EUROPÄISCHE
KOMMISSION

Brüssel, den 27.11.2013
COM(2013) 842 final

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

Ein EU-System zum Aufspüren der Terrorismusfinanzierung (EU-TFTS)

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

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

Ein EU-System zum Aufspüren der Terrorismusfinanzierung (EU-TFTS)

Diese an die Mitteilung KOM (2011) 429 vom 13. Juli 2011 anschließende Mitteilung dient dazu, das Europäische Parlament und den Rat über die Ergebnisse der Durchführbarkeitsanalyse für ein EU-System zum Aufspüren der Terrorismusfinanzierung (EU-TFTS) zu informieren.

1. KONTEXT

1.1. Hintergrund dieser Mitteilung und Begriffsabgrenzung

Bei den Verhandlungen über den Abschluss des Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten von Amerika für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus[1] (nachfolgend „SWIFT-Abkommen“) wurde insbesondere erörtert, wie personenbezogene Daten und Grundrechte im Rahmen des Abkommens optimal geschützt werden können. Einige Verhandlungsparteien argumentierten, durch den Umstand, dass die Datenextraktion im Hoheitsgebiet der EU erfolge, würden die an die USA übermittelten Datenmengen begrenzt und somit ein besserer Datenschutz garantiert. Ein Teil der Mitgliedstaaten hielt es für sinnvoll, langfristig ein EU-eigenes System zum Aufspüren der Terrorismusfinanzierung zu entwickeln. Das Europäische Parlament ersuchte den Rat und die Kommission, alle erforderlichen Maßnahmen zu ergreifen, um eine dauerhafte und rechtlich fundierte europäische Lösung für die Frage der Extraktion angeforderter Daten auf europäischem Boden zu finden. Der Rat und das Europäische Parlament forderten die Kommission bei der Annahme des SWIFT-Abkommens auf, spätestens ein Jahr nach dem Inkrafttreten des Abkommens einen rechtlichen und technischen Rahmen für die Extraktion der Daten auf dem Gebiet der EU und binnen drei Jahren nach dem Inkrafttreten des Abkommens einen Bericht über den Fortschritt bei der Entwicklung eines vergleichbaren EU-Systems vorzulegen[2]. Artikel 11 Absatz 1 des SWIFT-Abkommens sieht zudem vor, dass die

[1] ABl. L 195 vom 27.7.2010, S. 5.
[2] Beschluss des Rates vom 13. Juli 2010 (ABl. L 195 vom 27.7.2010, S. 3).

Kommission während der Laufzeit des Abkommens eine Studie über die mögliche Einführung eines vergleichbaren, eine gezieltere Datenübermittlung erlaubenden EU-Systems durchführt.

Für die Zwecke dieser Mitteilung sollte zwischen einem vergleichbaren EU-System und einem Rahmen für die Datenextraktion auf dem Gebiet der EU unterschieden werden. Unter einem *Rahmen für die Datenextraktion auf dem Gebiet der EU* wird ein System verstanden, dass im Hoheitsgebiet der EU durchzuführende Suchabfragen unter den gegenwärtig von der EU an die USA übermittelten Daten ermöglicht. Ein *vergleichbares EU-System* hingegen wäre ein EU-eigenes System zum Aufspüren der Terrorismusfinanzierung durch den Zugriff auf die Daten bezeichneter Anbieter, durch Suchabfragen unter diesen Daten und durch die Analyse dieser Daten. Im Falle der Einführung eines solchen EU-Systems müsste das SWIFT-Abkommen geändert werden.

1.2. Durchgeführte Maßnahmen

Im Dezember 2010 gab die Kommission hierzu eine Studie in Auftrag. Diese wurde im Juli 2011 ausgeweitet, um die zusätzliche Option der Einführung einer Regelung für die Datenvorhaltung und -extraktion zu prüfen. Im Zuge der Studie veranstaltete die Kommision vier Zusammenkünfte für Sachverständige, darunter Vertreter von Europol, der Europäische Datenschutzbeauftragte, der nach Maßgabe des SWIFT-Abkommens bezeichnete Anbieter von Zahlungsverkehrsdiensten[3] und zahlreiche Sachverständige aus interessierten Ministerien, Strafverfolgungs- oder Nachrichtendiensten und Datenschutzbehörden der Mitgliedstaaten.

Am 13. Juli 2011 stellte die Kommission in einer an das Europäische Parlament und den Rat gerichteten Mitteilung (nachfolgend „Mitteilung von 2011“) fünf von ihr ermittelte Optionen für ein EU-System zum Aufspüren der Terrorismusfinanzierung vor. Drei dieser Optionen wurden für umsetzbar gehalten. Durch die Mitteilung von 2011 sollte eine Diskussion über das weitere Vorgehen in Gang gebracht werden, und die Ergebnisse sollten in die erforderliche Folgenabschätzung einfließen.

Die Optionen wurden im Oktober 2011 auf der Tagung des Rates „Justiz und Inneres“ sowie im Ausschuss für bürgerliche Freiheiten des Europäischen Parlaments vorgestellt.

[3] Society for Worldwide Interbank Financial Telecommunication (SWIFT).

Da weder von den Mitgliedstaaten noch vom Europäischen Parlament eine eindeutige Präferenz für eine der Optionen zum Ausdruck gebracht wurde, wurde beschlossen, sämtliche Optionen im Rahmen einer von der Kommission durchgeführten Folgenabschätzung zu prüfen und die Optionen durch Ausarbeitung von Unteroptionen näher auszuführen. Auf dieser Folgenabschätzung[4] baut die vorliegende Mitteilung auf.

2. ZENTRALE GRUNDSÄTZE UND OPTIONEN

2.1. Die zentralen Grundsätze der unter dem schwedischen Ratsvorsitz angenommenen Strategie für das Informationsmanagement im Bereich der inneren Sicherheit

Bei ihrer Analyse der Vorschläge für das weitere Vorgehen hat die Kommission die zentralen Grundsätze berücksichtigt, die in der Strategie für das Informationsmanagement im Bereich der inneren Sicherheit von 2009[5] festgelegt und in ihren Mitteilungen „Überblick über das Informationsmanagement im Bereich Freiheit, Sicherheit und Recht“ (2010)[6] und „Stärkung der Zusammenarbeit der Strafverfolgungsbehörden in der EU: Das Europäische Modell für den Informationsaustausch“ (2012)[7] näher ausgeführt wurden.

Von zentraler Bedeutung hierbei sind die Grundsätze der Wahrung der Grundrechte, der Notwendigkeit, der Verhältnismäßigkeit und der Kostenwirksamkeit.

Bei der Ausarbeitung neuer Vorschläge, die die Verarbeitung personenbezogener Daten auf dem Gebiet der inneren Sicherheit berühren, misst die Kommission der Wahrung der in der Charta der Grundrechte der Europäischen Union festgeschriebenen Grundrechte und insbesondere dem Recht auf den Schutz der Privatsphäre und der personenbezogenen Daten zentrale Bedeutung bei. Im Einzelnen sieht die Charta vor, dass jede Person das Recht auf „Achtung ihres Privat- und Familienlebens“ (Artikel 7) und auf „Schutz der sie betreffenden personenbezogenen Daten“ (Artikel 8) hat. Ebenso wird in Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union, der für alle Mitgliedstaaten sowie EU-Organe, -Einrichtungen, -Ämter und -Agenturen bindend ist, bekräftigt, dass jede Person „das Recht auf Schutz der sie betreffenden personenbezogenen Daten“ hat. Nach Artikel 52 der Charta

[4] SWD(2013) xx vom …
[5] Schlussfolgerungen des Rates vom 30. November 2009 zu einer Strategie für das Informationsmanagement im Bereich der inneren Sicherheit (Ratsdokument 16637/09).
[6] KOM(2010) 385 vom 20. Juli 2010.
[7] COM(2012) 735 vom 7. Dezember 2012.

unterliegen etwaige Einschränkungen der Ausübung der in der Charta anerkannten Rechte und Freiheiten dem Grundsatz der Verhältnismäßigkeit und dürfen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.

Ein Eingriff in das Recht auf Privatsphäre gilt dann als notwendig, wenn er einem zwingenden gesellschaftlichen Erfordernis entspricht, wenn er im Vergleich zu dem verfolgten Ziel verhältnismäßig ist und wenn die staatliche Behörde den Eingriff „ausreichend begründet".

Auch wenn sich die durch Terrorismus verursachten Kosten finanziell nur schwer bemessen lassen, gilt der Grundsatz der Kostenwirksamkeit. Ein kostenwirksamer Ansatz berücksichtigt bestehende Lösungen, um Doppelarbeit weitestgehend zu reduzieren und möglichst viele Synergien zu schaffen. Außerdem gilt es jeweils zu bewerten, inwieweit es möglich ist, die Ziele eines gegebenen Vorschlags durch eine bessere Nutzung bestehender Instrumente zu verwirklichen.

2.2. Ansatz

Die Kommission hat im Lichte der oben genannten Grundsätze geprüft, ob ein EU-eigenes TFTS notwendig und im Vergleich zur gegenwärtigen Situation in Bezug auf die mit ihm verbundenen Kosten, seine Vorzüge und seine Auswirkungen auf die Grundrechte angemessen wäre.

Was die Vorzüge eines EU-eigenen Systems anbelangt, so könnte letzteres die Zugriffsmöglichkeien der EU und ihrer Mitgliedstaaten auf sachdienliche Daten erhöhen und die Möglichkeiten, Terroristen durch die Analyse von Finanztransaktionen zu verfolgen und zu identifizieren, verbessern. Da Finanztransaktionen wertvolle, aus anderen Quellen möglicherweise nicht einholbare Informationen liefern können, wäre diese Möglichkeit von besonderem Wert für die Aufdeckung terroristischer Handlungen und der an diesen beteiligten Personen. Insbesondere wenn es mehrere Anbieter von Finanzdaten und mehrere Transaktionsarten abdecken würde, könnte ein EU-eigenes TFTS somit ein zusätzliches Instrument für die Informationsbeschaffung und die Ermittlungsarbeit zur Terrorbekämpfung sowie für die Verbesserung der inneren Sicherheit in der EU sein. Gleichwohl gilt es die

Vorzüge eines EU-eigenen TFTS gegen die geschätzten Einführungs- und Instandhaltungskosten eines solchen Systems einschließlich der finanziellen Belastung, die der EU, den Mitgliedstaaten und den bezeichneten Anbietern der betreffenden Daten entstehen würden, abzuwiegen.

2.3. Die Optionen im Einzelnen

Sowohl für einen Rahmen für die Datenextraktion auf dem Gebiet der EU als auch für ein vergleichbares EU-System sind mehrere Optionen geprüft worden:

2.3.1. Ein Rahmen für die Datenextraktion auf dem Gebiet der EU

Ein Rahmen für die Datenextraktion auf dem Gebiet der EU könnte in Form eines Systems für die Vorhaltung und Extraktion von Daten des bezeichneten Anbieters geschaffen werden, das einen direkten Zugriff auf die Daten ermöglicht, die derzeit im Rahmen des SWIFT-Abkommens an die Vereinigten Staaten übermittelt werden. Ein solcher direkter Zugang würde mit entsprechenden Befugnissen ausgestatteten US-amerikanischen Analytikern oder Sachverständigen gewährt.

Eine Möglichkeit bei dieser Option bestünde darin, die betreffenden Daten auf dem Server des bezeichneten Anbieters für einen bestimmten Zeitraum vorzuhalten und die Suchabfragen unmittelbar auf diesem Server vorzunehmen. Der derzeitige im Rahmen des SWIFT-Abkommens bezeichnete Anbieter hat allerdings starke Datenschutz- und Sicherheitsmaßnahmen ergriffen, die keine Ermittlung von in den Verkehrsdaten erwähnten Personen zulassen, so dass in seinen Datenbanken keine Suchabfragen anhand personenbezogener Daten durchgeführt werden können. Mithin müsste eine separate Datenbank geschaffen werden.

Alternativ könnten die Daten extrahiert und an einem anderen sicheren Ort in der EU aufbewahrt werden. Die zur Durchführung der Suchabfragen ermächtigten US-amerikanischen Analytiker und Sachverständigen könnten entweder vor Ort in den Räumlichkeiten des bezeichneten Anbieters oder aber per Fernzugang auf die Daten zugreifen. In jedem Fall müssten unabhängig vom Aufbewahrungsort der Daten umfassende und zuverlässige, auf die konkrete Systemarchitektur zugeschnittene Sicherheitsvorkehrungen getroffen werden.

2.3.2. Ein vergleichbares EU-System

In Bezug auf die Einführung eines vergleichbaren EU-Systems sind verschiedene (in der Mitteilung von 2011 vorgestellte) Optionen in Betracht gezogen worden: ein vollständig zentrales System auf EU-Ebene, ein dezentrales System auf Ebene der Mitgliedstaaten und drei Hybridsysteme, an denen sowohl die EU als auch die Mitgliedstaaten beteiligt wären.

Bei jeder Option bestehen mehrere Möglichkeiten in Bezug auf den Umfang des EU-Systems. Es gilt jeweils zu entscheiden, welche Mitteilungsarten abgedeckt und welche Anbieter bezeichnet werden sollen. So könnte bei einem vergleichbaren EU-System an den im SWIFT-Abkommen festgelegten Finanzmitteilungsarten und bezeichneten Anbietern festgehalten oder aber darüber hinausgegangen werden.

- Die Option eines vollständig zentralen Systems auf EU-Ebene würde bedeuten, dass eine gemeinsame EU-Stelle sämtliche Schlüsselfunktionen des Systems erfüllen würde: Anfordern der Datenextraktion, Datenspeicherung, Durchführung von Suchabfragen und Datenanalysen, Schutz und Überwachung des Systems und Übermittlung von Ermittlungshinweisen an die Mitgliedstaaten. Diese Option ist jedoch rechtlich nicht gesichert, da gegen Artikel 72 AEUV verstoßen würde, welcher besagt, dass für die Aufrechterhaltung der öffentlichen Ordnung und den Schutz der inneren Sicherheit in erster Linie die Mitgliedstaaten zuständig sind. Für die Mitgliedstaaten wäre ein solches System weder machbar noch akzeptabel, weil eine zentrale EU-Stelle für die Datensammlung und -auswertung geschaffen werden müsste.
- Die Option eines vollständig dezentralen Systems auf Ebene der Mitgliedstaaten würde bedeuten, dass das System von den zuständigen Behörden der Mitgliedstaaten betrieben und keine Funktion auf EU-Ebene wahrgenommen würde. Die betreffenden Daten könnten somit gleichzeitig an alle 28 Mitgliedstaaten übermittelt und von diesen parallel durchsucht werden. Der Datenstrom würde dadurch vervielfacht, wodurch hohe Kosten entstünden. Auch würde sich die Gefahr erhöhen, dass die Daten nicht einheitlich behandelt und uneinheitliche Datenschutzverfahren eingeführt werden. Daher wird auch diese Option für nicht realisierbar erachtet.

Diese beiden Optionen wurden daher nicht weiter geprüft.

Die drei übrigen Optionen für ein vergleichbares EU-System (Hybridsysteme) beinhalten jeweils die Aufteilung der verschiedenen Funktionen auf unterschiedliche Stellen auf EU- und nationaler Ebene.

Bei allen drei Hybridsystemen müssten die Daten fortlaufend und jedes Mal neu per Anfrage an den bezeichneten Anbieter abgerufen, extrahiert und in einer an einem sicheren Ort in der EU befindlichen Datenbank gespeichert werden. Die Suchabfragen würden sodann unter den in dieser zentralen Datenbank gespeicherten Daten durchgeführt. Bei allen drei Optionen müssten geeignete Datenschutzvorkehrungen getroffen werden.

- A) Für das erste Hybridsystem, einem Koordinierungs- und Analysedienst im Rahmen eines EU-Systems zum Aufspüren der Terrorismusfinanzierung, müsste eine zentrale EU-Stelle geschaffen werden. Diese hätte die Aufgabe, Daten von den bezeichneten Anbietern anzufordern, Suchabfragen und Datenanalysen durchzuführen und die Ergebnisse weiterzuleiten. Im Unterschied zu einem vollständig zentralen System hätten die Mitgliedstaaten direkten Zugang zu dem System und könnten Suchabfragen beantragen, die dann in ihrem Namen von der Zentralstelle oder aber von ihren eigenen Analytikern durchgeführt würden.
- B) Für das zweite Hybridsystem, einem Datenextraktionsdienst im Rahmen eines EU-Systems zum Aufspüren der Terrorismusfinanzierung, wäre ebenfalls die Schaffung einer zentralen EU-Stelle erforderlich. Diese würde jedoch lediglich Suchabfragen auf Antrag der Mitgliedstaaten durchführen und die extrahierten Daten ohne Analyse an die Mitgliedstaaten weiterleiten. Zusätzlich könnte diese EU-Stelle von sich aus Suchabfragen durchführen und deren Ergebnisse analysieren.
- C) Beim dritten Hybridsystem, einer Koordinierungsstelle für die zentralen Meldestellen zur Entgegennahme von Geldwäsche-Verdachtsanzeigen (Financial Intelligence Units – FIU)[8], würde eine Ad-hoc-Plattform auf EU-Ebene geschaffen. Dabei würde es sich aber nicht um ein ständiges Gremium handeln, sondern um eine Gruppe von Experten auf dem Gebiet der Analyse von Finanzinformationen, die je nach Bedarf Zusammenkünfte abhalten würde. Zu diesem Zweck könnte die bestehende FIU-Plattform erweitert werden: Jeder Mitgliedstaat würde einen in

[8] Beschluss des Rates vom 17. Oktober 2000 über Vereinbarungen für eine Zusammenarbeit zwischen den zentralen Meldestellen der Mitgliedstaaten beim Austausch von Informationen.

seinem Namen handelnden Vertreter benennen. Dieses Ad-hoc-Gremium würde die Anfragen der zentralen Meldestellen der einzelnen Mitgliedstaaten bündeln und entsprechende Datenanfragen an die bezeichneten Anbieter richten. Die Vertreter der einzelnen Mitgliedstaaten hätten die Aufgabe, im Namen ihres Mitgliedstaats Suchabfragen und Datenanalysen durchzuführen und die Ergebnisse entsprechend weiterzuleiten. Anschließend wäre es Sache der zuständigen Behörden der Mitgliedstaaten, die Ermittlungshinweise zu nutzen und auf nationaler Ebene weiterzuleiten.

2.3.3. Status quo: SWIFT-Abkommen

Zurzeit können die EU und die Mitgliedstaaten im Rahmen des SWIFT-Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten von Amerika für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus (TFTP) von US-Beamten durchzuführende Suchabfragen beantragen.

Das TFTP wurde von den Vereinigten Staaten als Reaktion auf die Terroranschläge vom 11. September 2001 entwickelt. Sein Kernpunkt ist die Durchführung von Suchabfragen unter den vom bezeichneten Anbieter übermittelten Daten, die auch die aus der EU übermittelten Daten einschließen.

Das SWIFT-Abkommen regelt detailliert, wie die US-Behörden etwaige Ersuchen um Daten zu stellen haben. Europol überprüft jeweils, ob die aus den Vereinigten Staaten eingehenden Ersuchen im Einklang mit dem Abkommen stehen und so eng wie möglich gefasst sind, um die zu übermittelnde Datenmenge auf ein Minimum zu reduzieren. Die sichere Verarbeitung, Speicherung und Löschung der Daten ist durch zahlreiche Bestimmungen geregelt. Die übermittelten Daten werden an einem sicheren Ort aufbewahrt und von anderen Daten getrennt gespeichert. Das Abkommen sieht eine Vorhaltezeit von fünf Jahren und eine regelmäßige Überprüfung der Notwendigkeit, die Daten weiterhin aufzubewahren, vor. Zwei der unabhängigen Prüfer in den Vereinigten Staaten wurden von der EU ausgewählt. Sie kontrollieren fortlaufend, wie das System betrieben wird, und sie können jede von den Beamten des US-Finanzministeriums durchgeführte Suchabfrage überprüfen, um sich zu

vergewissern, dass die betreffende Suchabfrage tatsächlich im Zusammenhang mit einer terroristischen Handlung oder deren Finanzierung steht.

Das Abkommen enthält zudem Bestimmungen über den Zugang zu personenbezogenen Daten, über deren Berichtigung und über Rechtsbehelfe. Es sieht vor, dass jede Person, die der Ansicht ist, dass ihre personenbezogenen Daten unter Verstoß gegen das Abkommen verarbeitet wurden, das Recht hat, gemäß den Rechtsvorschriften der Europäischen Union, ihrer Mitgliedstaaten beziehungsweise der Vereinigten Staaten einen wirksamen administrativen und gerichtlichen Rechtsbehelf einzulegen. Zudem schreibt das Abkommen vor, dass allen Personen ohne Ansehen der Staatsangehörigkeit oder des Wohnsitzlands nach dem Recht der Vereinigten Staaten ein Verfahren zur Verfügung stehen muss, mit dem sie einen gerichtlichen Rechtsbehelf gegen ein sie beschwerendes Verwaltungshandeln einlegen können.

Der Rechtsbehelf gegen ein beschwerendes Verwaltungshandeln des Finanzministeriums im Zusammenhang mit gemäß dem SWIFT-Abkommen übermittelten personenbezogenen Daten ist insbesondere durch den Administrative Procedure Act und den Freedom of Information Act geregelt. So sieht der Administrative Procedure Act vor, dass Personen, die infolge einer Handlung der US-Regierung Schaden erlitten haben, Rechtsmittel dagegen einlegen können. Im Freedom of Information Act ist zudem festgeschrieben, dass alle Personen einen administrativen oder gerichtlichen Rechtsbehelf einlegen können, um staatliche Aufzeichnungen einsehen zu können. Die geltenden, von der Kommission, den US-Behörden und der Artikel-29-Datenschutzgruppe vereinbarten einheitlichen Verfahren für den Zugang zu personenbezogenen Daten und/oder deren Berichtigung, Löschung oder Sperrung sollen den EU-Bürgern die Ausübung dieser Rechte erleichtern. Die Anwendung des Abkommens und der darin vorgesehenen Sicherheitsgarantien und Kontrollen muss nach Artikel 13 des Abkommens regelmäßig überprüft werden. Bei den beiden bisherigen Überprüfungen in den Jahren 2011[9] und 2012[10] wurde jeweils der Schluss gezogen, dass das Abkommen ordnungsgemäß umgesetzt worden war. Die dritte Überprüfung ist für das Frühjahr 2014 geplant. Der gemäß Artikel 6 des Abkommens vorgelegte gemeinsame Bericht über den Nutzen der bereitgestellten Daten hat gezeigt, wie nützlich das TFTP für die Verhütung und

[9] SEC(2011)438 vom 30. März 2011.
[10] SWD(2012)454 vom 14. Dezember 2012.

Bekämpfung des Terrorismus und seiner Finanzierung ist und dass mehrere Mitgliedstaaten auf das TFTP zurückgegriffen haben. Dank der für das TFTP bereitgestellten Daten und ihrer Genauigkeit können weltweit Netze von Terroristen und ihrer Unterstützer aufgedeckt und verfolgt werden. Durch das Programm werden die bestehenden Finanzstrukturen terroristischer Organisationen ans Licht gebracht und Möglichkeiten zur Aufdeckung neuer Ströme an finanzieller Unterstützung und zur Ermittlung der beteiligten Personen eröffnet.

3. BEWERTUNG

Bei der Prüfung der Frage, ob sie einen Vorschlag zur Schaffung eines EU-TFTS ausarbeiten sollte, muss die Kommission den unterschiedlichen Standpunkten und Erwartungen in Bezug auf die Zielsetzungen für ein solches System gerecht werden. So bestehen unter den verschiedenen Akteuren ebenso wie bei den Entscheidungsträgern unterschiedliche Auffassungen darüber, welchen konkreten Zielen das System dienen sollte. Die Kommission hat jeweils für beide Szenarien geprüft, welche Möglichkeiten und Folgen diese in Bezug auf die bestehenden Grundsätze für die Entwicklung und Umsetzung der weiter oben näher ausgeführten politischen Maßnahmen mit sich bringen würden. Insbesondere wurden alle Optionen nach den Kriterien der Notwendigkeit, Verhältnismäßigkeit und Kostenwirksamkeit gewichtet.

3.1. Ein Rahmen für die Datenextraktion auf dem Gebiet der EU

Wie in Abschnitt 2.3.1. beschrieben, würde die Option einer Regelung für die Datenvorhaltung und -extraktion die Möglichkeit schaffen, Daten, die derzeit nach Maßgabe des SWIFT-Abkommens in die Vereinigten Staaten übermittelt werden, auf dem Gebiet der EU zu sammeln und zu speichern und unter ihnen Suchabfragen durchzuführen. Was etwaige Ermittlungshinweise anbelangt, würden dadurch im Vergleich zur gegenwärtigen Situation keine zusätzlichen Vorteile für die EU oder die Mitgliedstaaten entstehen. Im Gegenteil: Dadurch, dass die im Rahmen des TFTP erhobenen Daten teils in den Vereinigten Staaten und teils in der EU gespeichert würden, würde eine sich möglicherweise negativ auf die Zahl und die Qualität der Ermittlungshinweise und somit auf die Wirksamkeit des TFTP auswirkende Aufsplitterung der Suchabfragen entstehen, die ja gegenwärtig unter einer einzigen im Rahmen des TFTP zusammengetragenen Datenmenge erfolgen. Auch könnte sich der Analysevorgang erheblich verlangsamen, da es zur Verfolgung von Ermittlungshinweisen erforderlich sein könnte, mehrere aufeinander folgende Suchvorgänge unter an zwei

unterschiedlichen Orten gespeicherten TFTP-Daten durchzuführen. Für Ermittlungen über terroristische Handlungen ist ein rasches Vorgehen jedoch oftmals von wesentlicher Bedeutung.

Würden die Daten nicht in den Vereinigten Staaten, sondern auf EU-Gebiet extrahiert, wäre nicht automatisch ein besserer Schutz personenbezogener Daten gewährleistet. Unabhängig vom Aufbewahrungsort ist für eine ordnungsgemäße Datenbehandlung entscheidend, wie gut diese vor dem Zugriff geschützt sind. Deshalb müssten solide Schutzmaßnahmen ergriffen werden, durch die garantiert würde, dass die Daten jeweils den erforderlichen Anforderungen entsprechend behandelt und verarbeitet würden. So müsste das System mit einer Kontrollfunktion zur Verifizierung der Ersuchen um Durchführung von Suchabfragen und ihrer Begründung versehen werden. Bei der Sicherstellung, dass die Daten nur zu den begrenzten, im Abkommen über die Einführung des Systems festzulegenden Zwecken verwendet werden, käme den unabhängigen Prüfern eine entscheidende Rolle zu. Auch müssten Maßnahmen zur Verhinderung des Datenzugriffs oder der Datenoffenlegung durch Unbefugte (z.B. Aufbewahrung an einem sicheren Ort) ergriffen und Verfahren für den Zugang zu personenbezogenen Daten und deren Berichtigung festgelegt und diesbezügliche Rechtsbehelfe vorgesehen werden. Außerdem müsste ein externes Audit vorgesehen werden, durch das sichergestellt wird, dass das System ordnungsgemäß betrieben wird.

Im Rahmen des SWIFT-Abkommens haben die Vereinigten Staaten keineswegs zu sämtlichen Daten des bezeichneten Anbieters Zugang, sondern nur zu den Datensätzen, um deren Bereitstellung sie auf der Grundlage früherer oder laufender Analysen über Terrorrisiken ersuchen und zu deren Übermittlung Europol seine Zustimmung erteilt. Falls kein ähnlicher Mechanismus zur Eingrenzung derartiger Datenübermittlungsersuchen eingeführt würde, hätte die Erlaubnis, unmittelbare Suchabfragen unter sämtlichen Daten des bezeichneten Anbieters durchzuführen, eine weitere Exponierung der Daten mit entsprechenden Auswirkungen auf die Datenschutzrechte zur Folge. Daher müssten erhebliche Änderungen an der Arbeitsweise des bezeichneten Anbieters und der Speicherung seiner Daten vorgenommen werden. Die Finanzmitteilungen, die Gegenstand des Abkommens sind, werden derzeit in einer Form aufbewahrt, die keine Identifizierung der in den Mitteilungen erwähnten Personen zulässt. Jede Finanzmitteilung wird verschlüsselt und kann lediglich anhand der Metadaten (Versanddatum, Mitteilungsart, Name der Absender-

und der Empfängerbank) einer Suchabfrage unterzogen werden. Der bezeichnete Anbieter hat starke Datenschutz- und Sicherheitsmaßnahmen ergriffen, um die Daten seiner Kunden in der ganzen Welt zu schützen. Um unmittelbare Suchabfragen auf dem Server des derzeitigen bezeichneten Anbieters zu ermöglichen, müssten folglich alle Mitteilungen zunächst entschlüsselt werden. Dies würde jedoch einen übermäßigen, nicht angemessenen Aufwand mit sich bringen, da der Server des bezeichneten Anbieters mehr Mitteilungen enthält als für die Zwecke der Bekämpfung der Terrorismusfinanzierung erforderlich sind. Ein direkter Zugang für die Durchführung von Suchabfragen würde zudem in nicht zulässigem Umfang den täglichen Geschäftsbetrieb des bezeichneten Anbieters belasten und erhebliche Risiken in Bezug auf den Betrieb, die Sicherheit und das System mit sich bringen. Deshalb müsste eine separate Datenbank auf EU-Gebiet für die erforderlichen Daten des bezeichneten Anbieters geschaffen werden.

Um das System einführen und seine Übereinstimmung mit den Sicherheitsvorschriften garantieren zu können, wären umfangreiche Investitionen erforderlich. Die Räumlichkeiten des bezeichneten Anbieters oder andere sichere Räumlichkeiten müssten an die spezifischen Anforderungen angepasst werden, IT- und technische Lösungen müssten entwickelt und unterhalten werden, und es müsste hinreichend qualifiziertes Personal für die Verwaltung und Beaufsichtigung des Systems eingestellt und geschult werden.

Bei dieser Option hätten die EU und die Mitgliedstaaten sämtliche Nachteile und Kosten eines ausschließlich dem TFTP dienenden Instruments, das einem Drittland gehört, zu tragen. Der Rückgriff auf diese Option scheint zum gegenwärtigen Zeitpunkt weder notwendig noch verhältnismäßig oder kostenwirksam zu sein, da er keine zusätzlichen Vorteile für die Gewinnung von Ermittlungshinweisen mit sich bringen würde, die Umsetzung sehr kostspielig und anspruchsvoll wäre und möglicherweise Risiken für den Schutz personenbezogener Daten entstehen würden.

3.2. Ein vergleichbares EU-System

Die Option eines vollständig zentralen EU-TFTS wurde von einer weiteren Prüfung ausgeschlossen, da es ihr an einer Rechtsgrundlage fehlt und nur wenig wahrscheinlich ist, dass die Mitgliedstaaten eine zentrale Rolle der EU in einem in die Zuständigkeit der Mitgliedstaaten fallenden Bereich zulassen würden. Die Option eines vollständig dezentralen Systems wurde ausgeschlossen, weil sie mit enormen Kosten verbunden wäre und vielfache

Auswirkungen auf die Datenschutzrechte hätte. Die drei näher geprüften Hybridsysteme würden den Mitgliedstaaten eine unterschiedlich starke Kontrolle über die von ihnen und der zentralen EU-Stelle durchgeführten Suchabfragen ermöglichen.

Durch die Ausweitung eines vergleichbaren EU-Systems auf automatisierte Clearingstellen, elektronisches Geld und andere Nichtfinanzdaten würden Vorteile für die Gewinnung von Ermittlungshinweisen entstehen, da die Möglichkeiten der EU zur Verfolgung des innerhalb der EU erfolgenden Zahlungsverkehrs verbessert würden. Auch wäre ein solches System möglicherweise „zukunftssicherer“ als ein System, das sich ausschließlich auf Finanzmitteilungen erstreckt. Gleichwohl würde sich mit jedem hinzukommenden bezeichneten Anbieter die Gefahr der Verletzung von Datenschutzrechten erhöhen und somit die Einführung strenger Bedingungen, Sicherheitsgarantien und Kontrollmaßnahmen notwendig werden. Auch würde sich der Verwaltungsaufwand für die bezeichneten Anbieter erhöhen. Durch die Schaffung eines derart komplexen und organisatorisch und technisch anspruchsvollen, weil auf mehrere Datenanbieter und Mitteilungsarten ausgeweiteten Systems würden zudem die Kosten beträchtlich zunehmen.

Da die Vorteile einer Ausweitung auf mehrere Datenarten und -anbieter nach dem Dafürhalten der Kommission die beträchtlichen Kosten, die dabei den privaten Unternehmen entstehen würden, und die durch ein solches System verursachten Beeinträchtigungen der in Bezug auf den Schutz der Privatsphäre und den Datenschutz geltenden Rechte nicht aufwiegen können, wäre folglich nur ein sich ausschließlich auf Finanzmitteilungsdaten erstreckendes EU-TFTS machbar. Ein solches EU-eigenes System würde sich mithin nur auf denselben bezeichneten Anbieter und dieselbe Mitteilungsart wie das TFTP erstrecken und wäre sowohl in Bezug auf die Menge und die Qualität der gewonnenen Ermittlungshinweise als auch in Bezug auf die Exponierung der Daten mit dem bestehenden, im SWIFT-Abkommen zwischen der EU und den Vereinigten Staaten vereinbarten System vergleichbar.

Wie bereits gesagt, kommen für ein solches vergleichbares EU-System drei Optionen in Frage: A) ein Koordinierungs- und Analysedienst im Rahmen eines EU-Systems zum Aufspüren der Terrorismusfinanzierung, B) ein Datenextraktionsdienst im Rahmen eines EU-Systems zum Aufspüren der Terrorismusfinanzierung und C) eine Koordinierungsstelle für die zentralen Meldestellen.

Option A würde sich wahrscheinlich positiv im Hinblick auf die Prävention von Terrorismus und die Erhöhung der Sicherheit in der EU auswirken. Wenn sowohl EU- als auch mitgliedstaatliche Teams die Suchabfragen durchführen und deren Ergebnisse analysieren würden, wäre in gewissem Umfang sichergestellt, dass die einschlägigen Anforderungen der EU und der Mitgliedstaaten für die Informationsbeschaffung und -auswertung in vollem Umfang erfüllt würden und das System jeweils auf die spezifische „EU-weite Bedrohung" zugeschnitten wäre. Diese Verbesserung hinge jedoch von einer gesteigerten Bereitschaft und Fähigkeit der Mitgliedstaaten ab, mittel- bis langfristig Informationen weiterzugeben und zu analysieren. Es ist nicht klar, inwieweit auf eine solche Zunahme des Informationsflusses vertraut werden kann. Da die Mitgliedstaaten weiterhin die Möglichkeit hätten, die US-Behörden um Durchführung von Suchabfragen im Rahmen des TFTP zu ersuchen, würde ein solches System, um einen kohärenteren Überblick über die Situation in der EU liefern zu können, außerdem umfangreiche Investitionen der Mitgliedstaaten und ein hohes Maß an Zusammenarbeit erfordern.

Option B könnte sich ebenfalls in gewissem Umfang positiv im Hinblick auf die Prävention von Terrorismus und die Erhöhung der Sicherheit in der EU auswirken. Mit dem System wäre eine genauere Reaktion auf die Bedrohungsanalysen der EU möglich, weil die Suchabfragen nach Maßgabe des spezifischen Informationsbedarfs der Mitgliedstaaten durchgeführt würden. Allerdings wäre die Rolle der zentralen EU-Stelle auf die Durchführung von Suchabfragen und die Übermittlung der ermittelten Daten an den ersuchenden Mitgliedstaat somit in erster Linie auf die Zugangskontrolle beschränkt: Es würden keine Analysen auf EU-Ebene durchgeführt, und im Hinblick auf ein kohärentes Bild der Bedrohungslage in der EU wäre man bei einem solchen System gänzlich darauf angewiesen, dass die Mitgliedstaaten außerhalb des Systems miteinander Analyseergebnisse austauschen. Da bei einem solchen System keine einheitliche Herangehensweise an die Definition von Suchabfragen gewährleistet wäre, würde sich die Wahrscheinlichkeit falscher Positive und damit von Verstößen gegen das Recht auf den Schutz der Privatsphäre und der personenbezogenen Daten erhöhen.

Option C wäre auf den spezifischen Informationsbedarf der Mitgliedstaaten zugeschnitten und könnte sich daher in gewissem Umfang positiv im Hinblick auf die Prävention von Terrorismus und die Erhöhung der Sicherheit in der EU auswirken. Da jedoch die zentralen

Meldestellen für die Suchabfragen und die Analysen ihrer Mitgliedstaaten zuständig wären, würden die gleichen Nachteile wie bei Option B bestehen: Ein klares Bild der Bedrohungslage in der EU ließe sich nur erstellen, wenn die Mitgliedstaaten außerhalb des Systems verstärkt zusammenarbeiten würden. Zudem befassen sich die zentralen Meldestellen ausschließlich mit Finanzdaten, und die Trennung zwischen Finanz- und sonstigen ermittlungsrelevanten Daten könnte es erschweren, Zusammenhänge zu erkennen und Fälle von Terrorismusfinanzierung aufzudecken. Auch wäre bei dieser Option nur eine sehr geringe Mitwirkung der EU möglich, und verbesserte Möglichkeiten würden vor allem auf nationaler Ebene geschaffen.

All diese Optionen würden erhebliche Kosten für die EU, die Mitgliedstaaten und den bezeichneten Anbieter mit sich bringen (beispielsweise für die Entwicklung von IT-Infrastruktur, für Sicherheitseinrichtungen und für die Einstellung und Besoldung von zig, wenn nicht gar Hunderten von Bediensteten für die Verwaltung des Systems und die nötigen Sicherheitsvorkehrungen und Kontrollen). Gleichwohl könnten auch alle Systeme zu einer besseren Sicherheitslage in der EU beitragen, da sie sich auf speziell auf die europäischen Bedürfnisse zugeschnittene Bedrohungsanalysen stützen würden.

Wenn es ein EU-eigenes Instrument für die Informationsbeschaffung und -auswertung zur Gewinnung von Ermittlungshinweisen auf europäischem Boden gäbe, würde die Notwendigkeit entfallen, Daten zu diesem Zweck in die Vereinigten Staaten zu übermitteln. Gleichwohl wären bei wie auch immer gearteten EU-TFTS umfangreiche Datenschutzvorkehrungen und Kontrollen wie beim bestehenden SWIFT-Abkommen erforderlich, die zudem den geltenden Datenschutzvorschriften der EU und der Mitgliedstaaten genügen müssen. Bei jedem Ersuchen um Durchführung von Suchabfragen unter in EU-Systemen gespeicherten Daten müsste geprüft werden, ob die vorgeschriebene strenge Zweckbegrenzung auf die Bekämpfung von Terrorismus und seiner Finanzierung eingehalten wird und eine Datenübermittlung gerechtfertigt ist. Insbesondere würden unabhängige Prüfer benötigt, die bei jeder auf EU-Ebene oder in den Mitgliedstaaten durchgeführten Suchabfrage überprüfen, ob für diese eine ordnungsgemäße Ermächtigung vorliegt und ob diese Suchabfrage für die Zwecke der Bekämpfung des Terrorismus und seiner Finanzierung erforderlich war. Ferner müsste eine sichere Verarbeitung und Speicherung der Daten gewährleistet und verhindert werden, dass Unbefugte auf die Daten

zugreifen können. Auch wäre ein externes Audit des Betriebs des Systems und aller Sicherheitsvorkehrungen erforderlich. Alle erforderlichen Verfahren für den Zugang zu personenbezogenen Daten und für deren Berichtigung sowie für diesbezügliche Rechtsbehelfe müssten in das System integriert werden.

Fazit: Die Kommission hat der Aufforderung von Seiten des Europäischen Parlaments und des Rates entsprechend die für die Einführung eines EU-TFTS in Frage kommenden Optionen einschließlich einer Regelung für die Datenvorhaltung und -extraktion geprüft.

Die vorliegende Bewertung trägt den Grundsätzen der unter dem schwedischen Ratsvorsitz angenommenen Strategie für das Informationsmanagement im Bereich der inneren Sicherheit Rechnung. Jedes in Frage kommende System müsste den Grundsätzen der Notwendigkeit, der Verhältnismäßigkeit und der Kostenwirksamkeit genügen und die Grundrechte wahren. Die oben und in der Folgenabschätzung durchgeführte Analyse der Kommission hat ergeben, dass mit jeder realisierbaren Option Vor- und Nachteile verbunden sind. Die nicht realisierbaren Optionen wurden von der Kommission aus den genannten Gründen nicht näher geprüft.

Die zusammengetragenen Informationen legen den Schluss nahe, dass derzeit keine klare Notwendigkeit besteht, einen Vorschlag zur Schaffung eines EU-eigenen TFTS vorzulegen.

Die Kommission wäre dem Europäischen Parlament und den Rat dankbar, wenn sie zu dieser Mitteilung Stellung nehmen würden.