ihren Aufgaben im Rahmen dieser Ernennung unvereinbar ist.

Die renommierte Persönlichkeit berichtet der Kommission jedes Jahr schriftlich über ihre Feststellungen und Schlussfolgerungen. Die Kommission wiederum erstattet dem Europäischen Parlament und dem Rat gegebenenfalls Bericht.

Das Finanzministerium wird der renommierten Persönlichkeit den für die Erledigung ihrer Aufgaben erforderlichen Zugang gewähren und ihr die erforderlichen Informationen und Daten zur Verfügung stellen. Die renommierte Persönlichkeit hält jederzeit die gesetzlich vorgeschriebenen Anforderungen in Bezug auf die Geheimhaltungspflicht und die Vertraulichkeit ein. Die praktischen Einzelheiten werden mit dem Finanzministerium vereinbart.

Das Finanzministerium unterrichtet die Europäische Union ferner über alle materiellen Änderungen in Bezug auf die in diesen Zusicherungen dargelegten Garantien und über den Erlass von US-amerikanischen Rechtsvorschriften, die die in diesen Zusicherungen gegebenen Erklärungen materiell berühren.

Das Finanzministerium wird diese Zusicherungen im amerikanischen Bundesregister (*Federal Register*) veröffentlichen lassen und stimmt ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* zu.
