Franziska Boehm

Anlasslose Datensammlungen und die Mitarbeit Privater bei der Strafverfolgung – der neue Trend in der europäischen Verbrechensbekämpfung?

Vorratsdaten und Fluggastdatenspeicherung

Im Bereich des europäischen Strafrechts kommt es in letzter Zeit immer häufiger zur Mitarbeit privater Akteure bei der Strafverfolgung. Diese zu beobachtende Tendenz wirft die Frage nach der Rechtmäßigkeit dieser Maßnahmen auf. Welcher rechtliche Bezugsrahmen ist anwendbar und welche Rechtschutzmöglichkeiten für Betroffene stehen zur Verfügung?

Beispiele für diese Verflechtung zwischen privatem und öffentlichem Handeln finden sich vor allem im Bereich anlassloser Datensammlungen. Die Übermittlung von PNR,[1] d.h. Flugpassagierdaten von Fluggesellschaften, an US-amerikanische Behörden und die Richtlinie über die Vorratsdatenspeicherung sind zwei aktuelle Beispiele.[2] Der Vorschlag für eine Richtlinie über die Verwendung von Fluggastdatensätzen zu Strafverfolgungszwecken auf EU-Ebene (EU-PNR Vorschlag) und die Richtlinie über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln, bilden weitere Maßnahmen.[3]

In jedem dieser Fälle ist ein Zusammenwirken von staatlichem und privatem Handeln bei der Strafverfolgung zu beobachten, das immer häufiger in der rechtlichen Grauzone zwischen dem schon harmonisierten Datenschutzrecht der früheren ersten Säule und den noch nicht angeglichenen Datenschutzregeln der ehemaligen dritten Säule der EU[4] angesiedelt ist. Die folgenden beiden Beispiele sollen aus einer datenschutzrecht-

1 PNR heißt „passenger name records".

2 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, [2006] ABl. L105/54. Siehe Urteil zur Rechtsangleichung (Artikel 95 alter EG Vertrag) vom 10 Februar 2009, EuGH C-301/06 – Irland v. Parlament und Rat.

3 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität, KOM(2011) 32 endgültig vom 2. Februar 2011, im Folgenden: EU-PNR Vorschlag vom 2. Februar 2011; Richtlinie 2004/82/EG des Rates vom 29. April 2004 über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln [2004] ABl. L261/24.

4 Der Datenschutzrahmenbeschluss 2008/977 für die ehemalige dritte Säule (ABl. 2008 vom 30. Dezember 2008, L-350/60) harmonisiert nicht die innerstaatlichen Datenschutzvorschriften der Mitgliedstaaten, sondern betrifft nur den zwischenstaatlichen Datenaustausch im polizeilichen und justiziellen Bereich.

lichen Perspektive zeigen, in welchen Bereichen gravierende rechtliche Unsicherheiten bestehen und notwendiger Nachbesserungsbedarf besteht.

I. Die Vereinbarkeit des EU Vorschlages zur Speicherung von Fluggastdaten (EU-PNR Vorschlag) mit dem europäischen Datenschutzstandard

Im Anschluss an das im Juli 2007 geschlossenen Abkommen mit den USA über die Übermittlung von Fluggastdaten bzw. PNR an US-amerikanische Behörden zur Bekämpfung des Terrorismus,[5] legte die EU-Kommission vier Monate später einen Vorschlag für einen Rahmenbeschluss über die Nutzung von PNR innerhalb der EU vor.[6] Dieser wurde mittlerweile von dem Vorschlag für eine Richtlinie über die Verwendung von Fluggastdatensätzen zu Strafverfolgungszwecken auf EU-Ebene abgelöst (EU-PNR Vorschlag).[7]

Der Vorschlag bezweckt die Harmonisierung der mitgliedstaatlichen Vorschriften über die Pflichten der Fluggesellschaften, die Daten ihrer Flugpassagiere an die zuständigen nationalen Behörden zum Zwecke der Verhütung und Bekämpfung von terroristischen Straftaten und schwerer Kriminalität weiterzuleiten.[8]

Der EU-PNR Vorschlag beruht auf ähnlichen sicherheitspolitischen Erwägungen wie das mit den USA geschlossene Abkommen über die Übermittlung von Flugpassagierdaten. Darüber hinaus steht er in einem engen inhaltlichen und zeitlichen Zusammenhang.[9] Das Abkommen mit den USA regelt die Übermittlung von insgesamt 34 verschiedenen Datenelementen an die USA. Sie enthalten sämtliche Informationen, die mit der Abwicklung einer Flugreise zusammenhängen, u.a. die Kreditkartennummer des Passagiers, die Wohnadresse, alle Informationen über den Flugschein und die angetre-

5 Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records – PNR) und deren Übermittlung durch die Fluggesellschaften an das United States Departement of Homeland Security (DHS) (PNR-Abkommen von 2007) und Schreiben des DHS, ABl. 2007, L204/18.

6 Kommissionsvorschlag für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Strafverfolgungszwecken KOM (2007) 654 vom 6. November 2007.

7 Siehe EU-PNR Vorschlag vom 2. Februar 2011, siehe Fn. 2.

8 EU-PNR Vorschlag vom 2. Februar 2011.

9 Ausführliche Analyse, siehe: *Mendez*, 3 European Constitutional Law Review 2007, S. 127-147; *Schaar*, Multimedia und Recht 2006, S. 425-426.

tenen bzw. nicht angetretenen Flüge oder den Namen des Sachbearbeiters der Buchung.[10]

Der PNR Austausch mit den USA wurde heftig kritisiert.[11] Die Einwände bezogen sich sowohl auf die fehlenden Datenschutzgarantien auf amerikanischer Seite als auch auf die Anzahl der übermittelten Datensätze. Letztere wurden zwar vordergründig auf 19 Punkte reduziert, die allerdings dieselben 34 Datensätze enthalten, die bereits im Vorgänger-Abkommen beanstandet worden waren.[12] Der EU-PNR Vorschlag übernimmt diese 19 Datenkategorien.[13] Weiterhin existierte ein ähnliches Abkommen mit Kanada aus dem Jahr 2005, das allerdings im Jahr 2009 ausgelaufen ist. Ein weiteres Abkommen mit Australien wird zurzeit provisorisch angewandt. Einem Nachfolgeabkommen wurde im Oktober 2011 vom Europäischen Parlament zugestimmt.[14] Da das Parlament die Kommission im Mai 2010 aufgefordert hat, alle existierenden PNR Abkommen neu zu verhandeln, finden zurzeit auch Gespräche mit den USA und Kanada über den Abschluss neuer Abkommen statt. Trotz Kritik wurde im April 2012 ein Nachfolgeabkommen mit den USA vom Europäischen Parlament angenommen. Wesentliche

10 Insgesamt sind folgende Daten sind im PNR System enthalten: Das Datum, an dem der PNR erstmals angelegt wurde sowie nachfolgende Änderungen, flugspezifische Daten wie Flugtag(e) und -strecke(n), Flugnummer(n), Flugzeiten, Flugdauer, Vor- und Zuname des oder der Passagiere, Wohnadresse und Telefonnummer eines oder mehrere Passagiere, eine Adresse und Telefonnummer am Zielort, Zahlungsart: z. B. eine Kreditkartennummer und Ablaufdatum der Kreditkarte, Reisestatus des Passagiers: welche Strecken bereits abgeflogen sind und welche er noch vor sich hat, Informationen über die Splittung/Teilung einer Buchung, E-Mail-Adresse, Allgemeine Bemerkungen, spezielle Serviceanforderungen z. B. bezüglich Essen (koscher, vegetarisch u.a.), so genannte SSI und SSR (Sensitive Security Information/ Special Service Requests) Elemente, Information über den Auftraggeber und alle Änderungen des PNR mit Datum, Uhrzeit und Aktion. Weiterhin sind folgende Daten im PNR System gespeichert: Fluggerät (Typenbezeichnung des zum Einsatz kommenden Flugzeugs), Buchungsklasse (jedem Flugtarif ordnet die Fluglinie eine Bezeichnung zu, um später auch den richtigen Tarif berechnen zu können), Rechnungsanschrift, Vielflieger-Eintrag, Name der Buchungsagentur, Sachbearbeiter der Buchung, Codeshare-Information: wenn eine andere Fluggesellschaft als durch die Flugnummer angeführte den Flug ausführt, Informationen über Flugscheinausstellung (Ticketing), Daten über den Flugtarif, Daten der Flugscheinausstellung, Sitzplatzinformationen: welcher Status (auf Anfrage, bestätigt usw.), die Sitzplatznummer, Nummern der Gepäckanhänger (baggage tags), Historie über nicht angetretene Flüge (no show), Fluggäste mit Flugschein, aber ohne Reservierung (go show), Zahl der Reisenden im PNR, etwaige APIS-Informationen (Advance Passenger Information System) und ATFQ-Felder (automatische Tarifabfrage).

11 Siehe u.a.: *Simitis*, NJW 2006, S. 2011-2014; *Mendez*, 3 European Constitutional Law Review 2007, S. 127-147; *Schaar*, Multimedia und Recht 2006, S. 425-426; *Peeters*, MMR 2005, S. 11-17; *Knierim*, ZD 1/2011, S. 17-23.

12 Beispielsweise fassen die Punkte 2, 7, 10, 14 und 16 des PNR-Abkommens von 2007 insgesamt 18 Punkte des vorherigen Abkommens von 2006 zusammen und Punkt 14 des PNR-Abkommens von 2007 enthält Informationen über die Flugsscheinausstellung und fasst die Punkte 20, 22, 25, 26, 27, 32 und 34 des Abkommens von 2006 zusammen.

13 Siehe Anhang des EU-PNR Vorschlages vom 2. Februar 2011.

14 Siehe: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0470+0+DOC+XML+V0//DE.

Verbesserungen oder Änderungen im Vergleich zum Abkommen von 2007 sind in dem neuen Abkommen jedoch nicht enthalten.[15]

Das Ziel des EU-PNR Vorschlags ist die Verhütung, Aufdeckung, Aufklärung und strafrechtliche Verfolgung von terroristischen Straftaten, schwerer Kriminalität und schwerer grenzüberschreitender Kriminalität.[16] Um dieses Ziel zu erreichen, sollen sogenannte „Passenger Information Units" eingerichtet werden, die die PNR sammeln.[17] Diese neugeschaffenen PNR-Zentralstellen sollen die Daten analysieren, auswerten und dann mit den zuständigen Behörden austauschen. Es ist vorgesehen, die gesammelten Daten 5 Jahre lang zu speichern[18] Während der Speicherungszeit können die Daten verarbeitet und an Sicherheitsbehörden weitergeleitet werden.[19] Betroffen sind alle Flugpassagiere, die von einem Mitgliedstaat in das Hoheitsgebiet eines Drittstaates fliegen oder von einem Drittstaat in das Gebiet der EU.[20]

Die Verabschiedung dieses Rahmenbeschlusses würde zu einem Datenaustausch in einem bisher nicht gekannten Ausmaß zwischen Fluggesellschaften und PNR-Zentralstellen führen. 26.000 Flüge werden im Durchschnitt über Europa täglich abgefertigt und jeder Flugpassagier „produziert" dabei 34 verschiedene Datenelemente, die alle übermittelt, gespeichert und ausgewertet werden müssten.[21] Enorme Datensammlungen und massenhafte Datenanalysen in Europa wären die Folge. Ob dieses Vorhaben mit europäischen Grundrechten, insbesondere mit datenschutzrechtlichen Garantien übereinstimmt, soll die folgende Analyse zeigen.

1. Europäischer Datenschutzstandard

Der Europäische Datenschutzbeauftragte (EDSB), die Artikel 29 Datenschutzgruppe und die Agentur der Europäischen Union für Grundrechte gehen davon aus, dass der EU-PNR Vorschlag in seiner derzeitigen Fassung nicht „die Anforderungen der Erforderlichkeit und der Verhältnismäβigkeit erfüllt, die von Artikel 8 der Charta der Grundrechte der Europäischen Union, Artikel 8 der EMRK und Artikel 16 AEUV festgesetzt

15 "Comparative Study on the 2011 draft Agreement between the Unites States of America and the European Union on the use and transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security", Hornung, Gerrit and Boehm, Franziska, published by the Greens, European Free Alliance, 2012.

16 Artikel 1 des EU-PNR Vorschlages vom 2. Februar 2011.

17 Ibid Artikel 3.

18 Ibid Artikel 9; die Daten sollen 30 Tage in einer aktiven Form, danach 5 Jahre in einer Form, die die Identifizierung des Fluggastes nicht ermöglichen soll gespeichert werden.

19 Ibid Artikel 3 (1).

20 Ibid Artikel 1 in Verbindung mit 2 (b).

21 Vergleiche Europäische Flugsicherheit: http://www.eurocontrol.int/faq/corporate?tid=505.

werden".[22] Sie sehen in diesem Entwurf einen weiteren Schritt auf dem Weg zu einer routinemäßigen Erhebung von Daten von Personen, die keiner Straftat verdächtigt werden.[23]

Artikel 8 Charta der Grundrechte der EU fasst dabei den europäischen datenschutzrechtlichen Mindeststandard zusammen. Dieser ergibt sich aus dem Zusammenwirken von verschieden völker- und EU-rechtlichen Instrumenten. Artikel 8 EMRK, die Datenschutzrichtlinie 95/46 EG und die Datenschutzkonvention Nr. 108 des Europarates spielen dabei eine entscheidende Rolle. Artikel 8 Charta der Grundrechte der EU lautet:

> (1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
>
> (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
>
> (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Der Europäische Gerichtshof für Menschenrechte (EGMR) konkretisiert diesen Standard durch seine Rechtsprechung zu Artikel 8 EMRK. Der EGMR betont in Fällen, die die staatliche Datenspeicherung und Nutzung betreffen, dass die Rechtsgrundlage für solche Maßnahmen so präzise und eindeutig sein muss, dass Betroffene ihr Verhalten danach richten können. Grenzen der Befugnisse zur Informationssammlung und -Verarbeitung müssen klar definiert und festgelegt sein. Weiterhin muss bereits zu Beginn der Datenerhebung bestimmt sein, welche Art von Daten gespeichert und für welche Zwecke die Daten verwendet werden dürfen (Zweckbindungsgrundsatz) und welches

22 Stellungnahme des Europäischen Datenschutzbeauftragten (EDSB) zum Vorschlag einer Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität, ABl. vom 22. Juni 2011, C-181/24, Punkt 10 (im Folgenden: EDSB Stellungnahme ABl. vom 22. Juni 2011, C-181/24); WP 181 der Artikel 29 Datenschutzgruppe vom 5 April 2011 Stellungnahme 10/2011 zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität, pp. 9-10, para 9 (im Folgenden: WP 181 der Artikel 29 Datenschutzgruppe vom 5 April 2011) und Gutachten der Agentur der Europäischen Union für Grundrechte betreffend den Vorschlag für eine Richtlinie über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität (KOM(2011) 32 endgültig), Wien, 14. Juni 2011 (im Folgenden: Gutachten der Agentur für Grundrechte vom 14. Juni 2011).

23 EDSB Stellungnahme ABl. vom 22. Juni 2011, C-181/24, Punkte 16 und 31.

Verfahren dabei beachtet werden muss, welche Personen Zugang zu den Daten haben und für wie lange die Informationen gespeichert werden.[24]

Vor dem Hintergrund dieser Standards wirft der umfangreiche Datenaustausch zwischen den Fluggesellschaften und den PNR-Zentralstellen vier wesentliche Fragen auf:

Erstens ist die Verhältnismäßigkeit der vorgesehenen Maßnahmen zweifelhaft. Zweitens existieren Bedenken hinsichtlich des anwendbaren Rechtsrahmens. Es besteht die Gefahr, dass der Vorschlag ohne hinreichende politische Diskussion und ohne Berücksichtigung der Vereinbarkeit mit EU-rechtlichen Rahmenbedingungen beschlossen wird.[25] Drittens ist die Eigenschaft der Datenempfänger unklar und viertens ist die Weitergabe der Daten an Drittstaaten missverständlich geregelt.

2. Verhältnismäßigkeit des EU-PNR Vorschlages

Waren die ursprünglich geplanten Maßnahmen in der dritten Säule der EU zu verorten, sind sie nun auf Artikel 82 (1) (d) sowie 87 (2) (a) AEUV gestützt.[26] Der EU-PNR Vorschlag müsste demzufolge so gestaltet sein, dass er mit den Artikeln 7 und 8 Charta der Grundrechte der EU, Artikel 16 AEUV und als Mindestvoraussetzung mit den Garantien des Artikel 8 EMRK in Einklang steht. Dieser Artikel regelt den Schutz persönlicher Daten, der einen wesentlichen Teil des Rechts einer Person auf Schutz ihres Privatlebens darstellt.[27] Ihm kommt in polizeilichen und justiziellen Zusammenhängen eine besondere Bedeutung zu, da die EU die Grundrechte der EMRK als allgemeine

24 EGMR Urteil, Rotaru gegen Rumänien vom 4. Mai 2000, Application no. 28341/95, Rn. 57; vergleiche auch: EGMR Urteile: Leander gegen Schweden vom 26. März 1987, Application no. 9248/81; Amann gegen Schweiz vom 16. Februar 2000, Application no. 27798/95; Panteleyenko gegen Ukraine vom 29. Juni 2006, Application no. 11901/02; S. and Marper gegen das Vereinigte Königreich vom 4. Dezember 2008, Application nos. 30562/04 and 30566/04; Weber und Saravia gegen Deutschland vom 29. Juni 2006, Application no. 54934/00; C.G. u.a. gegen Bulgarien vom 24. April 2008, Application no. 1365/07; Association for European Integration and Human Rights and Ekimdzhiev gegen Bulgarien vom 28. Juni 2007, Application no. 62540/00; Malone gegen das Vereinigte Königreich vom 2the United Kingdom, Application no. 8691/79.

25 Siehe Stellungnahme des unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) vom 03. Dezember 2007, *Thilo Weichert*.

26 EU-PNR Vorschlag vom 2. Februar 2011, vor Erwägungsgrund (1).

27 *Meyer-Ladewig*, Kommentar zur Europäischen Menschenrechtskonvention, Artikel 8, Rn. 11, 2. Auflage 2006; siehe dazu: Urteil des EGMR Z. v Finnland, Beschwerdenummer 22009/93 vom 25. Februar 1997, Rn. 95.

Grundsätze des Unionsrechts anerkennt[28] und der EGMR – im Gegensatz zu den EU-Gerichten[29] – in diesem Bereich in den letzten Jahren eine umfangreiche Rechtsprechung entwickelt hat.[30] Artikel 52 (3) Charta der Grundrechte der EU fügt hinzu, soweit die Charta Rechte enthalte, die den durch die EMRK „garantierten Rechten entsprechen, haben sie die gleiche Bedeutung und Tragweite, wie sie ihnen in der genannten Konvention verliehen wird". Es kann daher von einer materiellen Bindung der EU an die EMRK ausgegangen werden.[31]

Um Artikel 8 EMRK zu genügen, müssen die geplanten Maßnahmen gesetzlich vorgesehen sein, eines der in Artikel 8 Abs. 2 EMRK genannten Ziele verfolgen und nachweislich notwendig sein, d.h. sie müssen durch ein zwingendes gesellschaftliches Erfordernis gerechtfertigt sein und mit dem Grundsatz der Verhältnismäßigkeit übereinstimmen.[32] Der Eingriff muss in Beziehung zum Zweck der Maßnahmen stehen und dieser Zweck darf nicht durch andere weniger einschneidende Mittel erreicht werden können.

a. Gesetzlich vorgesehen und verfolgtes Ziel

Neben den formalen stellt der Straßburger Gerichtshof auch qualitative Anforderungen an den Eingriff.[33] Das Gesetz muss für den Bürger zugänglich und in seiner Anwendung

28 Gemäß Artikel 6 (2) und (3) EU Vertrag stellen die Grundrechte der EMRK allgemeine Grundsätze des Unionsrechts dar. Darüber hinaus strebt die EU einen Beitritt zur Konvention des Europarates an. Diese Vertragsbestimmungen führen zu einer Annäherung zwischen dem Grundrechtssystem des Europarates und dem der EU. Der EuGH betont in seinen Urteilen immer wieder, „dass die Grundrechte integraler Bestandteil der allgemeinen Rechtsgrundsätze sind, deren Wahrung der Gerichtshof zu sichern hat. Der Gerichtshof lässt sich dabei von den gemeinsamen Verfassungstraditionen der Mitgliedstaaten sowie von den Hinweisen leiten, die die völkerrechtlichen Verträge über den Schutz der Menschenrechte geben, an deren Abschluss die Mitgliedstaaten beteiligt waren oder denen sie beigetreten sind. Hierbei kommt der EMRK besondere Bedeutung zu […]", siehe z.B.: EuGH Slg. 2007, I-5305 Rs. C-305/05 Ordre des barreaux francophones und germanophone u.a. *Streinz*, Europarecht, 7. Auflage 2005, S. 284, Rn. 760.

29 Bis zum Inkrafttreten des Lissabonner Vertrages war die Gerichtsbarkeit der EU Gerichte auf die Bereiche der ersten Säule (Gemeinschaftsrecht) beschränkt. Dadurch konnten Maßnahmen der ehemaligen dritten Säule (polizeiliche- und justizielle Zusammenarbeit in Strafsachen) nicht durch EU Gerichte überprüft werden. Auch nach Inkrafttreten des Lissabonner Vertrages gilt eine 5 jährige Übergangsfrist.

30 Ausführliche Analyse bei: *Siemen* „Datenschutz als europäisches Grundrecht", Duncker & Humblot 2006 und *Boehm* „Information Sharing and Data Protection in the Area of Freedom, Security and Justice – Towards harmonised Data Protection Principles for Information Exchange at EU-level", Springer 2011.

31 *Hilf/Schorkopf* in *Grabitz/Hilf*, Das Recht der Europäischen Union, Kommentar zum EU Vertrag, Artikel 6, Rn. 48, Januar 2004.

32 EGMR Urteil Norris gegen Irland vom 26 Oktober 1988, Application no. 10581/83, Rn. 41; Meyer-Ladewig, Kommentar zur Europäischen Menschenrechtskonvention, Artikel 8, Rn. 37, 2. Auflage 2006.

33 *Meyer-Ladewig*, Kommentar zur Europäischen Menschenrechtskonvention, Artikel 8, Rn. 38, 2. Auflage 2006.

vorhersehbar sein.[34] Vorhersehbar ist ein Gesetz, wenn es mit hinreichender Bestimmtheit gefasst ist, d.h. so, dass der Betroffene sein Verhalten danach ausrichten kann.[35]

Allerdings lässt sich der Zweck des EU-PNR Vorschlags nur schwer eingrenzen. Das „Gesamtziel" soll die Bekämpfung des Terrorismus, der schweren grenzüberschreitenden Kriminalität und der schweren Kriminalität sein.[36]

Diese Zielvorgaben sind denkbar weit gefasst und werden im EU-PNR Vorschlag selbst weder konkretisiert noch definiert. Allerdings sieht Artikel 2 (g)-(i) vor, dass für die Terrorismusdefinition auf den umfassenden Straftatenkatalog des Rahmenbeschlusses des Rates zur Terrorismusbekämpfung aus dem Jahre 2002 zurückgegriffen werden soll.[37] Die Begriffe der schweren Kriminalität und der schweren grenzüberschreitenden Kriminalität sollen dem Rahmenbeschluss des Rates über den Europäischen Haftbefehl entnommen werden.[38] Im Fall der schweren Kriminalität dürfen Mitgliedstaaten „diejenigen nicht ganz so schweren Straftaten ausnehmen […], bei denen eine Verarbeitung von PNR-Daten im Sinne dieser Richtlinie nach ihrem jeweiligen Strafrecht dem Grundsatz der Verhältnismäβigkeit widersprechen würde".[39] Diese schwammige Formulierung deutet darauf hin, dass den Mitgliedstaaten ein weites Ermessen bei der Beurteilung der Frage, welche Straftaten sie von der Vorschrift ausnehmen dürfen, eingeräumt wird.[40] Eine einheitliche Anwendung der Richtlinie wird so jedenfalls nicht garantiert.

Darüber hinaus weisen die beiden Referenzinstrumente über 50 verschiedene Straftatbestände auf, die weit gefasst sind und durch die Mitgliedstaaten in nationales Recht umgesetzt und konkretisiert werden müssen. Allein Artikel 2 des Rahmenbeschluss des Rates über den Europäischen Haftbefehl enthält 32 verschiedene Kategorien, die neben Menschenhandel und Kinderpornographie auch den illegalen Handel mit bedrohten Pflanzen- oder Baumarten, Kulturgütern oder Hormonen und anderen Wachtumsförderern umfassen.

Diverse Straftatbestände, die unter den Anwendungsbereich des EU-PNR Vorschlages fallen, sind daher nur schwer mit Formulierungen wie „Kampf gegen den Terrorismus" und „Bekämpfung schwerer Kriminalität" in Verbindung zu bringen. Für Flugpassagiere bleiben diese Begriffe abstrakt und wirken bedrohlich. Betroffene können nicht abschätzen, ob ihr Verhalten unter die vorgesehenen Maßnahmen fällt oder nicht. Es besteht die Gefahr, dass Flugpassagiere ihr Verhalten vorsichtshalber an mögliche Suchmuster anpassen. Ein genereller Verdacht gefährdet daher die Unbefangenheit des Verhaltens und führt bei jedem Flugpassagier zu Unsicherheit: er weiß nicht mehr, welches Verhalten auffällig ist und welches „normalen", also nicht verdächtigen, Verhal-

34 Zu den Anforderungen an die Zugänglichkeit eines Gesetzes, siehe auch: EuGH Urteil vom 10 März 2009, Rs. C-345/06 Heinrich, insbesondere Rn. 41-63.

35 *Meyer-Ladewig*, Kommentar zur Europäischen Menschenrechtskonvention, Artikel 8, Rn. 38, 2. Auflage 2006.

36 Artikel 1 (2) des EU-PNR Vorschlages vom 2. Februar 2011.

37 Rahmenbeschlusses des Rates vom 13. Juni 2002 zur Terrorismusbekämpfung, ABl. 2002 L 164/ 03, Artikel 1-4.

38 Rahmenbeschlusses des Rates vom 13. Juni 2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten, ABl. 2002 L 190/1, Artikel 2 (2).

39 Artikel 2 (h) des EU-PNR Vorschlages vom 2. Februar 2011.

40 Vergleiche Gutachten der Agentur für Grundrechte vom 14. Juni 2011, S. 15, Punkt 2.2.

tensweisen entspricht.[41] So werden Misstrauen und Zweifel zwischen den Flugpassagieren untereinander gesät.

Um den Anforderungen, die der EGMR an die Bestimmtheit aufstellt hat, zu genügen, ist eine präzisere und klarstellende Definition des Ziels der Maßnahme unumgänglich. Zum jetzigen Zeitpunkt hat sich der EU-PNR Vorschlag einen sehr weiten Anwendungsbereich und es ist zweifelhaft, ob er mit den Garantien der EMRK in Einklang steht.

b. Notwendigkeit der Maßnahmen: Zwingendes gesellschaftliches Erfordernis und Verhältnismäßigkeit

Gemäß Artikel 8 EMRK müsste der Eingriff notwendig sein, d.h. einem zwingenden gesellschaftlichen Erfordernis entsprechen und mit verhältnismäßigen Mitteln durchgesetzt werden.[42] Der Eingriff muss in Beziehung zum Zweck der Maßnahmen stehen und dieser Zweck darf nicht durch andere weniger einschneidende Mittel erreicht werden können.

Zunächst sollen die Mittel, mit denen dieser Zweck erreicht werden soll, einer näheren Betrachtung unterzogen werden.

Zusätzlich zur Verwendung der Daten zum Ausfindigmachen von gesuchten Terroristen oder bekannten Straftätern sollen die Daten solange aufbewahrt werden, bis sie für Ermittlungen verwendet werden können.[43] Strafverfolgungsbehörden sollen die Daten aber nicht nur reaktiv, sondern auch „in Echtzeit" und „Proaktiv" verwenden können. Aufschluss über die Bedeutung dieser Begriffe gibt die Begründung der Kommission für den EU-PNR Vorschlag. „In Echtzeit" bedeutet danach „vor Ankunft oder Abreise der Fluggäste, um eine Straftat zu verhindern, Personen zu beobachten oder festzunehmen, bevor eine Straftat begangen wird oder weil eine Straftat begangen wird bzw. wurde. In diesen Fällen sind PNR-Daten erforderlich, um anhand zuvor festgelegter Prüfkriterien einen Abgleich vorzunehmen, damit bisher „unbekannte" Verdächtige identifiziert und ein Datenabgleich mit verschiedenen Datenbanken für gesuchte Personen und Gegenstände durchgeführt werden können".[44] Proaktiv bezieht sich auf die „Analyse und Bestimmung von Prüfkriterien, die für eine Überprüfung der Fluggäste vor ihrer Ankunft oder Abreise herangezogen werden können".[45]

In einem ersten Begleitdokument zu dem ursprünglichen EU-PNR Vorschlag aus dem Jahr 2007 las es sich noch eindeutiger. Das Dokument sprach von einem „Abgleich der PNR-Daten mit einer Reihe von Merkmalen und Verhaltensmustern zwecks Erstellung

41 Im Bezug auf die Rasterfahndung, siehe Argumentation des BVerfG, 1 BvR 518/02, Rn. 117.
42 *Meyer-Ladewig*, Kommentar zur Europäischen Menschenrechtskonvention, Artikel 8, Rn. 42, 2. Auflage 2006.
43 Erwägungsgrund 21 des EU-PNR Vorschlag vom 2. Februar 2011.
44 Begründung des EU-PNR Vorschlag vom 2. Februar 2011, S. 4.
45 Begründung des EU-PNR Vorschlag vom 2. Februar 2011, S. 4.

eines Risikoprofils. Wenn ein Flugreisender in ein bestimmtes Risikoprofil passt, kann er als Passagier mit hohem Gefährdungspotenzial eingestuft werden".[46]

Liest man diese beiden Dokumente zusammen, so kann davon ausgegangen werden, dass die PNR Sammlung der Identifizierung von „Hochrisiko-Passagieren" dient. Eine Risikobewertung basiert normalerweise auf festgelegten Charakteristika und Verhaltensmustern. Die PNR würden dazu beitragen, Risikoanalysen in Bezug auf Personen vorzunehmen, neue Erkenntnisse zu sammeln und Verbindungen zwischen bekannten und unbekannten Personen herzustellen.[47] Im vorliegenden Richtlinienvorschlag wird zwar nicht mehr, wie früher, der Begriff „Risikobewertung" benutzt, es wird nur noch von „Überprüfung" gesprochen, dennoch ist nicht von der Hand zuweisen, dass zur Identifizierung von bisher unbekannten Verdächtigen „anhand zuvor festgelegter Prüfkriterien" die Erstellung von Reisemustern und Profilen notwendig ist. Das Hauptziel der vorgeschlagenen Maßnahme ist daher die Entdeckung von bisher unbekannten Verdächtigen, die notwendigerweise eine Unterscheidung zwischen normalen (d.h. als unverdächtig eingestuften) und verdächtigen Fluggästen zur Folge hat. Dies wird insbesondere dann deutlich, wenn die Kommission begründet, warum die bestehenden europäischen Überwachungssysteme wie das Visa- und das Schengener-Informationssystem nicht ausreichend sind, um die Kriminalität in der EU zu bekämpfen. Hier heißt es: „Wie die API-Daten werden das SIS und das VIS daher vor allem zur Identitätskontrolle und als Grenzmanagementinstrument eingesetzt und sind nur von Nutzen, wenn die Identität des Verdächtigen bekannt ist. Diese Instrumente eignen sich weder zur Überprüfung von Personen noch zum Aufspüren „unbekannter" Straftäter oder Terroristen".[48]

Da die aktuelle Fassung des EU-PNR Vorschlages lediglich Prüfkriterien verbietet, die „die Rasse oder ethnische Herkunft einer Person, ihre religiösen oder weltanschaulichen Überzeugungen, ihre politische Einstellung, ihre Mitgliedschaft in einer Gewerkschaft, ihren Gesundheitszustand oder ihr Sexualleben" zum Gegenstand haben,[49] gehen der Europäische Datenschutzbeauftragte und die Europäische Agentur für Grundrechte davon aus, dass die Überprüfung von Fluggästen auf der Grundlage unbekannter und nicht transparenter Prüfkriterien stattfinden soll.[50] Jede PNR-Zentralstelle soll in Zusammenarbeit mit den zuständigen Behörden eigene, nichtdiskriminierende Kriterien entwickeln.[51] Hier wird den Mitgliedstaaten ein weiter Umsetzungsspielraum überlassen. Um eine uneinheitliche oder auch mittelbar diskriminierende Anwendung[52] dieser Kriterien jedoch vollständig zu verhindern, wären hier weitergehende

46 Begleitdokument zum Vorschlag für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Strafverfolgungszwecken vom 12. November 2007, KOM (2007) 654 endgültig, Zusammenfassung der Folgenabschätzung, Punkt 2 (Problemstellung).

47 Vergleiche EDSB Stellungnahme ABl. vom 1.5.2008, C-110/01 zum ursprünglichen EU-PNR Vorschlag, Punkt 14.

48 EU-PNR Vorschlag vom 2. Februar 2011, Punkt 1, S. 8.

49 EU-PNR Vorschlag vom 2. Februar 2011, Artikel 4 (3).

50 Vergleiche Gutachten der Agentur für Grundrechte vom 14. Juni 2011, S. 21, Punkt 2.2.3.2. und EDSB Stellungnahme ABl. vom 22. Juni 2011, C-181/24, Punkt II, 1.16., S. 26.

51 EU-PNR Vorschlag vom 2. Februar 2011, Artikel 4 (3).

52 Zum Begriff und der Problematik der mittelbaren Diskriminierung, vergleiche: Gutachten der Agentur für Grundrechte vom 14. Juni 2011, S. 10, Punkt 2.1.2.2.

und vor allem harmonisierte Prüfkriterien notwendig, die allen Mitgliedstaaten gleichermaßen vorschreiben, welche Merkmale bei der Suche anzuwenden sind. Fälle, in denen die Auswertung der PNR zu Ermittlungen gegen Unschuldige führte, gilt es von vorneherein zu vermeiden.[53]

Eine spezielle externe und/oder unabhängige Kontrolle für die Verarbeitung der Daten durch die PNR-Zentralstellen, wie sie in der Rechtsprechung des EGMR und in Artikel 8 (3) der Charta der Grundrechte für jede Datenverarbeitung gefordert wird, ist bisher nicht vorgesehen.[54]

Zusätzlich bestehen Bedenken im Hinblick auf die Einhaltung des in Artikel 8 EU-Grundrechtecharta enthaltenen und von der Rechtsprechung des EGMR im Hinblick auf Artikel 8 EMRK konkretisierten Zweckbindungsgrundsatzes. Dieser legt fest, dass bei der Erhebung der Daten ein Zweck bestimmt werden muss, der auch im Laufe der Weiterverarbeitung der Daten nicht geändert werden darf.[55] Wer persönliche Daten preisgibt, muss wissen, zu welchen Zwecken diese verarbeitet werden.

Wer jedoch in Vorbereitung einer Reise Daten an die Fluggesellschaft weitergibt, rechnet nicht mit einer Verarbeitung der Daten zu Strafverfolgungszwecken und erst recht nicht mit der Verarbeitung der Daten zur Erstellung von Profilen oder zur Verfolgung Dritter.

Eine so umfassende präventive Sammlung und Auswertung von Daten europäischer Bürger hat es bisher noch nicht gegeben. Die vorgeschlagenen Maßnahmen gelten ausnahmslos für alle Flugpassagiere innerhalb der EU ungeachtet der Frage, ob Strafverfolgungsbehörden gegen sie ermitteln, oder nicht. Keine der geplanten Datenauswertungen setzt Anhaltspunkte für eine Straftat voraus. Es besteht lediglich die Vermutung, dass, erstens, unter den Flugpassagieren gesuchte Terroristen oder Kriminelle sein könnten, und zweitens dass, die Datenauswertung tatsächlich zum Auffinden von potentiellen Terroristen beiträgt.

Mit der Anzahl der gespeicherten Daten steigt auch das Missbrauchs- und Fehlerrisiko. Ferner können von solchen Maßnahmen Einschüchterungseffekte ausgehen, die zu einer Beeinträchtigung der Ausübung der Grundrechte führen können und die ein „Gefühl des Überwachungsstaates" entstehen lassen.[56] Mit Blick auf die große Streubreite des Eingriffs, d.h. die Gesamtzahl der von der PNR Auswertung betroffenen Personen, und der verdachtsunabhängigen Datenauswertung müsste zumindest der Nutzen des Systems eindeutig nachgewiesen sein, um den Eingriff rechtfertigen zu können.[57]

Aus der Analyse des Europäischen Datenschutzbeauftragten und der Agentur für Grundrechte geht allerdings eindeutig hervor, dass es an präzisen Informationen über

53 Siehe hier den Fall *Maher Arar*, der im Gutachten der Agentur für Grundrechte vom 14. Juni 2011, S. 18, Punkt 2.2.3 erwähnt wird.

54 Die Kontrolle würde, da die PNR-Zentralstellen national organisiert sind, auf mitgliedstaatlicher Ebene durch die lokalen Datenschutzbehörden stattfinden. Es ist jedoch zweifelhaft, ob diese finanziell oder materiell ausreichend ausgestattet sind um eine derart umfangreiche Kontrolle durchzuführen.

55 EGMR Urteil, Rotaru gegen Rumänien vom 4. Mai 2000, Application no. 28341/95, Rn. 57, siehe auch: Artikel 6 der Datenschutzrichtlinie 95/46.

56 Bundesverfassungsgericht, 1 BvR 518/02, Rn. 117.

57 Siehe: Gutachten der Agentur für Grundrechte vom 14. Juni 2011 und EDSB Stellungnahme ABl. vom 22. Juni 2011, C-181/24.

konkrete Ergebnisse der PNR Systeme, die von Behörden anderer Staaten erzielt wurden und auf die unbeirrt in der Begründung für den Vorschlag verwiesen wird, mangelt.[58] Im EU-PNR Vorschlag wird zwar auf die Erfolge bei der Bekämpfung des Drogen- und Menschenhandels verwiesen,[59] jedoch sind die angeführten Statistiken nicht unbedingt mit der ausschließlichen Auswertung von PNR in Verbindung zu bringen. Statistiken oder Beweise, dass PNR bei der Aufklärung von terroristischen Aktivitäten oder anderer schwerer Kriminalität hilft, fehlen ganz.

Weiterhin fehlt eine aussagekräftige Prüfung, ob weniger einschneidende (Ermittlungs-) Methoden zur Erreichung desselben Ziels bestehen. Diese müssen dann bevorzugt herangezogen werden – nur dann ist der Eingriff verhältnismäßig und notwendig in einer demokratischen Gesellschaft. Wie oben erwähnt werden bereits bestehende Datenbanken zur Kriminalitätsbekämpfung innerhalb der EU, wie das Visa- oder das Schengener-Informationssystem als nicht ausreichend betrachtet, weil sie nicht dazu beitragen würden, unbekannte Verdächtige aufzuspüren. Ihre Prüfung beschränkt sich allerdings auf eine einseitige kurze Zusammenfassung der Tätigkeitsfelder der Datenbanken und beinhaltet keine ausführliche Analyse.[60] Inwieweit die PNR Auswertung zu diesem Ziel beiträgt ist im EU-PNR Vorschlag ebenfalls nicht geklärt. Es ist daher nicht erwiesen, dass der Eingriff in Form der Auswertung der PNR in einer demokratischen Gesellschaft notwendig ist.

Im Hinblick auf die Rechtmäßigkeit der vorgesehenen Maßnahmen ergeben sich zum jetzigen Zeitpunkt also ernstzunehmende Zweifel, die das an sich legitime Ziel der Bekämpfung des Terrorismus und der schweren (grenzüberschreitenden) Kriminalität durch die rigorosen Methoden seiner Bekämpfung in Frage stellen.

3. Anwendbarer Rechtsrahmen und Rechte der Betroffenen

Rechtsunsicherheit besteht ebenfalls im Zusammenhang mit der Frage, welche Rechtsgrundlage für welche Akteure zu welchem Zeitpunkt gelten soll. Das bedeutet, es ist erstens zu klären, wer formell für die Durchführung der Vorschriften verantwortlich ist und zweitens, welcher Akteur die inhaltlichen Anforderungen des EU-PNR Vorschlages in der Praxis umsetzt und welcher Datenschutzstandard infolgedessen anwendbar ist.

Akteure sind zunächst die Fluggesellschaften, die privatrechtlichen Regelungen der früheren ersten Säule und somit der allgemeinen Datenschutzrichtlinie 95/46 unterworfen sind. Sie sollen die PNR dann an die jeweiligen PNR-Zentralstellen in den Mitgliedstaaten weiterleiten.

Nach einer Risikoanalyse durch die PNR-Zentralstellen sollen die PNR dann an die „zuständigen Behörden" weitergeleitet werden, bei denen es sich um Strafverfolgungsbehörden handelt, „die für die Verhütung, Aufdeckung, Aufklärung oder strafrechtliche Verfolgung von terroristischen Straftaten und schwerer Kriminalität" zuständig sind.[61] In diesem Zusammenhang sind dann die Vorschriften des Datenschutz-Rah-

58 Gutachten der Agentur für Grundrechte vom 14. Juni 2011, Punkt 2.2.3, S. 17 und EDSB Stellungnahme ABl. vom 22. Juni 2011, C-181/24, Punkt II.2., S. 25.

59 Begründung, Punkt 1, S. 2 und 7 des EU-PNR Vorschlags vom 2. Februar 2011.

60 Vergleiche: Begründung, Punkt 1, S. 8 des EU-PNR Vorschlags vom 2. Februar 2011.

61 Artikel 5 Abs. 2 des EU-PNR Vorschlag vom 2. Februar 2011.

menbeschlusses 2008/977 aus dem Jahr 2008 für die ehemalige dritte Säule (polizeiliche-und justizielle Zusammenarbeit) anwendbar, der allerdings seinerseits heftiger Kritik ausgesetzt ist.[62]

Der Datenschutzrahmen ändert sich also von den zunächst recht ausführlichen Garantien der ehemaligen ersten Säule hin zu den eingeschränkteren Rechten des Rahmenbeschlusses 2008/977. Insbesondere hinsichtlich der Rechte der betroffenen Personen bestehen hier Bedenken.[63] Im Rahmenbeschluss 2008/977 sind die Auskunftsrechte limitiert und beinhalten u.a. keine Auskunft über den Zweck der Verarbeitung.[64] Auch ist es den Mitgliedstaaten möglich, die Auskunftsrechte aus verschiedenen Gründen umfangreich zu begrenzen.[65] Weiterhin ist auch nicht geklärt, bei welchem Akteur oder welcher Behörde der Zugang zu den PNR zu beantragen ist bzw. Rechtsmittel einzulegen sind.

Nach Verabschiedung des Lissabonner Vertrages stellt sich deshalb die Frage, ob die angestrebte Harmonisierung im Datenschutzrecht[66] dadurch erleichtert wird, dass sich für den Schutz der Betroffenen auf Vorschriften der ehemaligen dritten Säule berufen wird, die damals der heftigen Kritik des Europäischen Parlaments ausgesetzt waren und die auch heute noch einen unzureichenden Individualrechtsschutz beinhalten. Wünschenswert wäre es hier eigene, verbesserte Datenschutzgarantien, die im Einklang mit der Richtlinie 95/45 stehen, zu schaffen.

Hier geht es aber nicht nur um die anwendbaren Datenschutzgarantien. Hinter dieser Problematik steckt noch ein anderer wichtiger Prozess: Originär staatliche Aufgaben wie die Strafverfolgung finden nicht mehr nur durch staatliche Behörden statt, Private üben ebenfalls eine (gesellschaftliche) Kontrolle über das Verhalten von Einzelpersonen aus.[67] Ursprünglich staatliche Eingriffsbefugnisse werden auf Private übertragen. Dadurch kommt es zu einer „Privatisierung" hoheitlicher Eingriffsbefugnisse.[68] Diese Kompetenzübertragung bringt die etablierten Datenschutzgrundsätze – und im weiteren

62 Siehe u.a.: Legislative Entschließung des Europäischen Parlaments vom 23. September 2008 zu dem Entwurf eines Rahmenbeschlusses des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (16069/2007 C6-0010/2008 – 2005/0202 (CNS)); Comments of the European Data Protection Supervisor on the recent developments with respect to the Proposal for a Council Framework Decision on the protection of personal data in the framework of police and judicial cooperation in criminal matters, 18 October 2007, interinstitutional file 2005/0202; Letter and Comments from EU Data Protection authorities to the Portuguese Council Presidency on the draft Framework Decision on personal data in police and judicial issues 7 November 2007.

63 EDSB Stellungnahme ABl. vom 22. Juni 2011, C-181/24, Punkt III.4., S. 28.

64 Vergleiche Artikel 17 (1) des Rahmenbschlusses 2008/977, ABl. 2008 vom 30. Dezember 2008, L-350/60.

65 Vergleiche Artikel 17 (2) des Rahmenbschlusses 2008/977, ABl. 2008 vom 30. Dezember 2008, L-350/60.

66 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, „Gesamtkonzept für den Datenschutz in der Europäischen Union", KOM(2010) 609 endgültig vom 4 November 2010.

67 Zur Problematik der „Sicherheit durch Privatisierung", siehe: *Albrecht* „Kriminologie, Eine Grundlegung zum Strafrecht" 3. Auflage 2005, S. 117-118.

68 Zu dieser Entwicklung, siehe: *Albrecht* „Kriminologie, Eine Grundlegung zum Strafrecht" 3. Auflage 2005, S. 365.

Sinne auch die anderen Rechtschutzmöglichkeiten – an ihre Grenzen. Wenn zwar die Mitarbeit der Privaten an der Verbrechensbekämpfung harmonisiert wird, sich im Laufe der Datenverarbeitung aber mehrmals der anwendbare Datenschutzstandard ändert, bleibt die Rechtsicherheit der Betroffenen auf der Strecke.

a. Vergleich zur Vorratsdatenspeicherungsrichtlinie

Diese Problematik taucht auch im Zusammenhang mit anderen Instrumenten wie der Vorratsdatenspeicherungsrichtlinie auf. Sie begründet ebenfalls rechtliche Verpflichtungen für private Akteure, ihre ursprünglich aus wirtschaftlichen Gründen erhobenen Daten den Strafverfolgungsbehörden auf Anfrage zur Verfügung zu stellen.[69] Im Jahr 2009 hat der Europäische Gerichtshof dazu Stellung genommen,[70] ein Jahr später das Bundesverfassungsgericht.[71]

Zunächst soll auf das europäische Verfahren eingegangen werden. Sein Ausgang war in doppelter Hinsicht interessant: Erstens würde es zur Klärung der oben aufgeworfenen Frage beitragen, welche (europäischen) Vorschriften im Zusammenhang mit der Verpflichtung Privater, an der Strafverfolgung mitzuarbeiten, anwendbar wären, zweitens bestimmte die Wahl der Rechtsgrundlage (ehemalige erste bzw. dritte Säule) den anwendbaren Datenschutzrahmen. Die tiefgreifenden grundrechtlichen Fragen, die die Vorratsdatenspeicherung aufwirft, waren hingegen nicht Gegenstand dieses Verfahrens.[72]

Nachdem schon der französische Generalanwalt *Yves Bot* im Oktober 2008 in seinen Schlussanträgen zu dem Ergebnis kam, dass die Harmonisierungsvorschrift des Art. 95 EG-Vertrag (heute Artikel 114 AEUV) die richtige Rechtsgrundlage für die Vorratsdatenspeicherungsrichtlinie sei, da sie keine Bestimmung über die polizeiliche und justizielle Zusammenarbeit in Strafsachen enthalte, die unter den damaligen EU-Vertrag fallen könne, schloss sich der Europäische Gerichtshof im Jahr 2009 dieser Ansicht an.[73]

Der Gerichtshof betonte zunächst, dass sich bei der Feststellung, ob ein Rechtsakt aufgrund von Vorschriften des vormaligen EU- oder des EG-Vertrages erlassen werden

69 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15 März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, ABl. L 105/54.

70 Rs. C-301/06, Irland gegen Europäisches Parlament und Rat der Europäischen Union, Urteil vom 10. Februar 2009.

71 BVerfG, 1 BvR 256/08 vom 2. März 2010.

72 Rechtssache C-301/06, Irland gegen den Rat der Europäischen Union und das Europäische Parlament, Urteil vom 10 Februar 2009, Rn. 57; Zur Vorratsdatenspeicherungsrichtlinie, siehe: *Braum*, KritV 1/2008, S. 82 ff.; *Gitter/Schnabel*, MMR 2007, S. 411 ff.; *Leutheuser-Schnarrenberger*, ZRP 2007, S. 9 ff.

73 Rechtssache C-301/06, Irland gegen den Rat der Europäischen Union und das Europäische Parlament, Urteil vom 10 Februar 2009. Schlussanträge des Generalanwalts Yves Bot vom 14. Oktober 2008 in der Rs. C-301/06 Irland gegen Parlament und Rat. Zur Kritik an diesen Schlussanträgen, siehe: *Gietl/Tomasic*, „Kompetenz der Europäischen Gemeinschaft zur Einführung der Vorratsdatenspeicherung", DuD 12/2008, S. 795 ff.

muss, die Rechtsgrundlage auf objektive, gerichtlich nachprüfbare Umstände, zu denen insbesondere Ziel und Inhalt des Rechtsakts gehören, stützen müsse.[74] Insbesondere im Fall von Unterschieden zwischen den nationalen Regelungen könne Artikel 95 des ehemaligen EG-Vertrages herangezogen werden. Diese Unterschiede müssten allerdings geeignet sein, die Grundfreiheiten zu beeinträchtigen oder Wettbewerbsverzerrungen zu verursachen und sich auf diese Weise unmittelbar auf das Funktionieren des Binnenmarktes auswirken.[75] Diese Anforderungen sah der Gerichtshof als erfüllt an. Die erhebliche Abweichung nationaler Vorschriften rechtfertige, insbesondere im Hinblick auf die Dauer der Vorratsspeicherung und die Art der zu speichernden Daten, den Erlass der Richtlinie auf Grundlage von Art. 95 EG-Vertrag (heute Artikel 114 AEUV).[76]

In seiner Argumentation vernachlässigt der Gerichtshof allerdings die entscheidende von Irland angesprochene Problematik: Bei der Suche nach der richtigen Rechtsgrundlage muss der Hauptzweck des in Frage stehenden Rechtsakts sowohl in seiner Zielsetzung als auch seinem Inhalt nach in der Umsetzung einer nach dem EG-Vertrag (heute AEUV) der Gemeinschaft zugewiesenen Politik bestehen.[77] Ergibt die Prüfung eines Rechtsakts, dass er zwei Ziele verfolgt oder zwei Komponenten hat, und lässt sich eine davon als wesentliche oder überwiegende ausmachen, während die andere nur von untergeordneter Bedeutung ist, so ist der Rechtsakt nur auf eine Rechtsgrundlage zu stützen, und zwar auf die Rechtsgrundlage, die die wesentliche oder überwiegende Zielsetzung oder Komponente erfordert.[78]

Folgt man dieser Rechtsprechung des Gerichtshofes, dann müssten also, neben dem Bestehen von nationalen Unterschieden, auch das überwiegende Ziel und der Inhalt der Richtlinie ausschlaggebend für die Wahl der Rechtsgrundlage sein.

Aus Artikel 1 der Vorratsdatenspeicherungsrichtlinie geht eindeutig hervor, dass die mitgliedstaatlichen Vorschriften im Bereich der Vorratsspeicherung von Verbindungsdaten harmonisiert werden sollen, um „sicherzustellen, dass die Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden, zur Verfügung stehen".[79]

Von einer Harmonisierung der Vorschriften, um die Kommunikationsdiensteanbieter vor ungleichen Marktbedingungen zu schützen, wie der Gerichtshof ausführt, ist nicht

74 Rechtssache C-301/06, Irland gegen den Rat der Europäischen Union und das Europäische Parlament, Urteil vom 10 Februar 2009, Rn. 60.
75 Ibid Rn. 63.
76 Ibid Rn. 69.
77 Rs. C-91/05, Kommission gegen Rat, Urteil vom 20 Mai 2008, Rn. 60.
78 Rs. C-491/01 British American Tobacco, Urteil vom 10 Dezember 2002, Rn. 94.
79 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15 März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, ABl. L 105/54.

die Rede.[80] Abgesehen davon sind die mitgliedstaatlichen Telekommunikationsmärkte weder auf europäischer Ebene harmonisiert, noch gibt ein grenzüberschreitendes Mobilfunk-, Telefon- oder Internet-Angebot.[81] Wettbewerbsunterschiede zwischen den auf dem Markt für elektronische Kommunikation agierenden Unternehmen sind daher ohnehin Realität.[82] Eine Harmonisierung der Speicherfristen für Kundendaten auf europäischer Ebene, noch dazu eine, die keine Kostenregelungen enthält, führt damit nicht zum Abbau finanzieller Belastungen.

Eindeutig ist in diesem Fall die Rechtsvereinheitlichung zum Schutz der Anbieter nur ein Nebenzweck der angestrebten Vorratsdatenspeicherung. Die strenge Trennung des Gerichtshofs zwischen der Speicherung der Daten und der späteren Nutzung durch die Polizeibehörden erscheint künstlich.[83] Der Gerichtshof koppelt den späteren Verwendungszweck der Daten von der reinen Verpflichtung zur Speicherung ab und kommt zu dem Schluss, dass die Richtlinie Tätigkeiten regelt, die „unabhängig von der Durchführung jeder eventuellen Maßnahme polizeilicher oder justizieller Zusammenarbeit in Strafsachen sind".[84] Diese Aussage führt die oben erwähnte Begründung der Richtlinie in Artikel 1 Abs. 1 ad absurdum, die eindeutig bestimmt, dass die Richtlinie die Vorratsdatenspeicherung harmonisiert um sicherzustellen, dass die Daten „zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten" den Strafverfolgungsbehörden zur Verfügung stehen.[85]

Insbesondere angesichts der Vorschriften des neuen Lissabonner Vertrages, der nun in Artikel 87 Abs. 2 lit. (a) eine Rechtsgrundlage für das „Einholen, Speichern, Verarbeiten, Analysieren und Austauschen sachdienlicher Informationen" in der polizeilichen Zusammenarbeit schafft, wirkt dieses Urteil zweifelhaft. Wurde im neuen Vertrag doch offensichtlich versucht, künftige Regelungen in diesem Bereich im Rahmen der gemeinsamen Polizeiarbeit anzusiedeln.

80 Wäre eine Harmonisierung gewollt gewesen, um die Serviceanbieter vor übermäßigen Kosten zu schützen, wie der Gerichtshof annimmt, dann wären in der Richtlinie auch Regelungen, die die Kostenverteilung der Vorratsdatenspeicherung betreffen, enthalten. Diese Entscheidung trifft jedoch jeder Mitgliedstaat für sich. Manche Mitgliedstaaten lassen die Anbieter alle Kosten übernehmen, andere zahlen einen Teil der Kosten, wieder andere erstatten die Kosten zurück. Die Gefahr, dass sich ein Anbieter elektronischer Kommunikationsdienste mangels Harmonisierung den mit der Vorratsspeicherung von Daten verbundenen Kosten stellen muss, je nachdem, in welchem Mitgliedstaat er seine Dienste anbieten möchte, besteht also auch weiterhin.

81 *Gietl/Tomasic*, „Kompetenz der Europäischen Gemeinschaft zur Einführung der Vorratsdatenspeicherung", DuD 12/2008, S. 795, 798.

82 Ibid S. 795, 798.

83 Rechtssache C-301/06, Irland gegen den Rat der Europäischen Union und das Europäische Parlament, Urteil vom 10 Februar 2009, Rn. 80.

84 Ibid Rn. 83.

85 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15 März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, ABl. 2006 L-105/54, Artikel 1 Abs. 1.

b. Anwendbare Vorschriften für die Telekommunikations- und PNR-Datensammlungen

Um auf die oben aufgeworfenen Fragen nach den anwendbaren Vorschriften für die (zeitlich) verschiedenen Übermittlungsetappen und nach dem anwendbaren Instrument für die Verpflichtung privater Akteure, an der Strafverfolgung mitzuarbeiten, zurückzukommen, lässt sich die erste Frage im Fall der Vorratsdatenspeicherung nun beantworten.

Folgt man der Meinung des Gerichtshofs, dann verpflichtet zunächst ein Instrument der ehemaligen ersten Säule, das der Binnenmarktharmonisierung dient, die Kommunikationsanbieter, ihre Daten zu speichern. Im Anschluss daran sind dann innerstaatliche Regelungen im Strafverfolgungsbereich anwendbar, die die Übermittlung der Daten und ihre spätere Verarbeitung regeln.[86] Innerhalb der ersten Verarbeitungsstufe der Daten ergibt sich also ein einheitlicher Rechtsrahmen, der ein einheitliches Schutzniveau (Anwendbarkeit der Regeln der ehemaligen ersten Säule, insbesondere Richtlinie 95/46) vorsieht.

Auf den ersten Blick scheint diese Lösung überschaubar zu sein. Aus datenschutzrechtlicher Sicht wird allerdings das komplette Dilemma der Vorratsdatenspeicherung deutlich: Die zu einem wirtschaftlichen Zweck erhobenen und gespeicherten Daten werden nämlich zu einem grundlegend anderen Zweck an die Strafverfolgungsbehörden weitergeleitet.

Auf diese Weise ändern sich innerhalb dieses Übermittlungsvorganges auch der Datenschutzrahmen, die Verarbeitungsverantwortlichen und die Rechtschutzmöglichkeiten der Betroffenen.

Damit verstößt zumindest dieser letzte Schritt gegen rechtsstaatliche Grundsätze und gegen den Zweckbindungsgrundsatz. Weiterhin sind Bestimmtheit und Verhältnismäßigkeit der Vorratsdatenspeicherungsrichtlinie sehr zweifelhaft.[87] Dies führt zu einer erheblichen Rechtsunsicherheit bei den Betroffenen.

Die Speicherung der Daten abgekoppelt vom eigentlichen Speicherungsgrund (Vereinfachung der Strafverfolgung) zu sehen, verschiebt lediglich das grundlegende Problem der anwendbaren Vorschriften auf die nächste Ebene und löst daher die fundamentalen datenschutzrechtlichen Probleme nicht.

Zweifelsohne kann von einer formellen Festlegung auf eine Rechtsgrundlage nicht die Lösung der sich anschließenden materiellrechtlichen Fragestellungen erwartet werden. Dennoch hängen in diesem Verfahren formelles und materielles Recht eng zusammen, weil die Festlegung auf eine Rechtsgrundlage materiellrechtliche Konsequenzen nach sich zieht und auch im formellen Teil die Frage nach dem eigentlichen Zweck der Speicherung aufgeworfen wird. Es ist nämlich entscheidend, ob sich der Datenschutz nach den Vorschriften der ehemaligen ersten oder der früheren dritten Säule richtet.

Nun könnte man vermuten, dass sich nach Inkrafttreten des Lissabonner Vertrages diese Streitigkeit erübrigt; dies ist jedoch nicht der Fall. Solange es keine einheitliche

86 § 100 g StPO enthält die Rechtsgrundlage für das Auskunftsersuchen der Strafverfolgungsbehörden gegenüber den deutschen Kommunikationsanbietern.

87 Siehe dazu, u.a.: *Braum*, KritV 1/2008, S. 82 ff.; *Gitter/Schnabel*, MMR 2007, S. 411 ff.; Leutheuser-Schnarrenberger ZRP 2007, S. 9 ff.

Regelung im Datenschutzbereich für die ehemalige dritte Säule gibt,[88] bleiben die alten fragmentierten Regeln anwendbar. Deswegen wird auch im EU-PNR Vorschlag ein ähnlicher Fehler wie bei der Vorratsdatenspeicherung wiederholt. Wird der Vorschlag in seiner derzeitigen Form verabschiedet, werden erneut verschiedene (Daten)Schutzstandards geschaffen. Auf der einen Seite würde die PNR Richtlinie die formelle Verpflichtung der Fluggesellschaften regeln, die Daten zur Speicherung und Auswertung an die PNR-Zentralstellen weiterzuleiten, auf der anderen Seite würde ein datenschutzrechtlich zweifelhaftes und veraltetes Instrument der ehemaligen dritten Säule den Schutzstandard festlegen. Ein Auseinanderdriften zwischen dem hohen Niveau des technischen Übermittlungsvorganges und den (eigentlich) dazugehörigen Rechten der Betroffenen wird dabei billigend in Kauf genommen. Sachverhalte, die eigentlich zusammengehören, werden so auf Kosten des Datenschutzstandards auseinander dividiert.

Diese Problematik wird vom deutschen Verfassungsgericht in seinem Vorratsdatenspeicherungsurteil erkannt. Der Gesetzgeber, der auch die Kompetenz zur Regelung des Telekommunikationsrechts inne hat, ist kraft Sachzusammenhangs dazu verpflichtet die damit „zu verbindenden datenschutzrechtlichen Bestimmungen" zu regeln, also ein einheitliches Regelungsniveau zu schaffen: „Andernfalls bestünde die Gefahr eines Inkongruenzen verursachenden Auseinanderfallens der technischen und datenschutzrechtlichen Regelungen der Datenverarbeitung".[89]

Die zweite Frage nach dem anwendbaren Instrument, das private Akteure verpflichtet, an der Strafverfolgung mitzuarbeiten, wird durch das Urteil des Europäischen Gerichtshofs nicht beantwortet. Ein Instrument, das vordergründig der Binnenmarktharmonisierung dient, um anschließend aber den Zugriff der Strafverfolgungsbehörden auf die Telekommunikationsdaten zu ermöglichen, kann schon aus rechtstaatlicher Sicht nicht die Lösung dieser Frage sein. In diesem Zusammenhang fehlt es weiterhin an einem zufriedenstellenden rechtlichen Rahmen, der einheitliche Kriterien und somit ein einheitliches Schutzniveau für die Daten von ihrer Erhebung über die Verarbeitung bis zu ihrer Nutzung schafft.

Aus Sicht des deutschen Verfassungsrechts stellt sich diese Frage nicht. Mit Bezug auf die finanziellen Lasten stellt das Gericht in seinem Urteil zur Vorratsdatenspeicherung fest, dass die Telekommunikationsanbieter als „Hilfspersonen für die Aufgabenerfüllung durch staatliche Behörden in Anspruch genommen"[90] werden können:

> *„Unzumutbar ist dieses [Speicherungspflicht] insbesondere nicht deshalb, weil dadurch private Unternehmen unzulässig mit Staatsaufgaben betraut würden. Eine kategorische Trennung von „Staatsaufgaben" und „privaten Aufgaben" mit der Folge der grundsätzlichen Unzulässigkeit einer Indienstnahme für Gemeinwohlzwecke von*

88 Hier gilt eine 5 jährige Übergangsfrist für die alten Instrumente der dritten Säule nach Artikel 10 Abs. 3 Protokoll Nr. 36, ABl. 2010 vom 30. März 2010, C-83/201.

89 BVerfG, 1 BvR 256/08 vom 2. März 2010, Rn. 201. Auch wenn es in Deutschland möglich ist für die Anordnung der Speicherungsverpflichtung (Bund) und der Zuständigkeit für die Schaffung der Abrufregelung und die Ausgestaltung der Transparenz und- Rechtschutzbestimmungen (Länder) Bundes- bzw. Landesrecht anzuwenden, gibt es keine so entscheidenden Unterschiede zwischen Bundes- und Landesdatenschutzrechten wie auf europäischer Ebene zwischen dem Datenschutzrecht der ehemaligen ersten Säule und dem der ehemaligen dritten Säule.

90 BVerfG, 1 BvR 256/08 vom 2. März 2010, Rn. 201.

Privaten auf deren Kosten lässt sich der Verfassung nicht entnehmen. Vielmehr hat der Gesetzgeber einen weiten Gestaltungsspielraum, welche Pflichten zur Sicherstellung von Gemeinwohlbelangen er Privaten im Rahmen ihrer Berufstätigkeit auferlegt (vgl. BVerfGE 109, 64 <85>). [...] Dabei ist der Gesetzgeber nicht darauf beschränkt, Private nur dann in Dienst zu nehmen, wenn ihre berufliche Tätigkeit unmittelbar Gefahren auslösen kann oder sie hinsichtlich dieser Gefahren unmittelbar ein Verschulden trifft. Vielmehr reicht insoweit eine hinreichende Sach- und Verantwortungsnähe zwischen der beruflichen Tätigkeit und der auferlegten Verpflichtung (vgl. BVerfGE 95, 173 <187>)".[91]

Laut europäischer sowie deutscher Rechtsprechung ist es also zu tolerieren, wenn der Staat Rückgriff auf Private nimmt, um seine Strafverfolgungsinteressen durchzusetzen. Der Unterschied zwischen beiden Rechtsprechungen liegt jedoch in der Regelung der dazugehörigen Datenschutzstandards. Das europäische Recht verkennt, dass bei einem so schwerwiegenden Eingriff wie der anlasslosen Datenspeicherung ein hohes einheitliches Datenschutzniveau auf allen Ebenen der Datenverarbeitung notwendig ist. Die derzeitigen Regelungen garantieren keinen ausreichenden Schutz für Betroffene.

4. Eigenschaft der Datenempfänger und Weitergabe der PNR an Drittstaaten

Ebenso wie die Rechte der Betroffenen einer Klarstellung bedürfen, so ist auch die Eigenschaft der Datenempfänger (PNR-Zentralstellen und zuständige Behörden) in dem Vorschlag nicht eindeutig festgelegt. Die Zusammensetzung der PNR-Zentralstellen und die Befugnisse der Mitarbeiter bedürfen einer Spezifizierung.[92]

Weiterhin besteht Klärungsbedarf in Bezug auf die Weitergabe der PNR an Drittstaaten, da in dem Vorschlag nur unzureichend erläutert wird, wie auf Gegenanfragen nach PNR aus Staaten reagiert wird, die ein niedrigeres Datenschutzniveau aufweisen. Es wird keine Unterscheidung zwischen Staaten, die kein PNR-Austausch Abkommen mit der EU geschlossen haben, und solchen, mit denen bereits ein Abkommen besteht, getroffen, sondern auf die Bedingungen des Datenschutz-Rahmenbeschlusses 2008/977 aus dem Jahr 2008 für die ehemalige dritte Säule verwiesen, der jedoch weitreichende Ausnahmen von den Anforderungen der Angemessenheit macht.[93]

II. Perspektiven

Insgesamt betrachtet bestehen erhebliche Unsicherheiten im Hinblick auf den EU-PNR Vorschlag, die sich auf die Rechtmäßigkeit der geplanten Maßnahmen sowie auf den anwendbaren Datenschutzrahmen, die Stellung der Datenempfänger und die Weitergabe der PNR an Drittstaaten beziehen.

---

91 BVerfG, 1 BvR 256/08 vom 2. März 2010, Rn. 301.

92 EDSB Stellungnahme ABl. vom 22. Juni 2011, C-181/24, Punkt III.2., S. 27.

93 EDSB Stellungnahme ABl. vom 22. Juni 2011, C-181/24, Punkt III.4., S. 28. Ausnahmen sind zum Beispiel schon im Fall „überwiegender berechtigter Interessen, insbesondere wichtiger öffentlicher Interessen" vorgesehen Vergleiche Artikel 13 Abs. 3 lit. (ii) des Rahmenbschlusses 2008/977, ABl. 2008 vom 30. Dezember 2008, L-350/60.

Die Erstellung von Verhaltensmustern und Risikoanalysen auf europäischer Ebene führt zur Auswertung und Bearbeitung von Datenmengen in bisher nicht gekanntem Ausmaß. Auf der Suche nach potenziell gefährlichen Straftätern werden aus dem „Datenberg" tausende Daten anhand von festgelegten Merkmalen abgeglichen, miteinander verknüpft und in einen anderen Kontext gesetzt. Dabei kann die Analyse dieser ungeheuer großen Datenmenge leicht zu Unregelmäßigkeiten und Fehlern führen, die angesichts des Datenumfangs schwer nachzuvollziehen oder zu korrigieren sind.[94] Effektiven Rechtschutz in solch einem anonymen System zu erhalten erscheint fast unmöglich.

Die verdachtsunabhängige Katalogisierung und Einteilung der Flugpassagiere in Gruppen (Risikopassagier oder harmloser Reisender), je nach dem, welchen Verhaltensmustern und Kriterien sie entsprechen, erinnert bedauerlich an Methoden der Rasterfahndung, die im April 2006 vom Bundesverfassungsgericht für verfassungswidrig erklärt wurden.[95] Das Karlsruher Gericht stellte dazu schon 1983 in seinem Volkszählungsurteil fest, dass „eine umfassende Registrierung und Katalogisierung der Persönlichkeit durch die Zusammenführung einzelner Lebensdaten und Personaldaten zur Erstellung von Persönlichkeitsprofilen der Bürger" auch in der Anonymität statistischer Erhebungen unzulässig sei.[96] Daher stellt sich, zumindest in Deutschland, die Frage, wie die geplante „Massenanalyse" mit den deutschen Grundrechten vereinbar sein soll.

Das Problem der anwendbaren datenschutzrechtlichen Vorschriften lässt sich auch nicht durch einen Vergleich mit der Vorratsdatenspeicherungsrichtlinie beantworten. Die Frage, in welchem Umfang der Staat überhaupt private Akteure zur Mitarbeit verpflichten darf, kann nur in einer tiefergehenden Analyse beantwortet werden. Grundsätzlich muss es jedoch bei der Trennung zwischen privatwirtschaftlichen Tätigkeiten und staatlichen Strafverfolgungsaufgaben bleiben.

In diesem Zusammenhang stellt sich auch die Frage, welche und wie viele Lebensbereiche der Staat – auch über den Umweg Europa – insgesamt überwachen darf.[97] Tritt der EU-PNR Vorschlag in Kraft, ist neben den Telekommunikationsdaten auch das Reiseverhalten der Bürger betroffen. Hier bleibt zu bedenken, dass das Bundesverfassungsgericht im Vorratsdatenspeicherungsurteil vom März 2010 die grundsätzlich „verfassungsrechtliche Unbedenklichkeit" der Vorratsdatenspeicherung darauf stützt, dass diese eine Ausnahme im Rechtsstaat bleibt.[98] Das Gericht betonte insbesondere:

> *„Die Einführung der Telekommunikationsverkehrsdatenspeicherung kann damit nicht als Vorbild für die Schaffung weiterer vorsorglich anlassloser Datensammlungen dienen, sondern zwingt den Gesetzgeber bei der Erwägung neuer Speicherungspflichten oder -berechtigungen in Blick auf die Gesamtheit der verschiedenen schon vorhandenen Datensammlungen zu größerer Zurückhaltung. Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland. [...] Durch*

94 Zu Gefahr, die von großen Datensammlungen ausgeht, siehe: *Simitis*, Einleitung zum BDSG, S. 64-71, Rn. 5-26.

95 Bundesverfassungsgerichtsbeschluss vom 4. April 2006, 1 BvR 518/02.

96 BVerfGE 65, 1, Rn. 177.

97 Hierzu vergleiche: *Knierim*, ZD 1/2011, S. 17-23.

98 BVerfG, 1 BvR 256/08 vom 2. März 2010, Rn. 218; siehe auch *Roßnagel*, NJW 2010, S. 1238, insbesondere 1240.

> *eine vorsorgliche Speicherung der Telekommunikationsverkehrsdaten wird der Spielraum für weitere anlasslose Datensammlungen auch über den Weg der Europäischen Union erheblich geringer.*"[99]

Schlussendlich bleibt die Problematik der Rechtmäßigkeit des EU-PNR Vorschlags. Zum bisherigen Zeitpunkt verstößt er gegen den europäischen Grundrechtsstandard. In diesem Fall bleibt nur zu hoffen, dass Rat und Kommission die Bedenken des Europäischen Datenschutzbeauftragten und der Agentur der Europäischen Union für Grundrechte ernster nehmen als dies bisher geschehen ist. Aktuelle Änderungsvorschläge lassen leider auf das Gegenteil schließen. Einige Staaten und die Kommission wollen 4 Jahre nach Inkrafttreten der Richtlinie prüfen, ob die PNR Speicherung auch auf innereuropäische Flüge ausgeweitet werden kann.[100]

99 BVerfG, 1 BvR 256/08 vom 2. März 2010, Rn. 218.

100 Begründung, Punkt 5., S. 15 EU-PNR Vorschlag vom 2. Februar 2011.