Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Peter Schaar
Bundesbeauftragter für den Datenschutz
und die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit,
Postfach 20 01 12. 53131 Bonn

An den
Vorsitzenden des Innenausschusses
des Deutschen Bundestages
Herrn Sebastian Edathy
Platz der Republik 1
11011 Berlin

HAUSANSCHRIFT Husarenstraße 30, 53117 Bonn
POSTANSCHRIFT Postfach 20 01 12, 53131 Bonn

TEL +49 (0)228-81995-511
ODER +49 (0)1888-7799-511
FAX +49 (0)228-81995-550
ODER +49 (0)1888-7799-550
E-MAIL ref5@bfdi.bund.de
INTERNET www.bfdi.bund.de

DATUM Bonn, 02.11.2006

BETREFF **24. Sitzung des Innenausschusses des Deutschen Bundestages am 6. November 2006**
HIER Öffentliche Anhörung von Sachverständigen "Anti-Terror-Datei und Terrorismusbekämpfungs-ergänzungsgesetz"
BEZUG Schreiben des Sekretariats des Innenausschusses des Deutschen Bundestages vom 23. Oktober 2006
ANLAGE - 4 -

Sehr geehrter Herr Edathy,

anliegend übersende ich die mit Schreiben vom 23. Oktober 2006 (Bezug) erbetene Stellungnahme. Aufgrund der Eilbedürftigkeit erfolgt die Übersendung nur per E-Mail.

Mit freundlichen Grüßen
gez.

Schaar

Stellungnahme

des

Bundesbeauftragten für den Datenschutz

und die Informationsfreiheit

Öffentliche Anhörung
des Innenausschusses des Deutschen Bundestages
am 6. November 2006 in Berlin

„Anti-Terror-Datei und Terrorismusbekämpfungsergänzungsgesetz“

Vorbemerkung

Bei der 28. Internationalen Datenschutzkonferenz, die vom 2. bis 3. November in London stattfand, standen die Gefahren einer Überwachungsgesellschaft im Mittelpunkt. Nach Auffassung der Datenschutzbeauftragten aus mehr als 40 Ländern stellt die Reaktion der demokratischen Staaten auf die terroristischen Anschläge der letzten Jahre eine der größten Herausforderungen für den Datenschutz dar. Die für den Fortbestand demokratischer Verhältnisse unverzichtbare Balance zwischen Sicherheit und Freiheitsrechten gerät in Gefahr, wenn sich die Gesellschaften immer stärker in Richtung Überwachung entwickeln.

Eine vom britischen Datenschutzbeauftragten Richard Thomas in Auftrag gegebene Studie („Ein Bericht zur Überwachungsgesellschaft, http://www.privacyconference2006.co.uk/index.asp?PageID=10) zeigt auf, dass immer effektivere technische Überwachungsmöglichkeiten und ihr Einsatz im privaten wie im öffentlichen Sektor zusammen mit immer weiter gehenden Befugnissen der Sicherheitsbehörden weltweit den Weg in eine Überwachungsgesellschaft ebnen.

Noch können wir uns entscheiden, ob wir dem Weg in die Überwachungsgesellschaft weiter folgen wollen. Dabei muss ins Blickfeld geraten, dass die einzelnen jeweils plausibel begründbaren Maßnahmen in ihrer Gesamtheit für die Demokratie untragbare Konsequenzen haben können. Ich hoffe, dass die Gefahren dieser Entwicklung erkannt und die richtigen Konsequenzen gezogen werden.

Angesichts dieser generellen Tendenzen und der verfassungsrechtlichen Bedenken gegen die beiden hier zur Diskussion stehenden Gesetzentwürfe rege ich an, den Gesetzentwurf zur Einführung einer Antiterrordatei und den Entwurf des Terrorismusbekämpfungsergänzungsgesetzes gemäß den folgenden Anregungen grundlegend zu überarbeiten.

Zu den Gesetzentwürfen haben die Datenschutzbeauftragten des Bundes und der Länder auf ihrer 72. Konferenz in Naumburg am 26./27. Oktober 2006 die anliegenden Entschließungen verabschiedet, in denen sie auf verfassungsrechtliche Risiken der vorliegenden Gesetzentwürfe hinweisen. Die Stellungnahme gründet auf diesen Entschließungen.

I.

Entwurf eines Gesetzes zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz) – BT-Drs. 16/2950

Mit der Antiterrordatei (vgl. Artikel 1 Gemeinsame-Dateien-Gesetz) soll ein im Online-Verbund nutzbarer Datenpool geschaffen werden, in dem möglichst umfassend die Erkenntnisse von Polizei und Nachrichtendiensten im Bereich der Terrorismusbekämpfung zusammengeführt werden.

Ich verkenne nicht die zur Begründung des Gesetzentwurfs geltend gemachte hohe Bedrohung durch den internationalen Terrorismus. In ihrer Entschließung zur Antiterrordatei vom 27. Oktober 2006 hat die 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder dies zum Ausdruck gebracht und zugleich betont, dass jede Intensivierung der informationellen Zusammenarbeit zwischen Polizeibehörden und Nachrichtendiensten den verfassungsrechtlichen Vorgaben, insbesondere dem Recht auf informationelle Selbstbestimmung, dem Grundsatz der Verhältnismäßigkeit und dem - in einigen Landesverfassungen ausdrücklich genannten - Trennungsgebot von Polizei und Nachrichtendiensten entsprechen muss.

Die informationelle Zusammenarbeit von Polizei und Nachrichtendiensten steht unter dem Vorbehalt der Beachtung des Trennungsgebots. Angesichts der zunehmenden informationellen Verflechtung dieser Behörden bildet diese Zusammenarbeit den „Hauptanwendungsfall für das Trennungsgebot“ [Baumann, in: DVBL 2005, 798 (801)].
Das Trennungsgebot bestimmt die Grenzen der informationellen Zusammenarbeit zwischen den Sicherheitsbehörden, um zu verhindern, dass die organisatorische Trennung von Polizei und Verfassungsschutz durch wechselseitige Unterstützungs- und Hilfsmaßnahmen unterlaufen wird. Diese Ausstrahlwirkung des Trennungsgebots auf die informationelle Zusammenarbeit von Polizei und Nachrichtendiensten hat auch der Verfassungsgerichtshof des Freistaates Sachsen in seinem Urteil vom 21. Juli 2005 (Az. Vf. 67-II-04) betont (vgl. a.a.O., S. 17 ff). Danach ist das Gebot organisatorischer Trennung unvollständig, wenn es nicht zugleich eine Abgrenzung der Aufgaben von Polizei und Geheimdiensten beinhaltet (vgl. a.a.O., S. 18). Nur so kann nach Auffassung des Gerichts vermieden werden, dass die Nachrichtendienste im Rahmen ihrer Aufgabenerfüllung unter Einsatz nachrichtendienstlicher Mittel gewonnene Daten an die Polizei übermitteln und auf dieser Datengrundlage polizeiliche Maßnahmen auch in den Fällen angeordnet werden, in denen diese Daten durch polizeiliche Maßnahmen nicht hätten erhoben werden dürfen (vgl. a.a.O.). Andernfalls könnten rechtsstaatlich ausgeformte Handlungsschwellen für den Einsatz polizeilicher Mittel unterlaufen werden. Das Trennungsgebot verhindert somit nicht die, insbesondere zur

Terrorismusbekämpfung, notwendige Intensivierung der Zusammenarbeit der Sicherheitsbehörden. Es definiert lediglich die Grenzen dieser Zusammenarbeit.

Ausgehend von diesen Vorgaben beinhaltet der vorliegende Entwurf des Gemeinsame-Dateien-Gesetzes schwerwiegende verfassungs- und datenschutzrechtliche Risiken. Dies gilt im wesentlichen - insbesondere in der Zusammenschau - für folgende Regelungen des Antiterrordateigesetzes (ATDG), die erst im Nachgang zum Beschluss der am 4. September 2006 in Berlin durchgeführten Sonderkonferenz der Innenminister des Bundes und der Länder (181. IMK) in den Gesetzentwurf aufgenommen worden sind:

1. § 1 Abs. 2 ATDG

Durch diese Regelung wird der Kreis der an der Antiterrordatei beteiligten Behörden über die in § 1 Abs. 1 ATDG abschließend aufgelisteten (Zentral-)Stellen hinaus erheblich erweitert. Teilnahmeberechtigt sind demnach auch die Polizeivollzugsbehörden (nach fachkundiger Schätzung sind dies mehrere hundert Behörden in der Bundesrepublik Deutschland), soweit die in § 1 Abs. 2 Nr. 1 und 2 ATDG geregelten Voraussetzungen vorliegen. Diese Voraussetzungen begründen weder eine angemessene, noch eine sachgerechte Beschränkung der Teilnahmeberechtigung. Zudem ist das Vorliegen der in § 1 Abs. 1 Nr. 1 ATDG enthaltenen Voraussetzung „nicht nur im Einzelfall besonders zugewiesen“ durch entsprechende Organisationserlasse steuerbar.

Die Einbeziehung einer unbestimmten Vielzahl von Polizeivollzugsbehörden in den Kreis der an der Antiterrordatei teilnahmeberechtigten Behörden ist mit dem Verhältnismäßigkeitsgebot nicht zu vereinbaren. Insoweit ist zu berücksichtigen, dass in der Antiterrordatei auch sensible weiche, d.h. auf ungesicherten Erkenntnissen beruhende, personenbezogene Daten der Nachrichtendienste gespeichert werden müssen, die von den Diensten im Vorfeldbereich der Gefahrenabwehr auf der Grundlage bereichsspezifischer - im Vergleich zu polizeilichen Eingriffsnormen niedrigerer - Eingriffsschwellen erhoben worden sind. Infolge der im Vorfeldbereich bestehenden hohen Ambivalenz der potentiellen Bedeutung einzelner Verhaltensumstände [vgl. Bundesverfassungsgericht (BVerfG), 1 BvR 668/04 vom 27.07.2005, Rdn. 121] können die Nachrichtendienste auch Daten von Personen erheben, deren Verhalten nicht nur zum Erfassungszeitpunkt, sondern auch bei weiterer Beobachtung vollkommen legal ist. Insofern können auch unbescholtene, d.h. sich rechtmäßig verhaltende, Personen in den Focus der Nachrichtendienste geraten. Dies ist eine spezifische Folge der den Nachrichtendiensten gewährten Befugnis zur Datenerhebung im Vorfeldbereich. Durch die Regelung des § 1 Abs. 2 ATDG ständen auch diese Daten einer unbestimmten Vielzahl von Polizeivollzugsbehörden zur Verfügung.

2. § 2 Satz 1 Nr. 3 ATDG i.V.m. § 3 Abs. 1 Nr. 1 Buchstabe a und b ATDG

In der Antiterrordatei sollen auch von Kontaktpersonen nicht nur Grunddaten im Sinne des § 3 Abs. 1 Nr. 1 Buchstabe a ATDG, sondern unter den Voraussetzungen des § 3 Abs. 1 Nr. 1 Buchstabe b ATDG auch umfängliche erweiterte Grunddaten gespeichert werden. Hiergegen bestehen erhebliche (verfassungs-)rechtliche Bedenken.

Bereits die Speicherung von Grunddaten in der Antiterrordatei ist ein tiefgreifender Eingriff in das Recht der Betroffenen auf informationelle Selbstbestimmung mit potentiell weitreichenden Folgen.

Aufgrund der weit gefassten Legaldefinition des § 2 Satz 1 Nr. 3 ATDG sind die Nachrichtendienste verpflichtet, auch Kontaktpersonen zu speichern, bei denen nur tatsächliche Anhaltspunkte für eine Zuordnung zu den in § 2 Satz 1 Nr. 1 Buchstabe a ATDG oder § 2 Satz 1 Nr. 2 ATDG genannten Personen bestehen. Für das Vorliegen tatsächlicher Anhaltspunkte reichen bereits konkrete und in gewissem Umfang verdichtete Umstände als Tatsachenbasis für den Verdacht aus [(vgl. BVerfG 1 BvR 2226/94 vom 14.07.1999, Rdn. 279); BVerfGE 100, 313 (395)]. Aufgrund der hohen Prognoseunsicherheit im Vorfeldbereich (s.o. I. 1) können diese Anhaltspunkte Bestandteil eines legalen Verhaltens der Betroffenen sein. Die Speicherpflicht des § 2 Satz 1 Nr. 3 ATDG umfasst auch diese Daten, mit der Folge, dass die an der Antiterrordatei beteiligten Polizeibehörden auf die Grunddaten auch dieser Kontaktpersonen unmittelbaren Zugriff erhalten (vgl. § 5 Abs. 1 Satz 2 Nr. 1 Buchstabe a ATDG), obgleich sie diese Daten nach den für sie geltenden bereichsspezifischen Befugnisnormen gemäß den restriktiven Vorgaben des Bundesverfassungsgerichts selbst nicht hätten erheben dürfen. Nach der Entscheidung des Bundesverfassungsgerichts vom 25. April 2001 zum hamburgischen Gesetz über die Datenverarbeitung der Polizei (1 BvR 1104/92) ist der Begriff der Kontakt- und Begleitperson im Polizeirecht „restriktiv auszulegen“ (a.a.O., Rdn. 54). „Vorausgesetzt sind konkrete Tatsachen für einen objektiven Tatbezug und damit für eine Einbeziehung in den Handlungskomplex der Straftatenbegehung, insbesondere eine Verwicklung in den Hintergrund oder das Umfeld der Straftaten“ (a.a.O.).
Durch die generelle Verpflichtung der Nachrichtendienste zur Speicherung von auch nur auf tatsächlichen Anhaltspunkten beruhenden Kontaktpersonendaten in der Antiterrordatei wird diese verfassungsgerichtlich vorgegebene Datenerhebungsschwelle nicht gewahrt. Infolgedessen können auch Kontaktpersonendaten unbescholtener Personen, die die Nachrichtendienste im Gegensatz zu Polizeibehörden im Rahmen ihrer spezifischen gesetzlichen Aufgaben- und Befugniszuweisungen erheben dürfen, durch die Speicherung in der Antiterrordatei zur Kenntnis der Polizeibehörden gelangen und als Grundlage operativer polizeilicher Maßnahmen gegen die Betroffenen dienen.

Ausgehend von diesen Erwägungen wird die in der Entwurfsbegründung (vgl. S. 30) zur Erhebung personenbezogener Daten von Kontaktpersonen festgelegte Prämisse („Soweit für die Erhebung und Speicherung von Daten zu Kontaktpersonen aufgrund spezialgesetzlicher Ausprägungen des Verhältnismäßigkeitsgrundsatzes besondere Anforderungen gelten, sind diese auch im Falle der Speicherung in der Antiterrordatei zu beachten“) nicht durchgängig gewahrt.

Verfassungs- und datenschutzrechtlich bedenklich ist auch die in § 3 Abs. 1 Nr. 1 Buchstabe b ATGD vorgesehene Speicherung erweiterter Grunddaten von Kontaktpersonen durch die Nachrichtendienste. Im Eilfall dürfen die Polizeibehörden auch auf diese umfänglichen nachrichtendienstlichen Erkenntnisse unmittelbar zugreifen (vgl. § 5 Abs. 2 Satz 1 ATDG).
Die gemäß § 3 Abs. 1 Nr. 1 b ATDG notwendige Differenzierung (Speicherung erweiterer Grunddaten nur von Kontaktpersonen, „bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie von der Planung oder Begehung einer in § 2 Satz 1 Nr. 1 Buchstabe a genannten Straftat oder der Ausübung, Unterstützung oder Vorbereitung von rechtswidriger Gewalt im Sinne von § 2 Satz 1 Nr. 2 Kenntnis haben“) erscheint in der Praxis (trennscharf) nicht umsetzbar. Infolgedessen besteht die erhebliche Gefahr, dass auch erweiterte Daten zu Kontaktpersonen gespeichert werden, die über keine entsprechende Kenntnis im Sinne des § 3 Abs. 1 Nr. 1 Buchstabe b ATDG verfügen.

Zweifelhaft erscheint zudem, ob die bloße Kenntnis im Sinne des § 3 Abs. 1 Nr. 1 Buchstabe b ATDG die Speicherung erweiterter Grunddaten zu rechtfertigen vermag. Problematisch ist dies insbesondere in den Fällen, in denen eine Kontaktperson aufgrund eines spezifischen, z.B. familiären, Näheverhältnisses zur Bezugsperson Kenntnis von deren (potentieller) Unterstützungs- bzw. Vorbereitungshandlung hat, sich hiervon jedoch innerlich distanziert und ihre Kenntnis ausschließlich aufgrund dieses Näheverhältnisses nicht offenbaren möchte. Im Bereich des materiellen Strafrechts hat der Gesetzgeber einer vergleichbaren Interessenkollisionen durch das sog. Angehörigenprivileg (vgl. § 258 Abs. 6 Strafgesetzbuch – Straffreiheit trotz Strafvereitelung) Rechnung getragen. Insofern erscheint zumindest eine entsprechende Differenzierung im Rahmen des § 3 Abs. 1 Nr. 1 b ATDG erforderlich.

3. § 3 Abs. 1 Nr. 1 Buchstabe b, rr ATDG

Verfassungs- und datenschutzrechtlich kritisch zu bewerten ist auch die nach § 3 Abs. 1 Nr. 1 Buchstabe b, rr ATDG zulässige Speicherung von auf tatsächlichen Anhaltspunkten beruhenden zusammenfassenden besonderen Bemerkungen, ergänzenden Hinweisen und Bewertungen zu Grunddaten und erweiterten Grunddaten. Die Speicherung entsprechender Freitexte in der Antiterrordatei eröffnet den teilnehmenden Behörden die Mög-

lichkeit, eine Vielzahl auch weicher personenbezogener Daten (z.B. nicht überprüfte bzw. überprüfbare Hinweise und Vermutungen) ohne Bindung an hinreichend konkrete Festlegungen des Gesetzgebers in der Antiterrordatei zu erfassen.

II.

Entwurf eines Gesetzes zur Ergänzung des Terrorismusbekämpfungsgesetzes [Terrorismusbekämpfungsergänzungsgesetz (TBEG)] – BT-Drs. 16/2921

Ausweislich der Entwurfsbegründung (A. Allgemeiner Teil, S.1) setzt das TBEG die Erkenntnisse aus der Evaluierung des Terrorismusbekämpfungsgesetzes (TBG) um. Nach Auffassung der Bundesregierung bestätigt die Evaluierung die gesetzgeberische Entscheidung und rechtfertigt die Notwendigkeit zur Aufnahme neuer, über den Anwendungsbereich des TBG hinausgehender Bestimmungen (vgl. a.a.O.).

Diese Prämisse ist kritisch zu bewerten [vgl. Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) an den Innenausschuss des Deutschen Bundestages zum „Bericht der Bundesregierung zu den Auswirkungen der nach Artikel 22 Abs. 2 des Terrorismusbekämpfungsgesetzes befristeten Änderungen des BVerfSchG, MADG, BNDG, Artikel 10-Gesetzes, SÜG und des § 7 Abs. 2 BKAG“ (A-Drs. 16(4)71, Anlage 4)]. Der Evaluierungsbericht enthält wesentliche Defizite (vgl. a.a.O.) und ist auch aus diesem Grund keine wirksame Legitimationsgrundlage für das TBEG.

Zusätzlich zu dieser Kritik bestehen verfassungs- und datenschutzrechtliche Bedenken, insbesondere gegen folgende Entwurfsregelungen:

1. Artikel 1 Nr. 2 (§ 8a BVerfSchG [neu])

Gegenüber dem geltenden Recht (§ 8 Abs. 5 ff BVerfSchG) senkt diese Neuregelung die materiellen Anwendungsvoraussetzungen und Verfahrenssicherungen ab (vgl. auch Entwurfsbegründung S. 4 f). Legitimiert wird dies unter Hinweis auf den unterschiedlichen Eingriffsgehalt der Auskunftsbefugnisse (vgl. a.a.O.). Hierzu ist folgendes anzumerken:
Der Innenausschuss des Deutschen Bundestages hat in seinem Bericht zum TBG (BT-Drs. 14/7864 vom 13.12.2001) die Gleichwertigkeit der in § 8 Abs. 5 bis 8 BVerfSchG normierten Befugnisse in Bezug auf deren Eingriffsintensität durch die Feststellung dokumentiert, dass im Hinblick auf die Eingriffstiefe der Erhebungsbefugnisse (§ 8 Abs. 5 bis 8 BVerfSchG) zur Gewährleistung einer effektiven Kontrolle ein Maximum an Kontrolldichte erforderlich sei und dieses auf hohem Niveau vereinheitlicht werden müsse (a.a.O., S. 4). Die Ausführungen des Innenausschusses sind wortidentisch mit den

Ausführungen der Bundesregierung in dem von ihr vorgelegten Entwurf eines Gesetzes zur Terrorismusbekämpfung.
Mit den Regelungen der § 8 Abs. 5 bis 8 BVerfSchG sind den Nachrichtendiensten zusätzliche Befugnisse in besonders sensiblen Bereichen zugestanden worden (vgl. BT-Plenarprotokoll 201. Sitzung vom 15.11.2004, S. 19666). Angesichts der damit verbundenen „schwerwiegenden Eingriffsmöglichkeiten in Bürgerrechte“ (BT-Drs. 15/4694, S. 4) sind die bestehenden Verfahrenssicherungen weiterhin erforderlich und angemessen. Dies entspricht auch der (neueren) Rechtsprechung des Bundesverfassungsgerichts. Danach hängt die verfassungsrechtliche Beurteilung einer Informationserhebung auch davon ab, welche Schutzvorkehrungen (Verfahrenssicherungen) getroffen worden sind (vgl. BVerfG 1 BvR 2378/98, Rdn. 330). Namentlich die verfahrensmäßigen Sicherungen sind - neben dem Erfordernis einer normenklaren, bereichsspezifischen Regelung des Eingriffszwecks sowie der Wahrung des Übermaßverbots - zum Schutz der betroffenen Grundrechte entwickelte Vorkehrungen (vgl. BVerfG 1 BvF 3/92 vom 03.03.2004, Rdn. 158). Bereits im Volkszählungsurteil (BVerfGE 65, 1 ff.) hat das Bundesverfassungsgericht darauf hingewiesen, dass die Sicherung des Rechts auf informationelle Selbstbestimmung „besonderer Vorkehrungen für die Durchführung und Organisation der Datenerhebung und –verarbeitung“ (BVerfGE 65, 1(49)) bedarf.

Bei den aus der Sicht der Betroffenen „besonders gravierenden“ (19. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz (BfD), 17.1, S. 110) Datenerhebungsbefugnissen des § 8 Abs. 5 bis 8 BVerfSchG handelt es sich „im Grunde um polizeiliche Befugnisse“ (a.a.O.), da den Nachrichtendiensten „Mittel in die Hand“ [Garstka, schriftliche Stellungnahme anlässlich der öffentlichen Sachverständigenanhörung des Innenausschusses des Deutschen Bundestages zum TGB – siehe Protokoll der 78. Sitzung des Innenausschusses des Deutschen Bundestages vom 30. November 2001 (kurz: Prot. 78. Sitzung BT-IA), S. 185] gegeben worden sind, „die weit in den exekutiven Bereich hineinreichen, zumal Auskünfte von Finanzinstituten in der Regel eine Beziehung zu konkreten Straftaten haben dürften“ (Garstka, a.a.O.) und die Daten bei Vorliegen der Voraussetzungen ausschließlich an die Strafverfolgungsbehörden weitergegeben werden dürfen bzw. müssen [vgl. Entwurf eines Gesetzes zur Bekämpfung des internationalen Terrorismus, BT-Drs. 14/7386 (neu) vom 08.11.2001, Begründung zu § 8 Abs. 5 BVerfSchG, S. 39]. Durch die geltende Regelung des § 8 Abs. 5 bis 8 BVerfSchG sind die Befugnisse der Verfassungsschutzbehörden „wesentlich erweitert“ (Denninger, schriftliche Stellungnahme anlässlich der Sachverständigenanhörung des Innenausschusses des Deutschen Bundestages zum TBG, Prot. 78. Sitzung BT-IA, S. 188) worden, hin zu einem „präventiven funktionalen Fahndungsverbund“ (a.a.O.) im Bereich der Terrorismusbekämpfung, d.h. zu einem „Funktionsverbund der Sicherheitsorgane, (...) in welchem der § 20 BVerfSchG weniger als Schranke als vielmehr als verbindendes Scharnier fungiert.“ (a.a.O.).

Angesichts dessen sollten die in § 8 Abs. 5 ff BVerfSchG normierten materiellen Anwendungsvoraussetzungen und Verfahrenssicherungen uneingeschränkt fortbestehen.

2. Artikel 1 Nr. 4 Buchstabe b (§ 17 Abs. 3 BVerfSchG [neu])

Durch diese Neuregelung soll dem Bundesamt für Verfassungsschutz (BfV), dem Militärischen Abschirmdienst (MAD) und dem Bundesnachrichtendienst (BND) die Befugnis zur eigenständigen Ausschreibung von Personen und Sachen im nationalen polizeilichen Informationssystem (INPOL) sowie im Schengener Informationssystem (SIS) ermöglicht werden. Nach geltendem Recht (vgl. § 11 Abs. 2 BKAG) sind Nachrichtendienste auf INPOL nicht zugriffsberechtigt - weder lesend noch schreibend. Nach § 17 Abs. 2 BVerfSchG können Ersuchen um polizeiliche Beobachtung durch die Nachrichtendienste an die Bundespolizei gerichtet werden, die diese dann nach § 31 BPolG selbst ausschreibt.
§ 17 Abs. 3 BVerfSchG-E ermöglicht den Diensten eine eigenständige Ausschreibung in INPOL auf der Grundlage ihrer Erkenntnisse zwecks Eröffnung der Möglichkeit der Ausschreibung einer verdeckten Registrierung im SIS gemäß Art. 99 Abs. 3 SDÜ (vgl. Entwurfsbegründung, S. 12 f).

Kritisch zu hinterfragen ist bereits die Zielsetzung, den Nachrichtendiensten die Ausschreibung im SIS gemäß Art. 99 Abs. 3 SDÜ zu eröffnen. Unter dem Vorbehalt der Geltung nationalen Rechts legitimiert Art. 99 Abs. 3 SDÜ eine Ausschreibung im SIS zur Abwehr einer von dem Betroffenen ausgehenden erheblichen Gefährdung oder anderer erheblicher Gefahren. Ob eine derartige „erhebliche Gefahrenabwehr“ nach nationalem Recht unter den Aufgabenbereich der Nachrichtendienste subsumiert werden kann oder diese Form der Gefahrenabwehr vielmehr ausschließlich dem Zuständigkeitsbereich der Polizei zugeordnet werden muss, erscheint zumindest fraglich.
Das Vertragsgesetz zur Umsetzung des SDÜ enthielt bewusst keine entsprechende Regelung zugunsten der Nachrichtendienste, da die SIS-Ausschreibung ein polizeiliches Fahndungsinstrument ist.

In Bezug auf die Befugnis der Nachrichtendienste zur Ausschreibung in INPOL bestehen aufgrund des nach nationalem Recht zu beachtenden Trennungsgebots und im Hinblick auf die in § 8 Abs. 3 BVerfSchG normierten Restriktionen erhebliche datenschutzrechtliche Bedenken.

3. Artikel 3 Nr. 2 (§ 4a MADG [neu]); Artikel 4 Nr. 2 (§ 2a BNDG[neu])

Im Gegensatz zum geltenden Recht (vgl. § 10 Abs. 3 MADG; § 2 Abs. 1a BNDG) sollen die in § 8a BVerfSchG-E neu geregelten Auskunftsbefugnisse des BfV inhaltsgleich auf den MAD und BND übertragen werden.
Die Erforderlichkeit einer entsprechenden Befugniserweiterung zugunsten des MAD und BND ist auf der Grundlage des von der Bundesregierung vorgelegten Evaluierungsberichts zum TBG nicht überzeugend zu legitimieren und daher abzulehnen.

Ergänzende Ausführungen im Rahmen der mündlichen Anhörung bleiben vorbehalten.

Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26. bis 27. Oktober 2006 in Naumburg

Verfassungsrechtliche Grundsätze bei Antiterrordatei-Gesetz beachten

Mit dem Entwurf eines Gesetzes zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz-BT-Drs. 16/2950) – verschärft durch Forderungen aus dem Bundesrat - sollen in der Bundesrepublik Deutschland erstmals die rechtlichen Grundlagen für die Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten geschaffen werden. Von besonderer Bedeutung ist die beim Bundeskriminalamt zur Aufklärung und Bekämpfung des internationalen Terrorismus einzurichtende Antiterrordatei, in welcher umfangreiches Datenmaterial der beteiligten Sicherheitsbehörden zusammengeführt werden soll.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder verkennt nicht die zur Begründung des Gesetzentwurfs geltend gemachte hohe Bedrohung durch den internationalen Terrorismus und die Notwendigkeit zur Optimierung des Informationsaustauschs. Jede Intensivierung der informationellen Zusammenarbeit zwischen Polizeibehörden und Nachrichtendiensten muss jedoch den verfassungsrechtlichen Vorgaben, insbesondere dem Recht auf informationelle Selbstbestimmung, dem Grundsatz der Verhältnismäßigkeit und dem - in einigen Landesverfassungen ausdrücklich genannten - Trennungsgebot zwischen Polizei und Nachrichtendiensten entsprechen. Der vorliegende Entwurf zur Antiterrordatei enthält schwerwiegende verfassungs- und datenschutzrechtliche Risiken.

Insbesondere den folgenden brisanten Aspekten wird im Rahmen der anstehenden parlamentarischen Beratungen besondere Beachtung zu schenken sein:

- **Die Anti-Terror-Datei sieht gravierende Erweiterungen des Datenaustauschs vor. Deshalb ist zumindest eine weitergehende Präzisierung der zu erfassenden Personen erforderlich. Insoweit ist insbesondere zu berücksichtigen, dass die Nachrichtendienste in der Antiterrordatei auch Personen erfassen, bei denen nur auf weichen Informationen beruhende tatsächliche Anhaltspunkte für eine Zuordnung zum internationalen Terrorismus bestehen. Diese Anhaltspunkte können auf legalem Verhalten beruhen, mit der Folge, dass auch unbescholtene**

Personen in der Antiterrordatei erfasst werden und deren Daten allen zugriffsberechtigten Behörden zur Verfügung stehen. Dass im Bereich der Vorfeldermittlungen ein besonders hohes Risiko einer Fehlprognose besteht, ist auch bereits verfassungsgerichtlich festgestellt.

- **Die Definition der in der Datei zu erfassenden sog. Kontaktpersonen muss präzisiert werden und der Kreis der Betroffenen ist einzuschränken. Dies gilt insbesondere für solche Kontaktpersonen, gegen die keinerlei belastende Erkenntnisse vorliegen. Es muss sichergestellt werden, dass nicht bereits unverdächtige soziale Kontakte zu einer Erfassung von Personen aus dem Umfeld Verdächtigter führen.**

- **Die Aufnahme besonderer Bemerkungen, ergänzender Hinweise und Bewertungen in Freitextform eröffnet den am Verbund teilnehmenden Behörden die Möglichkeit, eine Vielzahl, auch weicher personenbezogener Informationen (z.B. nicht überprüfte Hinweise oder Vermutungen) ohne Bindung an hinreichend konkrete Festlegungen des Gesetzgebers in der Datei zu erfassen. Deshalb sollte darauf verzichtet werden.**

- **In diesem Zusammenhang ist auch der Zugriff von Polizeibehörden auf Vorfelderkenntnisse der Nachrichtendienste im Hinblick auf das Trennungsgebot kritisch zu hinterfragen. Besonders bedenklich erscheint dabei die Zulassung von Ausnahmen vom verfassungsrechtlichen Trennungsgebot in den sog. Eilfällen, in welchen den beteiligten Behörden ein unmittelbarer Online-Zugriff auf alle Daten gestattet wird.**

- **Die zugriffsberechtigten Sicherheitsbehörden sind nicht klar genug bezeichnet. Aufgrund der Speicherung auch höchst sensibler personenbezogener Vorfelddaten muss der Gesetzgeber aus rechtsstaatlichen Gründen selbst festlegen, welche Stellen zugriffsberechtigt sein sollen.**

- **Im Übrigen sind auch die bereits jetzt erkennbaren Tendenzen zu einer Erweiterung der Antiterrordatei über die Terrorismusbekämpfung hinaus nicht akzeptabel. Dies gilt insbesondere für die im Gesetzentwurf vorgesehene Nutzung der Datei im Rahmen der Strafverfolgung. Es darf nicht zu einer immer niedrigeren Eingriffsschwelle kommen.**

Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26. bis 27. Oktober 2006 in Naumburg

Verfassungsrechtliche Grundsätze bei Antiterrordatei-Gesetz beachten

Mit dem Entwurf eines Gesetzes zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz-BT-Drs. 16/2950) – verschärft durch Forderungen aus dem Bundesrat - sollen in der Bundesrepublik Deutschland erstmals die rechtlichen Grundlagen für die Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten geschaffen werden. Von besonderer Bedeutung ist die beim Bundeskriminalamt zur Aufklärung und Bekämpfung des internationalen Terrorismus einzurichtende Antiterrordatei, in welcher umfangreiches Datenmaterial der beteiligten Sicherheitsbehörden zusammengeführt werden soll.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder verkennt nicht die zur Begründung des Gesetzentwurfs geltend gemachte hohe Bedrohung durch den internationalen Terrorismus und die Notwendigkeit zur Optimierung des Informationsaustauschs. Jede Intensivierung der informationellen Zusammenarbeit zwischen Polizeibehörden und Nachrichtendiensten muss jedoch den verfassungsrechtlichen Vorgaben, insbesondere dem Recht auf informationelle Selbstbestimmung, dem Grundsatz der Verhältnismäßigkeit und dem - in einigen Landesverfassungen ausdrücklich genannten - Trennungsgebot zwischen Polizei und Nachrichtendiensten entsprechen. Der vorliegende Entwurf zur Antiterrordatei enthält schwerwiegende verfassungs- und datenschutzrechtliche Risiken.

Insbesondere den folgenden brisanten Aspekten wird im Rahmen der anstehenden parlamentarischen Beratungen besondere Beachtung zu schenken sein:

- **Die Anti-Terror-Datei sieht gravierende Erweiterungen des Datenaustauschs vor. Deshalb ist zumindest eine weitergehende Präzisierung der zu erfassenden Personen erforderlich. Insoweit ist insbesondere zu berücksichtigen, dass die Nachrichtendienste in der Antiterrordatei auch Personen erfassen, bei denen nur auf weichen Informationen beruhende tatsächliche Anhaltspunkte für eine Zuordnung zum internationalen Terrorismus bestehen. Diese Anhaltspunkte können auf legalem Verhalten beruhen, mit der Folge, dass auch unbescholtene**

Personen in der Antiterrordatei erfasst werden und deren Daten allen zugriffsberechtigten Behörden zur Verfügung stehen. Dass im Bereich der Vorfeldermittlungen ein besonders hohes Risiko einer Fehlprognose besteht, ist auch bereits verfassungsgerichtlich festgestellt.

- **Die Definition der in der Datei zu erfassenden sog. Kontaktpersonen muss präzisiert werden und der Kreis der Betroffenen ist einzuschränken. Dies gilt insbesondere für solche Kontaktpersonen, gegen die keinerlei belastende Erkenntnisse vorliegen. Es muss sichergestellt werden, dass nicht bereits unverdächtige soziale Kontakte zu einer Erfassung von Personen aus dem Umfeld Verdächtigter führen.**

- **Die Aufnahme besonderer Bemerkungen, ergänzender Hinweise und Bewertungen in Freitextform eröffnet den am Verbund teilnehmenden Behörden die Möglichkeit, eine Vielzahl, auch weicher personenbezogener Informationen (z.B. nicht überprüfte Hinweise oder Vermutungen) ohne Bindung an hinreichend konkrete Festlegungen des Gesetzgebers in der Datei zu erfassen. Deshalb sollte darauf verzichtet werden.**

- **In diesem Zusammenhang ist auch der Zugriff von Polizeibehörden auf Vorfelderkenntnisse der Nachrichtendienste im Hinblick auf das Trennungsgebot kritisch zu hinterfragen. Besonders bedenklich erscheint dabei die Zulassung von Ausnahmen vom verfassungsrechtlichen Trennungsgebot in den sog. Eilfällen, in welchen den beteiligten Behörden ein unmittelbarer Online-Zugriff auf alle Daten gestattet wird.**

- **Die zugriffsberechtigten Sicherheitsbehörden sind nicht klar genug bezeichnet. Aufgrund der Speicherung auch höchst sensibler personenbezogener Vorfelddaten muss der Gesetzgeber aus rechtsstaatlichen Gründen selbst festlegen, welche Stellen zugriffsberechtigt sein sollen.**

- **Im Übrigen sind auch die bereits jetzt erkennbaren Tendenzen zu einer Erweiterung der Antiterrordatei über die Terrorismusbekämpfung hinaus nicht akzeptabel. Dies gilt insbesondere für die im Gesetzentwurf vorgesehene Nutzung der Datei im Rahmen der Strafverfolgung. Es darf nicht zu einer immer niedrigeren Eingriffsschwelle kommen.**

Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26. bis 27. Oktober 2006 in Naumburg

Das Gewicht der Freiheit beim Kampf gegen den Terrorismus

Seit dem 11. September 2001 wandelt sich der Staat immer mehr zu einem Präventionsstaat, der sich nicht darauf beschränkt, Straftaten zu verfolgen und konkrete Gefahren abzuwehren. Der Staat verlagert seine Aktivitäten zunehmend in das Vorfeld der Gefahrenabwehr. Sicherheitsbehörden gehen der abstrakten Möglichkeit von noch nicht einmal geplanten Taten nach. Immer mehr Daten werden auf Vorrat gesammelt und damit eine Vielzahl unverdächtiger Menschen erfasst. Auch unbescholtene Bürgerinnen und Bürger werden als Risikofaktoren behandelt, ohne dass diese dafür Anlass gegeben haben. Dieses neue Verständnis von innerer Sicherheit führt zu gravierenden Einschränkungen der Freiheitsrechte. Beispiele sind die von der Europäischen Union beschlossene Speicherung der Telekommunikationsverkehrsdaten oder die im Jahr 2002 verfassungswidrig durchgeführten Rasterfahndungen.

In diesem Zusammenhang ist auch der "Entwurf eines Gesetzes zur Ergänzung des Terrorismusbekämpfungsgesetzes" kritisch zu bewerten. Die ursprünglich zur Terrorismusbekämpfung geschaffenen Befugnisse werden immer weiter ausgedehnt und nicht mehr nur auf Terrorverdächtige beschränkt.

Bei allen Gesetzen und Maßnahmen zur Terrorbekämpfung stellt sich die Frage nach deren Eignung und Verhältnismäßigkeit. Mehr Überwachung führt nicht automatisch zu mehr Sicherheit, aber stets zu weniger Freiheit. Es gibt keine absolute Sicherheit.

Die verfassungsrechtlich notwendige wissenschaftliche Evaluation der bisherigen Vorschriften zur Terrorismusbekämpfung durch eine unabhängige Stelle fehlt bislang. Der "Bericht der Bundesregierung zu den Auswirkungen des Terrorismusbekämpfungsgesetzes" ist keine vollwertige Evaluation der bisherigen Vorschriften. Damit steht sowohl die Notwendigkeit einer Verlängerung als auch die Erforderlichkeit der Schaffung neuer Befugnisse in Zweifel.

Zunehmende Befugnisse verlangen nach zusätzlichen Kontrollen. Daher ist es unerlässlich, einen angemessenen Ausgleich zwischen den Befugnissen der Sicherheitsbehörden und den Kompetenzen der Kontrollorgane zu schaffen. Insbesondere müssen die Handlungsmöglichkeiten der parlamentarischen Kontrollorgane entsprechend ausgestaltet sein.

Übersicht seit dem 11. September 2001 zur Bekämpfung des internationalen Terrorismus ergangener bzw. in Vorbereitung befindlicher wesentlicher Maßnahmen:

National

- 09.01.2002 Terrorismusbekämpfungsgesetz (TBG) – BGBl. I, S. 361
- 18.08.2002 Gesetz zur Verbesserung der Bekämpfung der Geldwäsche und der Bekämpfung der Finanzierung des Terrorismus – BGBl. I, S. 3105 (Maßnahmen des GWG sollen auch zur Aufdeckung der Finanzströme des Terrorismus genutzt werden)
- 11.01.2005 Luftsicherheitsgesetz – BGBl. I, S. 78 (Einführung einer Art personellen Sabotageschutzes für das Personal bei Einrichtungen, die dem Luftverkehr dienen)
- 09.2006 Entwurf eines Gesetzes zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz) – BT-Drs. 16/2950

  Entwurf eines Gesetzes zur Ergänzung des Terrorismusbekämpfungsgesetzes (Terrorismusbekämpfungsergänzungsgesetz) – BT-Drs. 16/2921
- 10.2006 Entwurf verschiedener Änderungen (AufenthG; FreizügG/EU; AZR-Durchführungsverordnung) infolge der ausländerrechtlichen Erkenntnisse zu den versuchten Kofferbombenanschlägen

International

- 28.02.2002 Beschluss des Rates der EU über die Errichtung von Eurojust
- 13.06.2002 Rahmenbeschluss über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten
- 25.11.2005 Vorschlag für einen Beschluss des Rates über den Zugang der für die innere Sicherheit zuständigen Behörden der Mitgliedstaaten und von Europol zum VISA-Informationssystem (VIS) für Datenabfragen u.a. zum Zweck der Aufdeckung terroristischer und sonstiger schwerwiegender Straftaten