**Ronellenfitsch**

# Datenschutzrechtliche Schranken bei der Terrorismusbekämpfung

I.

Eine häufig gebrauchte Formulierung des BVerfG lautet: „Das Grundgesetz ist eine wertgebundene Ordnung, die den **Schutz von Freiheit und Menschenwürde** als den obersten Zweck allen Rechts erkennt."[1] Diese Zwecksetzung **kollidiert** mit dem **„Grundrecht auf Sicherheit"**, das nicht ausdrücklich im Grundgesetz normiert ist. Ob es ein derartiges Grundrecht überhaupt gibt, ist zweifelhaft.[2] Aus dem staatlichen Gewaltmonopol und dem Wesen der Verfassungsstaatlichkeit, zu der sich das Grundgesetz bekennt, folgt aber jedenfalls ein Staatsziel der Sicherheitsgewährleistung im Sinne einer Pflicht des Staates zur Abwehr von Gewalttätigkeiten Dritter. In seiner Entscheidung über die Verfassungsbeschwerde von RAF-Häftlingen gegen das sog. Kontaktsperregesetz hat das BVerfG am 1. August 1978 ausgeführt: „Das menschliche Leben stellt innerhalb der grundgesetzlichen Ordnung einen Höchstwert dar. Demgemäß folgt aus Art. 2 Abs. 2 Satz 1 in Verbindung mit Art. 1 Abs. 1 Satz 2 GG die umfassende, im Hinblick auf den Wert des Lebens besonders ernst zu nehmende Pflicht des Staates, jedes menschliche Leben zu schützen, es vor allem vor rechtswidrigen Eingriffen von seiten anderer zu bewahren".[3] Die Kollision von Rechtsgütern mit Verfassungsrang ist im Wege der Abwägung aufzulösen.[4] Ob dabei die Denkfigur der praktischen Konkordanz, die rhetorische Formel, gerade unter den Vorzeichen terroristischer Bedrohungen müsse der Staat eine „Balance von Freiheit und Sicherheit" herstellen[5] oder die Forderung, der Widerstreit zwischen verfassungsrechtlich geschützten Belangen sei nach Maßgabe der grundgesetzlichen Werteordnung und unter Berücksichtigung der Einheit dieses grundlegenden Wertesys-

---

[1] BVerfGE 12, 45 (51); 33, 1 (10); 37, 57 (65). Hervorhebung durch Verf.

[2] Grundlegend *Isensee,* Das Grundrecht auf Sicherheit, 1983; *ders*., in: HStR V, 2. Aufl. 2000, § 115 Rn 115. Vgl. auch Art. 5 Abs. 1 Satz 1 EMRK.

[3] BVerfGE 49, 24 (53).

[4] BVerfGE 34,238 (240).

[5] *Schwarz,* Gutachterliche Stellungnahme im Rahmen der Anhörung zum Gesetzentwurf der Landesregierung zur Änderung des Gesetzes über das Landesamt für Verfassungsschutz und des Hessischen Ausführungsgesetzes zum Gesetz zu Art. 10 Grundgesetz – LT-Drs. 16/6963 – und zum Änderungsantrag der Fraktion BÜNDNIS 90/DIE GRÜNEN – LT-Drs. 16/7072 vom 11.05.2007, Ausschussvorlage INA/16/68, S. 6.

tems aufzuheben,[6] allzu hilfreich für die **konkrete Abwägung** sind, sei dahingestellt. Immerhin ist damit die Richtung der Abwägung umschrieben. Für planungsrechtlich geschulte Juristen gehört es zur methodischen Routine, die relevanten Abwägungsbelange zu sichten, zu gewichten und erst dann zu wägen. Einen Schritt in diese Richtung unternahm bereits die ehemalige Präsidentin des BVerfG *Limbach,* als sie auf dem 53. Deutschen Anwaltstag 2002[7] das Terrorismusbekämpfungsgesetz kritisch würdigte, sich dabei aber auf eine Verhältnismäßigkeitsprüfung zurückzog. Die folgenden Ausführungen beschränken sich auf den Teilaspekt des Datenschutzes.

II.

1. Die „German Angst" ist legendär. Technische Entwicklungssprünge schüren bei uns immer Ängste. Das galt auch für die Entwicklung der Großrechnertechnologie zu Beginn der 70er Jahre. Die Vorstellung vom „gläsernen Menschen" kam auf, als er noch reine Utopie war. Dennoch stieß die Datenerhebung nach dem Volkszählungsgesetz 1983 auf massiven Widerstand. Im Rechtsstreit um dieses Gesetz gelang dem BVerfG durch das Urteil vom 15. Dezember 1983[8] eine Befriedung, weil das Gericht die Gelegenheit nutzte, die **verfassungsrechtlichen Grundlagen des Datenschutzes** umfassend darzustellen. Mit der Kreation des Rechts auf „**informationelle Selbstbestimmung**", das die Befugnis des Einzelnen gewährleistet, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, verankerte das Gericht den Datenschutz als Grundrecht in der Verfassung. Darauf aufbauend entwickelte sich in Deutschland auf der Grundlage eines ausgefeilten Datenschutzrechts eine hohe Datenschutzkultur. Dies war **und ist** auch nötig. Seit 1983 hat sich das Datenumfeld gravierend verändert. Die **Informationsgesellschaft** ist Wirklichkeit geworden. In der Informationsgesellschaft besteht die Möglichkeit, automatisiert Informationen zu beschaffen und zu verarbeiten, um „**Profile**" zu erstellen (Kundenprofil, Wählerprofil, Täterprofil, Gesundheitsprofil, Bewegungsprofil), die in ihrer Verknüpfung ein genaues Persönlichkeitsbild abgeben. Die individuelle Privatheit wird dadurch praktisch aufgehoben. Der **Staat** beansprucht zunehmend die Berechtigung, solche Verknüpfungen vorzunehmen. Das müsste an sich den Widerstand gegen derartige Offenlegungstendenzen wieder aufleben lassen. Dem ist nicht so. In Zeiten des weltweiten Terrorismus ist offenbar das Sicher-

[6] BVerfGE 49, 24 (56).
[7] Ist die kollektive Sicherheit der Feind der individuellen Freiheit? 2002.
[8] BVerfGE 65, 1.

heitsbedürfnis so groß, dass man geneigt ist, **alle** Formen des Datenzugriffs zuzulassen.

2. Dem steht in der EU und in Deutschland das **Datenschutzrecht** entgegen. Auf **europäischer Ebene** ist an erster Stelle Art. 8 Grundrechtecharta zu nennen. Weiter ist zu erwähnen das Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention Nr. 109) vom 28. Januar 1981. Im **Primärrecht** der Europäischen Gemeinschaften findet sich eine explizite datenschutzrechtliche Regelung nur pro domo, nämlich Art. 286 EG, der durch die Verordnung (EG) Nr.45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr ergänzt wird. Im EU-Datenschutzrecht werden die drei Säulen[9], d.h. der Kompetenzbereich der Europäischen Gemeinschaften und die Bereiche der Gemeinsamen Außen- und Sicherheitspolitik (GASP) sowie die polizeiliche und justizielle Zusammenarbeit in Strafsachen (PJZS) streng getrennt. So gelten die auf Art. 95 EG gestützten Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[10] (DSRL) und die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation[11] (DSRL-EK)) nur für die erste Säule, also nicht für Tätigkeiten gemäß den Titeln V (Gemeinsame Außen- und Sicherheitspolitik) und VI (polizeiliche

---

[9] Hierzu *Epping*, in: Ipsen (Hrsg.), Völkerrecht, 5. Aufl., 2004, § 33 Rn 4.

[10] ABl. L 281 v. 23.11.1995, S. 31. Hierzu *Brühann,* in: Roßnagel, Handbuch des Datenschutzrechtes 2003, S. 131 ff. Vgl. auch Erster Bericht über die Durchführung der Datenschutzrichtlinie (EG/95/46), KOM (2003), 265 endg. V. 15.5.2003; Mitteilung der Kommission an das Europäische Parlament und den Rat, Stand des Arbeitsprogrammes für eine bessere Durchführung der Datenschutzrichtlinie, KOM (2007) 87 v.7.3.2007.

[11] ABl. L 201 v. 31.7.2002, S. 37. Vgl. auch Stellungnahme 4/2005 der Gruppe 29 zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (KOM (2005) 438 endgültig; 21.09.2005 Zuvor galt die RL 97/66/EG des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und des Schutzes der Privatsphäre im Bereich der Telekommunikation vom 15.12.1997ABl. L 24 vom 30.1.1998, S. 1.

und justizielle Zusammenarbeit in Strafsachen) EUV. Für die Terrorismusabwehr ist daher in erster Linie der Kommissionsentwurf für einen Rahmenbeschluss über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justizielle Zusammenarbeit in Strafsachen verarbeitet werden,[12] interessant, der sich noch im Gesetzgebungsverfahren befindet. Noch nicht verabschiedet ist auch der Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt[13]. Auf **nationaler Ebene** bilden die Rechtsgrundlage für das allgemeine Datenschutzrecht das Bundesdatenschutzgesetz i.d.F. der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 60) und die Datenschutzgesetze der Länder. Daneben gibt es eine kaum überschaubare Vielzahl **bereichsspezifischer** datenschutzrechtlicher Bestimmungen in den Rechtsbereichen der Gefahrenabwehr und der Geheimdienste, der Strafverfolgung, des Sozial- und Gesundheitswesens, des Schul- und Erziehungswesens, der Telekommunikation, der Statistik, des Melde- und Passwesens. Datenschutzrechtliche Bestimmungen finden sich weiter im Arbeits- und Beamtenrecht. Zu erwähnen ist schließlich noch das Steuerrecht. Soll der Datenschutz – möglichst geräuschlos – relativiert werden, bietet sich eine Korrektur der bereichsspezifischen Regelungen an. Jedoch sind auch dann die verfassungsrechtlichen Vorgaben zu berücksichtigen, die im allgemeinen Datenschutzrecht ihren Niederschlag gefunden haben.

2. Als einfachgesetzliche Ausformung des Grundrechts auf informationelle Selbstbestimmung normiert das allgemeine Datenschutzrecht eine Reihe von **Datenschutz-**

---

[12] KOM (2005) 475 endgültig. Der Schutz personenbezogener Daten im Rahmen der dritten Säule wurde bereits 1998 erörtert. Der vom Rat angenommene sog. „Wiener Aktionspan“ (ABl. C 19 v. 23.1.1999) enthielt einen Prüfungsauftrag. 2001 scheiterte die Annahme einer Entschließung über die Aufnahme von entsprechenden Datenschutzbestimmungen in Rechtsakte der dritten Säule (Arbeitsdokument des Rates 6316/2/01 REV 2 JAI 15). 2005 sprachen sich die Datenschutzstellen der Mitgliedstaaten der EU und der Europäische Datenschutzbeauftragte für ein neues Rechtsinstrumentarium für den Schutz personenbezogener Daten im Rahmen der Dritten Säule aus. Am 4.10.2005 nahm die Kommission diesen Vorschlag an und übermittelte ihn im Rahmen des Konsultationsverfahrens dem Europäischen Parlament und dem Rat der EU.

[13] KOM (2004) 835 endg. Zu den Aktivitäten der EU und der Gemeinschaften auf dem Gebiet des Datenschutzes, Neunter Jahresbericht der Art. 29 Datenschutzgruppe, 2006, S. 115 ff.

**grundsätzen**. So ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dies eine Rechtsvorschrift erlaubt oder anordnet oder der Betroffene hierzu ohne jeden Zweifel einwilligt (**Grundsatz des Erlaubnis- bzw. Einwilligungsvorbehalts**), [14] wenn dies für festgelegte, eindeutige und rechtmäßige Zwecke erfolgt (**Zweckbindungsgrundsatz**),[15] wenn dies zur rechtmäßigen Aufgabenerfüllung der datenverarbeitenden Stelle erforderlich ist (**Erforderlichkeitsgrundsatz**)[16] und wenn die Gestaltung und Auswahl von Datenverarbeitungssystemen am Ziel der Datenvermeidung und Datensparsamkeit ausgerichtet sind (**Grundsatz der „Datenaskese“**)[17] im Gegensatz zur erwünschten Informationsvielfalt. So bescheiden die Datenschutzgrundsätze sind, so hinderlich werden sie bei der Terrorismusbekämpfung empfunden.[18]

III.

1. Der Begriff **„Terrorismus“** ist umstritten. Das hängt damit zusammen, dass der Ausdruck „Terror“ negativ besetzt ist. Schon das lateinische Ursprungswort bezeichnete Gemütslagen, die durch Schrecken und Furcht geprägt sind. Die Ursachen für Schrecken und Furcht sind vielfältig. In der Regel wird Terror mit menschlichem Verhalten assoziiert. In den deutschen Sprachgebrauch gelangte 1794 „Terror“ aus dem Französischen, wo mit „Le Terreur“ die Schreckensherrschaft des revolutionären Konvents gemeint war. Diejenigen, die Terror ausüben, müssten eigentlich automatisch als „**Terroristen“** betrachtet werden. Dem ist aber nicht so. Mit „Terror“ können nämlich auch erstrebenswerte Ziele verfolgt werden. Wird ein Despot in Schrecken und Furcht versetzt, wird das im Allgemeinen begrüßt. Dann scheut man sich, von Terrorismus zu sprechen, um potentielle Freiheits- oder Widerstandskämpfer nicht terminologisch zu diskreditieren. Der „Gegenterror“ wird zur „humanitären Intervention“. „Terrorismus“ ist ein **polemischer Begriff,** der vielfach dazu dient, den politischen Gegner zu stigmatisieren und in seiner Rechtsstellung zu schmälern. Kein Wunder, dass eine völkerrechtlich allgemein anerkannte **Definition** des Terrorismus bislang noch nicht zu Stande gekommen ist,[19] obwohl sich zahlreiche internationale

---

[14] § 4 Abs. 1 BDSG.
[15] Art 6 Abs. 1 lit. b DatenschutzRL.
[16] §§ 13 Abs. 1, 14 Abs. 1, 15 Abs. 1 Nr.1, 16 Abs. 1 Nr.1 BDSG.
[17] § 3a BDSG. Kritisch *Bull,* Zweifelsfragen um die informationelle Selbstbestimmung – Datenschutz als Datenaskese?, NJW 2006, 1617ff.
[18] Vgl. *Nehm,* Ein Jahr danach. Gedanken zum 11. September 2001, NJW 2002, 2665 ff.
[19] Vgl. hierzu *Stein / von Butlar,* Völkerrecht,8. Aufl., 2005, S. 323 ff.

Übereinkommen speziell gegen terroristische Staaten und auf Unterdrückung des Terrorismus richten. Das Übereinkommen zur Bekämpfung der Finanzierung des Terrorismus von 1999[20] enthält in Art. 2 Abs.1 lit. b) sogar einen Definitionsversuch.[21] In der Folge wird der Einfachheit halber davon ausgegangen, dass terroristische Verhaltensweisen solche Taten sind, die sich gegen die Zivilbevölkerung richten, allgemein anerkannte Regeln missachten und geeignet sind, Schrecken und Angst zu verbreiten.

2. Der Terrorismus ist ein altes Phänomen. Seit jeher gab es terroristische Anschläge, wobei die jeweiligen Gegner als wahre Terroristen bezeichnet wurden. Wie erwähnt, wurde das Wort „Terror“ zunächst zur Bezeichnung gewaltsamer Regierungsmaßnahmen entlehnt. An den „Terreur“ gegen mögliche Konterrevolutionärer knüpfte der „Rote Terror“ unter *Lenin* und *Stalin* an. Staatsterroristische Methoden wandten die Nationalsozialisten und zahlreiche faschistische Systeme an. Nach dem Zweiten Weltkrieg kamen Terrornetze vor allem im Kalten Krieg zustande und wurden on den Supermächten zum Führen von Stellvertreterkriegen finanziert. Auch der Dschihadismus und der Krieg, der gegen ihn geführt wird, sind nicht neu. So war der Terrorismus in Israel nicht erst seit dem Anschlag auf das King-David-Hotel in Jerusalem im Jahr 1946 Alltag, ehe er sich gegen die USA als Schutzmacht Israels wendete und religiös verbrämt wurde. Anschläge auf die Botschaften der USA in Nairobi und Daressalam von 1998 hatten bereits verheerende Wirkung. In den USA wurde der erste Anschlag auf das World Trade Center heruntergespielt. Es war aber nur eine Frage der Zeit, bis Terroranschläge in den USA selbst Erfolg haben würden. Die Anschläge am 11. September 2001 verliehen dem Terrorismus nur eine neue Qualität, wenn man angesichts der Größe der angerichteten Schäden von einem Umschlag der Quantität in Qualität ausgeht. Von neuer Qualität waren unstreitig die öffentliche Wahrnehmung der Terrorismusgefahr und die Reaktionen der politischen Entschei-

---

[20] Convention for the Suppression of the Financing of Terrorism angenommen durch A/RES/ 54/109 v. 9.12.1999.

[21] „Any.. act intended to cause death or serious bodily injury to a civilian, or to any other person not taking active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act.”

dungsträger. Einen neuen Stellenwert erlangte die **Terrorismusbekämpfung**. Darum geht es im Kern, wenn vom „neuen“ Terrorismus die Rede ist.[22]

IV.

1. Nach dem 11. September 2001 wurde der Begriff **„Krieg gegen den Terrorismus“** (war on terrorism) geprägt. Gemeint ist eine kriegsähnliche Auseinandersetzung. Dass gegen die Terroristen, die sich selbst nicht an das Kriegsrecht halten, das ius in bello angewandt wird, ist damit nicht gesagt. Vielmehr sind **Terroristen** keine Kombattanten, sondern Kriminelle. Am gefährlichsten ist in diesem Zusammenhang die **islamistische Bedrohung**. Der Kampf gegen den terroristischen Islamismus wird gemeinhin als gemeinsames Anliegen jedenfalls der westlichen Verfassungsstaaten angesehen. Generell ist der Kampf gegen den internationalen Terrorismus jedoch eine Aufgabe der Staatengemeinschaft. Dem dienen zahlreiche Resolutionen der Generalversammlung der Vereinten Nationen, namentlich die Resolution A/RES/51/210 über Maßnahmen zur Beseitigung des internationalen Terrorismus und die dieser als Anlage beigefügte Erklärung zur Ergänzung der Erklärung von 1994 über Maßnahmen zur Beseitigung des internationalen Terrorismus, die Resolution A/RES/49/60 über Maßnahmen zur Beseitigung des internationalen Terrorismus und die dieser als Anlage angefügte Erklärung über Maßnahmen zur Beseitigung des internationalen Terrorismus. Zu erwähnen ist weiter[23]das Übereinkommen zur Bekämpfung von terroristischer Bombenanschläge.[24]

2. Als Reaktion auf die Anschläge vom 11. September 2001 wurde im Oktober 2001 das Gesetzespaket zur Terrorismusbekämpfung in den USA, der USA Patriot Act

---

[22] Zum “neuen” Terrorismus *Lutz*, in: Koch (Hrsg.), Terrorismus – Rechtsfragen der äußeren und inneren Sicherheit, Symposium für Hans Peter Bull und Helmut Rittstieg am 31.5.2002, 2002, S. 9 (18 ff.).

[23] Vgl. noch das Übereinkommen über die Verhütung, Verfolgung und Bestrafung von Straftaten gegen völkerrechtlich geschütze Personen einschließlich Diplomaten v. 14.12.1993; Internationales Übereinkommen gegen Geiselnahme v. 17.12. 1979; Übereinkommen über den physischen Schutz von Kernmaterial v. 3.3.1980; Protokoll zur Bekämpfung widerrechtlicher gewalttätiger Handlungen auf Flughäfen, die der internationalen Zivilluftfahrt dienen v. 24.2.1988; Übereinkommen zur Bekämpfung widerrechtlicher Handlungen gegen die Sicherheit der Seeschifffahrt v. 10,3,1988; Protokoll zur Bekämpfung widerrechtlicher Handlungen gegen die Sicherheit fester Plattformen, die sich auf dem Festlandsockel befinden v. 10.3.1988.

[24] Convention for the Suppression of Terrorist Bombing, angenommen A/RES/52/164 v. 15.12.1997.

(„Uniting an Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act) angenommen, von dessen befristeten Regelungen die meisten später permanenten Status erhielten. Auf der Grundlage des USA Patriot Acts sind **Datenzugriffe** möglich, die weit über das bei uns Erlaubte hinausgehen. Selbst daran hielt man sich nicht. Präsident *Bush* bestätigte, dass er in den Wochen nach dem 11. September 2001 den Geheimdienst NSA mit Abhöraktionen gegen terrorverdächtige Personen betraute, ohne dass eine gerichtliche Kontrolle der Abhörmaßnahmen erfolgte. Die NSA ist für Auslandüberwachung zuständig; das FBI im Inland untersteht der Kontrolle eines Sondergerichts. Durch einen geschickten Wechsel der Zuständigkeiten konnte so das Recht unterlaufen werden.

3. Inwieweit der Dschihad unmittelbar auf Deutschland und die europäischen Nachbarn zielt, lässt sich nicht sicher beurteilen,[25] da die Zielrichtung des Dschihad unklar ist. Bekämpft werden danach zunächst die Eindringlinge in das „Haus des Islam“. Offenbar soll aber darüber hinausgehend die westlich-christliche Gesellschaft generell in eine islamische Gesellschaftsordnung überführt werden. Zu diesem Zweck werden institutionalisierte Parallelgesellschaften in den westlichen Staaten aufgebaut. Zur räumlichen gesellt sich die ethnische virtuelle Verbindung. Das alles schafft auch in Europa eine Gefahrenlage. Der Terrorismus erfasst insbesondere die EU in ihrer Gesamtheit. Dementsprechend haben die Mitgliedstaaten des Europarats am 27. Januar 1977 das Europäische Übereinkommen zur Bekämpfung des Terrorismus[26] abgeschlossen und dieses durch Protokoll vom 15. Mai 2003[27] aktualisiert. Des Weiteren ist die Gemeinsame Außen- und Sicherheitspolitik der EU (Art. 11 ff. EUV) auf die Terrorismusbekämpfung ausgerichtet. Schwierigkeiten bereitet lediglich die Übertragung der für die EG geregelten Sanktionsmechanismen auf die EU, die der EuG im Falle der targeted sanctions

[25] Hierzu *Theveßen, Elmar,* „Terroralarm“. Deutschland und die islamische Bedrohung, 2005.
[26] SEV Nr. 90.
[27] SEV Nr. 190.

durch kühne Konstruktionen hergestellt hat.[28] Vor allem aber hat die EU hat auf den 11. September durch eine Befestigung der dritten Säule, d.h. der polizeilichen und politischen Zusammenarbeit der Mitgliedstaaten, reagiert. In diesen Zusammenhang gehören:[29] der Gemeinsame Standpunkt 2001/931/GASP des Rates über die Anwendung besonderer Maßnahmen zur Bekämpfung des Terrorismus[30] mit Durchführungsstandpunkt 2006/1011/GASP[31], die Rahmenbeschlüsse zur Terrorismusbekämpfung,[32] zum Europäischen Haftbefehl[33] und zum Einfrieren von Straftaterträgnissen,[34] die Errichtung von Eurojust[35], die Verordnung des Rates über spezifische Maßnahmen zur Terrorismusbekämpfung[36],die Verordnung (EG) Nr. 881/2002 des Rates über die Anwendung bestimmter spezifischer restriktiver Maßnahmen gegen bestimmte Personen und Organisationen, die mit Osama bin Laden, dem Al-Quaida-Netzwerk und den Taliban in Verbindung stehen[37] und die Ratsempfehlung über die Zusammenarbeit bei der Finanzierungsbekämpfung des Terrorismus.[38] Datenschutzrechtliche Relevanz erlangte in diesem Zusammenhang insbesondere das Abkommen zwischen der EU und der USA über die Ü-

---

[28] EuG, Urteil vom 21.9.2005 – T-306/01, EuZW 2005, 672 L –Ahmed Ali Yusuf ./. Rat und Kommission;- T 315/01, EuZW 2095, 672 L Yassin Abdulah Kadi ./. Rat und Kommission: Verknüpfung von Art. 308 EG mit Art. 3, Art. 11 EUV. Zu weitgehend *Tietje / Hamelmann,* Gezielte Finanzsanktionen der Vereinten Nationen im Spannungsverhältnis zum Gemeinschaftsrecht und zu Menschenrechten, EuG, BecksRS 2005,79726, JuS 2006, 299 ff. (300 f.).

[29] Vgl. *von Bubnoff*, Terrorismusbekämpfung – eine weltweite Herausforderung, NJW 2002, 2672 ff.

[30] Vom 27.12.2001; AB. L 344 v. 28.1.2001,S. 93. Hierzu EuGH, Rs. C-355/04 – Segi u. a. / Rat der EU, Königreich Spanien, Vereinigtes Königreich Großbritannien und Nordirland; 354/04 – Gestoras / wie vorstehend.

[31] Vom 21.12.2006, ABl. 379 v. 28.12.2006, S. 129.

[32] Rahmenbeschluss vom 13.6.2002, Ratsdokumente 14845/1/01.

[33] Rahmenbeschluss vom 13.6.2002, Ratsdokumente 14867/1/01.

[34] ABlEG 2001 Nr. L 182, S. 1.

[35] ABlEG 2002 Nr. L 61, S. 1.

[36] VO EG Nr. 2580/2001 vom 27.12.2001, ABl. 2001 L 344.

[37] I.d.F. der achtundsiebzigsten Änderungsverordnung (EG) Nr. 639/2007 v. 8. 6. 2007 (ABl. L 148 v. 9.6..2007, S. 5).

[38] Gemeinsamer Standpunkt des Rates vom 27.12.2001, ABlEG 2001 Nr. L, S. 90

bermittlung von Fluggastdaten von USA-Reisenden am US-Behörden vom 28. Mai 2004. Der entsprechende Ratsbeschluss wurde vom EuGH auf Klage des Europäischen Parlaments mit Urteil vom 30. Mai 2006 aufgehoben[39]. Die EU schloss nunmehr am 16. und 19. Oktober 2006 mit den USA ein neues internationales Abkommen über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records „PNR“) und deren Übermittlung durch die Fluggesellschaften an das United States Departement of Homeland Security zum Zwecke der Verbrechensbekämpfung ab.[40] Von großer Bedeutung ist schließlich der am 27. Mai 2005 in Prüm zwischen Belgien, Deutschland, Spanien, Frankreich, Luxemburg, den Niederlanden und Österreich geschlossene Vertrag über die Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration (**Prümer Vertrag)**,[41] der den Datenaustausch der Polizei- und Strafverfolgungsbehörden der beteiligten Staaten vorsieht. Diese Behörden können zugreifen auf DNA-Analysedateien, Datenbanken mit elektronischen gespeicherten Fingerabdrücken, elektronische Register mit Kraftfahrzeug- und Kraftfahrzeughalterdaten. Die Daten- und Informationsübermittlungen werden durch Nationale Kontaktstellen durchgeführt. Eingeschränkt wird der Datenaustausch durch bereichsspezifische datenschutzrechtliche Bestimmungen. Der Prümer - Vertrag soll einen Vorreiterrolle in Europa übernehmen. Nachdem Italien, Finnland, Portugal und Slowenien ihre Absicht erklärt hatten, dem Vertrag

---

[39] C-317/04 und C-318/04 („PNR“).

[40] ABl. L 298 v. 27.10.2006, S. 29. Hierzu *Volz*, Extraterritoriale Terrorismusbekämpfung, 2007.

[41] BGBl.2006 II S. 626. ferner Ausführungsgesetz - Prümer Vertrag v. 10.7.2006 (BGBl I S.1458). Hierzu *Schaar*, Datenschutz und Datenaustausch im Vertrag von Prüm, DuD 2006, 691ff.; *Weichert*, Wo liegt Prüm? Der polizeiliche Datenaustausch in der EU bekommt eine neue Dimension, https://www.datenschutzzentrum.de/polizei/0630329-Pruem.

beizutreten,[42] beschlossen die Justiz- und Innenminister der Mitgliedstaaten der EU am 15. Februar 2007, die Regelungen des Prümer Vertrags in den EU-Acquis zu überführen.[43] Diese genannten Maßnahmen tragen die Rechnung, dass die Terrorismusabwehr schwerpunktmäßig eine **Aufgabe der Mitgliedstaaten** ist. Ob Deutschland sich in einem nicht erklärten Krieg mit dem islamischen Terrorismus befindet oder nicht, ist zwar primär eine völkerrechtliche Frage. Die Befugnisse zur Bekämpfung der Terroristen ergeben sich aber aus deutschem Verfassungsrecht. Danach ist der förmliche Verteidigungsfall – oder auch nur Spannungsfall – nicht ausgerufen, so dass ein Einsatz der Streitkräfte grundsätzlich nicht in Betracht kommt. Die Terroristen sind daher mit **polizeilichen Mitteln** zu bekämpfen. Maßgeblich ist das Sicherheitsrecht.Nach den Anschlägen vom 11. September 2001 wurde durch einen Ausbau des **Sicherheitsrechts** reagiert. Am 4.12.2001 erging das Gesetz zur Änderung des Vereinsgesetzes.[44] Am 10.12. 2001 erging des Gesetz zur Finanzierung der Terrorbekämpfung.[45] Namentlich das zweite Sicherheitspaket vom damaligen Bundesinnenminister *Schily* wurde als Gesetz zur Bekämpfung des internationalen Terrorismus (**Terrorismusbekämpfungsgesetz)** vom 9. Januar 2002[46] geradezu durchgepeitscht[47]. Später folgten das Geldwäschebekämpfungsgesetz vom 8.6. 2002[48] und

---

[42] Antwort der Bundesregierung auf die Kleinen Anfrage der Abgeordneten *Christian Ahrendt* u.a. und der Fraktion der FDP „Prümer Vertrag und die europäische Integration“, BT-Druck16/3994.

[43] Heise online news v. 15.02.2007 www.heise.de/newsticker/melddung/85383/from/r. Vgl. auch ABlEG. C 71 v. 28.3.2007, S. 35

[44] BGBl. I S. 3319. Zuletzt geändert durch das 34. Strafrechtsänderungsgesetz vom 22.8.2002 (BGBl. I S. 3390) .

[45] BGBl. I S. 3436.

[46] BGBl. I S. 361.

[47] Das Gesetz wurde am 14.12.2001 vom Bundestag und bereits sechs Tage später am 20.12.2001 vom Bundesrat verabschiedet. Am 1.1.2002 wurde die Pressemitteilung auf der Homepage der Bundesregierung verbreitet, das Gesetz sei an diesem Tag in Kraft getreten. Zu diesem Zeitpunkt lag das Gesetz dem Bundespräsidenten noch zur Prüfung vor. Die Verkündung im Bundesgesetzblatt erfolgte am 11.1.2002.

[48] BGBl. I S. 3105.

das Vierunddreißigste Strafrechtsänderungsgesetz vom 22.8. 2002[49]. Der Errichtung einer Antiterrordatei diente das Gesetz zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame Dateien- Gesetz) vom 1.12. 2006. [50] Dass die Nachbesserung des Gesetzes zur Ergänzung des Terrorismusbekämpfungsgesetzes (Terrorismusbekämpfungsergänzungsgesetz) vom 5. Januar 2007[51] zu einer Konsolidierung geführt hat, ist kaum zu hoffen. Die Momentaufnahme ergibt: Bei dem in diesem Zusammenhang bedeutsamsten Terrorismusbekämpfungsgesetz[52] und dem Terrorismusbekämpfungsergänzungsgesetz handelt es sich um ein Artikelgesetze. Geändert wurden u.a. das Bundesverfassungsschutzgesetz,[53] das MAD-Gesetz[54] und das BND-Gesetz,[55] das BKA-Gesetz,[56] das Artikel 10-Gesetz,[57] das Sicherheitsüberprüfungsgesetz[58] und die Sicherheitsüberprüfungsfeststellungsverordnung,[59] das Bundesgrenzschutz-, nunmehr Bundespolizeigesetz,[60] das Gesetz zu dem Schengener Übereinkommen,[61]

---

[49] BGBl. I 3390. Zum Zeugnisverweigerungsrecht des abgeurteilten Mitglieds einer terroristischen Vereinigung nach § 55 Abs.1 StPO vgl. BGH, NStZ 2006, 509.

[50] BGBl. I S. 3409.

[51] BGBl. I S.2.

[52] *Rublack*, Terrorismusbekämpfungsgesetz: Neue Befugnisse für die Sicherheitsbehörden, DuD 2002, 202 ff.

[53] Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (BVerfSchG) v. 20.12.1990 (BGBl. I S. 2954), zuletzt geändert durch Gesetz v. 22.12.2006 (BGBl. I S. 3409).

[54] MADG v. 20.12.1990 (BGBl. I S. 2954, 2977), zuletzt geändert durch Art. 8 des Gesetzes v. 22.4.2005 (BGBl. I S. 1106).

[55] BNDG v. 20.12.1990 (BGBl. I S. 2954, 2979), geändert durch Art. 3 des Gesetzes v. 22.12.2005 (BGBl. I S. 3409).

[56] Bundeskriminalamtsgesetz v. 7.7.1997 (BGBl. I S.1690), zuletzt geändert durch Art. 22 des Gesetzes v. 21.6.2005 (BGBl. I S. 1818).

[57] Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10.Gesetz – G 10) v. 26.6.2001 (BGBl. I S.1254), zuletzt geändert durch 37. Strafrechtsänderungsgesetz v. 11.2.2005 (BGBl. I S. 239).

[58] SÜPG v. 20.4.1994 (BGBl. I S.867).

[59] SÜV v. 30.7.2003 (BGBl. I S. 1553), zuletzt geändert durch Art. 343 der Verordnung v. 31.10.2006 (BGBl. I S. 2407).

[60] Gesetz über die Bundespolizei (Bundespolizeigesetz- BPolG) v. 17.10 1994 (BGBl. I S. 2978), zuletzt geändert durch das Umbenennungsgesetz v. 21.6.2005 (BGBl. I S. 1818).

[61] Gesetz zu dem Schengener Übereinkommen vom 19.6.1990 betreffend den schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen v. 15.7.1993 (BGBl. II S.1010), zuletzt geändert durch Art. 11 Nr. 4 des Gesetzes v. 30.7.2004 (BGBl. I S. 1950).

das Vereinsgesetz[62] das Pass-[63] und Personalausweisgesetz,[64] das Zollverwaltungsgesetz[65], das Straßenverkehrsgesetz,[66] das Luftsicherheitsgesetz[67], eine Reihe ausländerrechtlicher Gesetze[68] und das Bundeszentralregistergesetz.[69] Zu erwähnen ist noch das Europäische Haftbefehlsgesetz,[70]das weit über die Terrorismusbekämpfung hinausgreift. Jüngste Errungenschaft mit einem geringen Beitrag zur Terrorismusbekämpfung ist das Gesetz zur Änderung des Zollfahndungsdienstgesetzes und anderer Gesetze vom 12. Juni 2007.[71] Auf der Agenda von Bundesinnenminister *Schäuble* stehen dem Vernehmen nach[72] Regelungen zur Rasterfahndung, zu Online-Durchsuchungen, zum allgemeinen polizeibehördlichen Zugriff auf die Melderegister, um nur die wichtigsten zu nennen..

V.

---

[62] VereinsG v. 5.8.1964 (BGBl I S 593), zuletzt geändert durch Art. 5 Abs. 2 des Gesetzes v.22.8.2002 (BGBl. I S. 3390).

[63] PassG v. 19.4.1986 (BGBl. I S.537), zuletzt geändert durch Art. 13 Gesetz v. 21.6.2005 (BGBl. I S. 1818).

[64] Gesetz über Personalausweise i.d.F. der Bek. v. 21.4.1986 (BGBl. I S.548), zuletzt geändert durch Art. 4 des Gesetzes v. 25.3.2002 (BGBl. I S.1186).

[65] ZollVwG v. 21.12.1992 (BGBl. I S. 2125, 1993 I S. 2493), zuletzt geändert durch Art. 31 des Gesetzes v. 21.6.2005 (BGBl. I S.1818).

[66] StVG idF der Bek. v. 5.3.2003 (BGBl. I S.310, 919), zuletzt geändert durch Art. 2 des Gesetzes v. 14.8.2006 (BGBl. I S.1958).

[67] LuftSiG v. 11.1.2005 (BGBl. I S.78), zuletzt geändert durch Art. 337 der Verordnung v. 31.10.2006 (BGBl. I S.2407).

[68] Nunmehr Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet (Aufenthaltsgesetz – AufenthG) v. 3.7.2004 (BGBl. IS. 1950), zuletzt geändert durch Gesetz v.14.3.2005 (BGBl. I S. 721); Gesetz über das Ausländerzentralregister (AZR-Gesetz) v. 2.9.1994 (BGBl. I S. 2265), zuletzt geändert durch Gesetz v. 14.3.2005 (BGBl. I S. 721); Asylverfahrensgesetz i.d.F. der Bek. v. 27.7.1993 (BGBl. I S. 1361), zuletzt geändert durch Gesetz v. 14.3.2005 (BGBl. I S. 721).

[69] Bundeszentralregistergesetz i.d.F. der Bek. v. 21.9.1984 (BGBl. I S. 1229; 1985 S. 195); zuletzt geändert durch Art. 7 des Gesetzes v. 15.6.2005 (BGBl., I S. 1626).

[70] EuHbG v. 20.7.2006 (BGBl. I S. 1537); *Böhm,* Das neue Europäische Haftbefehlsgesetz, NJW 2006, 2592 ff.; vgl. BVerfGE 113, 273 m. Anm. *Böhm,* NJW 2005, 2588; *Bosbach,* NStZ 2006, 104; *Hufeld,* JuS 2005, 865; *Knopp*, JR 2005, 448; *Schünemann*, StV 2005, 681; *Hillgruber*, JZ 2005, 838 ff.; OLG Karlsruhe, NJW 2007, 615, 617; 659; KG, NJW 2007, 3507. Zu weitgehend OLG Stuttgart, NJW 2007, 613 .

[71] BGBl. I S. 1037.

[72] Die vage Formulierung soll verhindern, dass dem Bundesinnenminister Vorschläge unterschoben werden, die er in dieser For gar nicht gemacht hat; vgl. *Schäuble*, in: BamS 15.7.2007, S.2f.

Ob all dies auf dem verfassungsrechtlichen Prüfstand besteht, ist fraglich.[73] Nahezu alle Änderungen sind datenschutzrechtlich relevant und erfordern eine sorgfältig Würdigung. In der Folge werden einige Themenkomplexe herausgegriffen und Gesichtspunkte angedeutet, die bei der verfassungsrechtlichen Abwägung zwischen Freiheitsrechten und Sicherheitsbelangen mit zu berücksichtigen sind.

1. Der Gesetzgeber hat den **Beobachtungsauftrag** des **Bundesamtes für Verfassungsschutz** und des **Militärischen Abschirmdienstes (MAD)** auf Bestrebungen erweitert, die gegen den Gedanken der Völkerverständigung, insbesondere gegen das friedliche Zusammenleben der Völker gerichtet sind.[74] Das Bundesamt für Verfassungsschutz ist auf die Beobachtung solcher Bestrebungen im Inland beschränkt. Der Beobachtungsauftrag des MAD erfasst solche Bestrebungen im In- und Ausland, die Personen ausgehen, welche im Geschäftsbereich des Bundesministeriums der Verteidigung tätig sind oder tätig sein sollen.[75] Die Befugnisse des für die Auslandüberwachung zuständigen **Bundesnachrichtensdienstes (BND)** waren im Übrigen schon durch das Urteil des BVerfG vom 14. Juli 1999 zurückgeschnitten worden.[76] Auch bislang durften gewaltbereiten Extremisten beobachtet werden. Die Erweiterung umschließt nunmehr das **Vorfeld** extremistischer Bestrebungen, das den Nährboden für den Terrorismus bilden kann. Es geht nicht mehr nur um Informationen über geplante und durchgeführte Gewaltanwendungen, sondern um **extremistische Auffassungen,** die bereits an der Schwelle des politisch Unkorrekten beginnen können. Dadurch drohen ausufernde Datensammlungen, die nichts mehr mit dem (islamischen) Terrorismus zu tun haben.[77] Nahezu gegen **alle Datenschutzgrundsätze** kann dann verstoßen werden. Zur Erfüllung seiner Aufgaben darf das Bundesamt für Verfassungsschutz im Einzelfall ferner unentgeltliche **Auskünfte** verlangen bei Ban-

---

[73] Vgl. HDSB, 35. Tätigkeitsbericht 2006, S. 36.

[74] § 3 Abs.1 Nr. 4 BVerfSchG; § 1 Abs.1 Satz 2 MADG. Bezugsnormen sind Art. 9 Abs. 2 und Art. 26 Abs. 1 GG. Im Sinne von Art. 9 Abs. 2 richten sich Vereinigungen gegen die Völkerverständigung, wenn durch sie nach Art. 26 Abs. 1 verbotene oder sonstige völkerrechtswidrige Tätigkeiten vergleichbaren Gewichts verfolgt werden. Kritik an fremden Staaten ist selbstverständlich zulässig. Nicht erfasst werden sollen räumlich und zeitlich begrenzte Sammlungen für bewaffnete Organisationen durch Privatpersonen (*Jarass,* in: Jarass / Pieroth, GG, 7. Aufl., 2004, Rn 3. Ob das BVerfSchG im Hinblick auf die Unterstützung terroristischer Vereinigungen so eng verstanden werden will, erscheint fraglich.

[75] § 1 Abs.1 Satz 1 MADG.

[76] BVerfGE 100, 313 mit Bespr. *Arndt*, NJW 2000, 47ff.

[77] *Rublack,* DuD 2002, 203.

ken über Konten, Konteninhaber und sonstige Berechtigte sowie weitere am Zahlungsverkehr Beteiligte, über Geldbewegungen und Geldanlagen bei Postdienstleistern über Namen, Anschriften, Postfächern und sonstige Umstände des Postverkehrs bei Telekommunikations- und Teledienstleistern, über Telekommunikationsverbindungsdaten und Teledienstesnutzungsdaten bei Luftfahrtunternehmen über Namen, Anschriften und über die „sonstigen Umstände des Luftverkehrs." Zwar sind die tatbestandlichen Voraussetzungen solcher Auskunftsverlangen recht eng: Es müssen tatsächliche Anhaltpunkte für schwerwiegende Gefahren für die im BVerfSchG genannten Schützgüter vorliegen bzw. die Voraussetzungen des G 10 gegeben sein. Die Aufklärungsmaßnahmen bewegen sich jedoch schwerpunktmäßig im Aufgabenbereich der allgemeinen Polizeibehörden, so dass die datenschutzrechtliche gebotene **Trennung zwischen Verfassungsschutz und Polizei** aufgeweicht wird und leicht doppelte Datenbestände angelegt (gespiegelt) werden, was mit dem **Grundsatz der Datensparsamkeit** kollidiert. Außerdem dürfte der Betroffene faktisch diskriminiert sein, wenn sich der Verfassungsschutz bei seinem Kreditinstitut über seine Konten und Transaktionen erkundigt, ohne dass ein strafrechtlicher Anfangsverdacht vorliegt. Schließlich bedeutet es einen Systembruch, wenn die Eingriffsbefugnisse des Bundesamts für Verfassungsschutz und der Verfassungsschutzämter der Länder im Anwendungsbereicht des G 10 nicht im G 10 geregelt sind. Entsprechendes gilt für die vergleichbaren Auskunftsberechtigung des MAD[78] und des BND, dem obendrein noch ein Zugriffsrecht auf die Geldverkehrdaten zusteht[79]. Auch das **Bundeskriminalamt** (BKA) wurde mit erweiterten Ermittlungsbefugnissen ausgestattet. Es kann nunmehr, „soweit es zur Erfüllung seiner Zentralstellenaufgabe erforderlich ist", **eigenständig**, d.h. unabhängig von den Länderpolizeien und damit letztlich im Widerspruch zur Zentralstellenfunktion, bei allen öffentlichen oder nichtöffentlichen Stellen Daten mittels Auskünften oder Anfragen erheben, um vorhandene Sachverhalte zu ergänzen oder sonst „zu Zwecken der Auswertung". Dadurch wird die Koordination mit den Landespolizeien umgangen und die Gefahr von Doppelerhebungen heraufbeschworen, die in der Praxis durch Datenabgleich gebändigt wird. Der Datenabgleich ermöglicht BKA und Landespolizeien aber den Zugriff auf Datenbestände, auf die sich ihre Aufgabenstellung gar nicht erstreckt. Das verstößt gegen den Grundsatz der Zweckbindung, ist aber immer noch nicht so weitgehend wie die

[78] § 9 Abs. 4 MADG.
[79] § 2 Abs. 1a BNDG.

ursprünglich vorgesehene „Initiativermittlungsbefugnis“ des BKA, die ohne Vorliegen eines strafrechtlichen Anfangsverdachts oder einer polizeilichen Gefahr Ermittlungen gegen bestimmte Personen zugelassen hätte.[80] So wären leicht sämtliche Muslime unter Terrorismusverdacht gestellt worden. Das Motto „Wehret den Anfängen“ ist gleichwohl immer noch Leitlinie des Bundesinnenministeriums, wie die Forderung von Minister *Schäuble* nach der Strafbarkeit von Vorbereitungshandlungen bei terroristischen Aktivitäten zeigt.[81] Dem setzen die Datenschützer das „Wehret den Anfängen“ des Überwachungsstaats entgegen.

2. Die akustische Wohnraumüberwachung („großer Lauschangriff“) wurde bereits mit Änderung von Art. 13 Abs. 3 GG im Jahr 1998[82] legalisiert. Einen Teil der darauf gestützten zur Bekämpfung der Organisierten Kriminalität vorgenommenen Änderungen der StPO wurde aber vom BVerfG mit **Urteil vom 3. März 2004** aufgehoben.[83] Mit Beschluss vom gleichen Tag übertrug das BVerfG seine Grundsätze auf die Telekommunikationsüberwachung nach dem Außenwirtschaftsgesetz.[84] Recht blauäugig fordert das BVerfG unter Berufung auf seine ständige Rechtsprechung einen (absolut) abhörsicheren „Kernbereich privater Lebensgestaltung“[85], lässt dagegen weitgehende Eingriffe in den mobilitätsgeprägten Lebensbereich zu[86]. Der Gesetzgeber ergänzte mit dem Gesetz zur Umsetzung des Urteils des BVerfG vom 3. März 2004 (akustische Wohnraumüberwachung) vom 24. Juni 2005 (BGBl. I S. 1841) die Ausgestaltung des Lauschangriffs entsprechend den verfassungsrechtlichen Vorgaben[87]. Mit Kammerbeschluss vom 11. Mai 2007 hat das BVerfG die Verfassungsmäßigkeit des neugefassten § 100c Abs. 1 StPO bestätigt.[88] Eine umfassende Regelung auf dem Gebiet der strafprozessualen heimlichen Ermittlungsmethoden ist bezweckt mit

---

[80] Vgl. n.v. Referentenentwurf des Bundesministeriums vom 12.10.2001: „§ 7 a Feststellung zureichender Anhaltspunkte für eine Straftat: Das BKA kann zur Feststellung, ob zureichende tatsächliche Anhaltspunkte für eine Straftat vorliegen, in den Fällen, in denen es für die Strafverfolgung nach § 4 Abs. 1 zuständig ist, personenbezogene Daten erheben sowie weitere Maßnahmen durchführen. Die Vorschriften der StPO über besondere Maßnahmen der Datenerhebung bleiben unberührt.“

[81] ZRP 2006, 71.

[82] Gesetz vom 26.3.1998 (BGBl. I S. 610).

[83] BVerfGE 109, 279.

[84] BVerfGE 110, 33.

[85] BVerfGE 109, 279 (313); Urteil vom 27.7.2005 –1 BvR 668/04.

[86] Vgl. hierzu *Ronellenfitsch,* Mobilität und Datensicherheit, SächsVBl. 2006, 101 ff.

[87] Vgl. auch BT-Drs 15/4533; BGH, NJW 2005, 3295.

[88] 2 BvR 543/06.

dem Gesetzentwurf der Bundesregierung zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 27.04.2007[89]. Hinsichtlich des absoluten Kernbereichs privater Lebensgestaltung hat sich der Kammerbeschluss vom 11. Mai 2007 eine Rückzugsmöglichkeit eröffnet, indem es eine positive Konkretisierungspflicht verneinte und auf die Kasuistik setzte.[90] Damit wird es möglich, unabhängig von der Wohnung private und öffentliche Bereiche zu unterscheiden, ohne gleich räumliche Tabuzonen zu errichten. Ich habe für Hessen eine entsprechende Konstruktion im Verfassungsschutzgesetz vorgeschlagen. § 32a Abs. 2 Zollfahndungsdienstgesetz in der Fassung vom 12. Juni 2007 enthält folgende Regelung: „Ist der Kernbereich privater Lebensgestaltung betroffen, ist die Maßnahme zu unterbrechen, sobald dies ohne Gefährdung der eingesetzten Person möglich ist“ (Stichwort: Der Beamte im Schlafzimmerschrank). „Aufzeichnungen über Vorgänge, die den Kernbereich privater Lebensgestaltung betreffen, sind unverzüglich zu löschen. Erkenntnisse über solche Vorgänge dürfen nicht verwertet werden. Die Tatsache der Erfassung der Daten und ihre Löschung ist zu dokumentieren.“ Die Terrorismusbekämpfung spielte bei der Argumentation des BVerfG keine Rolle, obwohl der „kleine Lauschangriff“ in Gestalt der Befugnis des Bundesamts für Verfassungsschutz zum Einsatz verdeckter technischer Mittel zum Schutz der bei einem Einsatz in Wohnungen tätigen Personen in das Sicherheitspaket zur Terrorismusbekämpfung eingefügt worden war[91]. Der Sachzusammenhang mit der Terrorismusbekämpfung war damals in der Tat fraglich, da bekanntlich ein Einschleusen von verdeckten Ermittlern in die Strukturen des islamistischen Terrors kaum möglich war. Mittlerweile sollte sich die Lage gebessert haben, da sich die einzelnen Terrorgruppen selbst bekriegen. Die Überwachung der Kommunikation bis in den Wohnbereich spielt dagegen bei der Terrorismusbekämpfung eine zentrale Rolle.[92] So ermittelten seit Mitte Juli 2002 die Polizeidirektion Heidelberg in Zusammenarbeit mit dem Landeskriminalamt, dem BKA und einer US-Polizeibehörde gegen ein Paar, das verdächtigt wurde, einen Anschlag auf eine US-Einrichtung in Heidelberg oder in der dortigen Innenstadt zu planen. Im September wurden bei der Wohnungsdurchsuchung des Paares Chemikalien und Bauteile ge-

---

[89] BT-Drs. 275/07.

[90] BVerfGE 6,32 (41), 389 (433); 27, 1 (6),344 (350f.);32, 373 (378 f.); 33, 367 (376 f.); 34, 238 (248); 80, 367 (374); 109, 279 (314).

[91] § 9 Abs.2 BVerfSchG.

[92] *Baldus*, Präventive Wohnraumüberwachung durch Verfassungsschutzbehörden der Länder, NVwZ 2003, 1289 ff.

funden, die zur Herstellung von Rohrbomben geeignet waren, ferner ein Bild von *Osama bin Laden* und auf den Dschihad bezogene Bücher. Die Ermittlungsakten wurden einer Richterin als Haftrichterin zugeleitet. Noch während der laufenden Ermittlungen erfuhr die Presse von der Verhaftung. Die Amtsrichterin geriet in Verdacht der Verletzung des Dienstgeheimnisses, da ihr der Reporter des „Spiegel“, der als erster vom Ermittlungsverfahren erfahren hatte, persönlich bekannt war. Die Überprüfung der Verbindungsdaten der von der Richterin benutzten Telekommunikationsanschlüsse des Amtsgerichts ergab keine Verbindungsaufnahme zu dem Reporter. Fünf Monate nach dem Vorfall ordnete das Landgericht die Durchsuchung der Wohnung und des Dienstzimmers sowie die Beschlagnahme ihrer Computer und von Einzelverbindungsnachweisen ihres Mobilfunks an. Rechtsmittel blieben ohne Erfolg, woraufhin die Richterin Verfassungsbeschwerde erhob. Das BVerfG gab der Verfassungsbeschwerde mit Urteil vom 2. März 2006 statt[93]. Nach Abschluss des Übertragungsvorgangs sei zwar das Fernmeldegeheimnis des Art. 10 Abs. 1 GG nicht mehr einschlägig, wohl aber gegebenenfalls Art. 13 Abs. 1 GG und das Grundrecht auf informationelle Selbstbestimmung, in das nur unter strenger Beachtung des Verhältnismäßigkeitsgrundsatzes eingegriffen werden dürfe. Der Fall belegt, zu welchen Auswüchsen die Terrorismusneurose führen kann.

3. Die Online Durchsuchung hatte bislang keine Ermächtigungsgrundlage. Als erste landesrechtliche Regelung sieht nunmehr § 5 Abs. 2 Nr. 11 Satz 1 3. Alt. i.V.m. § 7 des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen vom 20. Dezember 2006[94] vor: Heimliches Beobachten und sonstiges Aufklären des Internets, wie insbesondere die verdeckte Teilnahme an seinen Kommunikationsreinrichtungen bzw. die Suche nach ihnen, sowie der heimliche Zugriff auf informationstechnische Systeme auch mit dem Einsatz technischer Mittel. Soweit solche Maßahmen einen Eingriff in das Brief-, Post- und Fernmeldegeheimnis darstellen bzw. in Art und Schwere diesem gleichkommen, ist dieser nur unter den Voraussetzungen des Gesetzes zu Artikel 10 Grundgesetz zulässig. In der Gesetzesbegründung[95] heißt es hierzu: „Mit der Einfügung der neuen Nr. 11 wird das bisher schon zulässige nachrichtendienstliche Mittel des Eindringens in technische Kommunikationsbeziehungen durch Bild-, Ton- und Datenaufzeichnungen für den Bereich des Internets näher mo-

[93] 2 BvR 2099/04.
[94] GV NW 2006, S. 620.
[95] LT-Drs .14/2211, S. 17.

difiziert. Die zunehmende Kommunikationsverlagerung extremistischer Bestrebungen auf das Internet, insbesondere dessen verdeckte oder verschlüsselte Bereiche und die Cyber-Angriffe von Extremisten auf fremde Systeme macht eine wirksame Nachrichtenbeschaffung auch in diesem technischen Umfeld erforderlich. Hierzu soll zukünftig neben der Beobachtung der offenen Internetseiten auch die legendierte Teilnahme an Chats, Auktionen und Tauschbörsen, die Feststellung der Domaininhaber, die Überprüfung der Homepagezugriffe, das Auffinden verborgener Webseiten und der Zugriff auf gespeicherte Computerdaten ermöglicht werden. Während die Abfrage von Ix-Adressen beim Provider oder durch Telekommunikationsgesellschaften ermöglichte Mithören von Gesprächen im Art. G 10-Gesetz geregelt sind, bedarf es hinsichtlich der übrigen Maßnahmen zur offensiven Nutzung des Internets einer Präzisierung der schon bestehenden landesrechtlichen Vorschrift." Gegen diese Regelung wurden fünf Verfassungsbeschwerden erhoben, die beim BVerfG unter dem Az. 1 BvR 377/ 07 und 1 BvR 595/07 anhängig sind. Auf dem diesjährigen Hessischen Forum Datenschutz im Juni habe ich die Online Durchsuchung als datenschutzrechtliche Sauerei bezeichnet. Das war weniger verfassungsrechtlich gemeint als informationspolitisch. Auch von staatlicher Seite werden den Verbrauchern alle Arten technischer Geräte zu elektronischen Kommunikation schmackhaft gemacht und empfohlen, alles zu tun, um die Sicherheit des Kommunikationsvorgangs zu gewährleisten. Und dann dringt der Staat wie ein Einbrecher in den Kommunikationsvorgang ein, ohne dass die Betroffenen dies überhaupt bemerken. Er schreckt dabei nicht einmal davor zurück, den Telekommunikationsvorgang lückenlos zu erfassen. Gegenstand der Online Durchsuchung sollen „informationstechnische Systeme" sein. Auch wenn die Begründung zum Verfassungsschutzgesetz nur auf den Internetbezug abstellt, werden jegliche elektronische Systeme erfasst, mit denen Informationen verarbeitet werden. Dazu gehören Großrechner, PC, Notebooks, Kleinstrechner, ferner Digitaltelefone, digitale Anrufbeantworter, Mobiltelefone,[96] digitale Videorecorder, elektronische Sensoren (digitale Kamerasysteme, Mikrofone, Messfühler ), Funkmikrofone, Systeme zur Ortsfeststellung, Navigationseinrichtungen), smart Chips, RFID-Chips u. dgl.[97] Kurz: Der Gegenstand der Online Durchsuchungen ist nicht präzisiert und da-

[96] Zum Lauschprogramm für Mobiltelefone „Flexispy", BILD v.18.7.2007, S.7.

[97] Vgl. Mitteilung der Kommission der Europäischen Gemeinschaften an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss un den Ausschuss der Regionen zur Funkfrequenzkennzeichnung (RFID) in Europa:

mit uferlos. Auch die Mittel der Zugriffe sind nicht begrenzt. Nicht einmal durch Abschalten der Geräte kann man sich schützen, weil vielfach eine Fernaktivierung der Programme (z.B. Anschalten von Mikrofon und Kamera) durch die Überwachungsorgane möglich ist. Ob dies verhältnismäßig ist, darf bezweifelt werden.

4. Das Bundesamt für Verfassungsschutz und einige Landesverfassungsschutzbehörden dürfen zur Erfüllung ihrer Aufgaben technische Mittel zur Ermittlung des Standortes eines aktiv geschalteten Mobilfunkgeräts und zur Ermittlung der Geräte- und Kartennummer einsetzen[98]. Damit sind die für die Verkehrsabwicklung in den Mobilfunknetze gebräuchlichen Kennungen IMEI (International Mobile Equipment Identity = Gerätenummer) und IMSI (International Mobile Subscriber Identity = Nummer der SIM[99]-Karte ) gemeint. Vereinfachend spricht man generell vom **IMSI-Catcher,** dessen Messtechnik auch bei bloßem Stand-by-Betrieb die Ermittlung des Standorts einer Person und der von ihr verwendeten Geräte- und Kartennummer ermöglicht[100]. Das Anliegen ist datenschutzrechtlich durchaus legitim. Zur Vorbereitung und Begehung unterschiedlichster Straftaten werden auch moderne Kommunikationstechniken eingesetzt. Die Sicherheitsbehörden sind daher gezwungen, mit dem technischen Forstschritt Schritt zu halten. Benötig wird der IMSI-Catcher, wenn die Rufnummer nicht bekannt ist, weil der Betroffene sich ein Mobiltelefon von einem Unbekannten geliehen, die Chipkarte getauscht oder eine Karte unter falschen Personalien gekauft hat. Nur durch die Ermittlung der Bestandsdaten des genutzten Mobiltelefons wird dann eine Überwachung der Telekommunikation möglich. Das BVerfG hat denn auch die Verfassungsbeschwerde gegen § 100i StPO nicht zu Entscheidung angenommen.[101] Eine entsprechende schulmäßige Verhältnismäßigkeitsprüfung würde diesem Ergebnis auch hinsichtlich der Eingriffsbefugnisse der Verfassungsschutzbehörde bestätigen.[102] Der Verfassungsschutz dient legitimen Zielen mit

---

Schritte zu einem ordnungspolitischen Rahmen, KOM(2007)97 endg., Ratsdok 7544/07; ferner BT-Drs 197/07.

[98] § 9 Abs. 4 BVerfSchG § 5 Abs. 2 Hess LVerfSchGE.

[99] Subscriber Identity Module.

[100] Mit Hilfe des IMSI-Catchers kann ohne Mitwirkung des TK-Dienstanbieters die Rufnummer oder Gerätekennung eines Handys ermittelt werden. Der Inhaber der Geräte- bzw. Kartennummer wird dann über eine Anfrage beim TK-Dienstanbieter ermittelt.

[101] Beschl. vom 22.9.2006 – 2 BvR 1345/03-.

[102] So auch *Heckmann,* Schriftliche Stellungnahme zum Gesetzentwurf der Landesregierung für ein Gesetz zur Änderung des Gesetzes über das Landesamt für Verfassungsschutz und des hessischen Ausführungsgesetzes zum Gesetz zu Art. 10

Verfassungsrang (Art. 73 Nr. 10 GG). Der Einsatz des IMSI-Catchers ist zur Wahrnehmung der Aufgaben und Befugnisse der Verfassungsschutzbehörden geeignet, weil er die Zuordnung der Rufnummer zu dem von einer Zielperson benutzten Mobiltelefon als notwendige Voraussetzung für die später erfolgende Telekommunikationsüberwachung ermöglicht. Ein milderes Mittel mit dem gleichen Ergebnis ist nicht bekannt. Übermäßig ist der Eingriff in das Grundrecht auf informationelle Selbstbestimmung der unmittelbar Betroffenen nicht, wenn man das hohe Schutzgut der Sicherheit vor terroristischen Bedrohungen ins Feld führt. Die Eingriffsintensität bei dem mitbetroffenen Dritten ist nach Ansicht des BVerfG so gering,[103] dass auf deren Benachrichtigung verzichtet werden könne. So einfach darf man es sich m.E. indessen nicht machen. Die Risiken der IMSI-Catcher sind erheblich. Denn beim Einsatz des IMSI-Catchers werden die Daten des Kommunikationspartners zunächst ebenfalls abgefangen und der Inhalt der Gespräche zugänglich gemacht, da es auch möglich ist, die Verschlüsselung der Gespräche auszuschalten. Ferner simuliert der IMSI-Catcher eine Funkzelle mit starker Feldstärke, so dass sich alle Handys in einem bestimmten Umkreis nicht nur beim Provider als der eigentlichen Funkstelle, sondern auch beim IMSI-Catcher melden. Die so „eingefangenen" Telefon- und Gerätenummern können dann gespeichert und verarbeitet werden. Der erste Schritt in die **schrankenlose Telefonüberwachung** wäre getan. Faktisch muss jeder, der durch Aktivschaltung seines Mobilfunkgeräts erreichbar bleiben will, damit rechnen, dass sein gegenwärtiger Aufenthaltsort jederzeit ermittelt werden kann. Der sachliche und personelle Aufwand des Einsatzes von IMSI-Catcher ist obendrein so hoch, dass von der Möglichkeit selten Gebrauch gemacht werden wird. Hinzu kommen die leichten Umgehungsmöglichkeiten durch den häufigen Wechsel von Telefonen und SIM-Karten und den Gebrauch ausländischer SIM-Karten. Die **Verhältnismäßigkeit** des Eingriffs in die informationelle Selbstbestimmung ist m.E. nicht mehr gegeben.

5. Personen, die in sicherheitsrelevanten Aufgabenfeldern des Bundes und der Länder beschäftigt werden, unterliegen seit jeher einer **Sicherheitsüberprüfung**. Das Terrorismusbekämpfungsgesetz hat für den Zuständigkeitsbereich des Bundes eine einfache Sicherheitsüberprüfung (Ü 1) für sicherheitsempfindliche Tätigkeiten inner-

---

Grundgesetz, Drucksache 16/6936, vom 11.5.2007; Ausschussvorlage INA /16/68, S. 22ff. (27ff.).

[103] AaO Abs. 77

halb einer lebens- und verteidigungswichtigen Einrichtung eingeführt, um auf diese Weise vorbeugenden **Sabotageschutz** zu betreiben.[104] Da durch Terroraktionen gegen Daseinsvorsorgeeinrichtungen Lebens- und Gesundheitsgefahren großer Teile der Bevölkerung drohen[105], ist eine derartige Regelung erforderlich, geeignet und angemessen. Die Gegenstandsbereiche der Daseinsvorsorge stehen nicht von vornherein fest. Die Ermächtigung zu einer insoweit normergänzenden Rechtsverordnung in § 34 SÜG genügt aber den Anforderungen des Art. 80 GG.

6**.** Ähnlich wie die Sicherheitsüberprüfung zählt die **Rasterfahndung** schon lange zum Repertoire der Sicherheitsbehörden.[106] Die Rasterfahndung erfolgt durch die Übermittlung personenbezogener Daten bestimmter Personengruppen zum automatisierten Abgleich mit anderen Datenbeständen. Im September 2001 enthielten die Polizeigesetze der Bundesländer Ermächtigungsgrundlagen für solche Fahndungen. Nach dem 11.9.2001 liefen denn auch in allen Bundesländern Rasterfahndungen an, um „Schläfer" aufzufinden. Die Maßnahmen richteten sich insbesondere gegen Studenten technischer Fachrichtungen aus vorwiegend arabischen Herkunftsländern. Das Problem bestand nun darin, dass ein Teil der Polizeigesetze das Vorliegen einer gegenwärtigen Gefahr erforderten,[107] die nicht nachzuweisen war. In Hessen etwa wurde die Rasterfahndung gerichtlich kassiert[108], worauf das dortige Polizeigesetz dahingehend geändert wurde, dass **tatsächliche Anhaltspunkte** für die Erforderlichkeit der Rasterfahndung zur Verhütung erheblicher Straftaten genügen[109]. Die daraufhin wieder aufgenommenen Rasterfahndungen blieben gleichwohl weitgehend erfolglos. Das alles dürfte wohl mit dazu beigetragen haben, dass das BVerfG mit Beschluss vom 4. April 2006[110] die Anordnung einer Rasterfahndung in Nordrhein-Westfalen kassierte und eine präventive polizeiliche Rasterfahndung mit dem Grundrecht auf informationelle Selbstbestimmung nur für vereinbar erklärte, wenn eine

---

[104] § 1 Abs. 4 und 5 SÜG.
[105] BT-Drucks. 14/7386, S. 43.
[106] Ende der 1970er Jahre wurde im Wege der Rasterfahndung eine konspirative Wohnung der RAF entdeckt und ein Mitglied der RAF festgenommen. Das Bekanntwerden der Maßnahme führte dann dazu, dass sich die Täter auf sie eingespielt haben.
[107] § 47 Abs. 1 BerlASOG; § 46 Abs. 1 BbgPolG, § 44 Abs. 1 MVSOG; § 31 NWPolG.
[108] HDSB, 31. Tätigkeitsbericht 2002, S. 16 ff. Vgl. aber auch HessStGH, Urteil vom 12.12.2005 – P.St. 19/14 – NVwZ 2006, 685 = NJW 2006, 1951 (Ls.).
[109] § 26 HSOG; vgl. auch LT-Drs 15/3755.
[110] 1 BvR 518/02.; NJW 2006, 1939.

**konkrete Gefahr** für hochrangige Rechtsgüter besteht. Um im Thema zu bleiben: Nur die konkrete Gefahr terroristischer Anschläge legitimiert eine Rasterfahndung. Diese Rechtsprechung stieß auf Kritik in den eigenen Reihen. Im Schrifttum war von „Fessel für die wehrhafte Demokratie“[111] Die Rede. An Stelle einer konkreten Gefahr solle eine abstrakte Dauergefahr genügen.[112] Praktisch werden dadurch die Muslime gewissermaßen als latente Störer unter Generalverdacht gestellt. Denn der Fischzug der Rasterfahndung verspricht nur Ertrag, wenn das Netz engmaschig geknüpft ist. Wie Richterin Haas in ihrer abweichenden Meinung zutreffend betont, hängt die Eingriffsintensität vom jeweiligen Fahndungsraster ab.

7. Durch eine Änderung des Pass- und Personalausweisgesetzes wurde die Möglichkeit geschaffen, im Reisepass und Personalausweis neben Lichtbild und Unterschrift „weitere **biometrische Merkmale** von Fingern oder Händen oder Gesicht“ des Dokumenteninhabers aufzunehmen.[113] Die biometrischen Merkmale dürfen nur zur Überprüfung der **Echtheit** des Dokumentes und zur **Identitätsprüfung** des Dokumenteninhabers ausgelesen und verwendet werden[114]. Eine bundesweite Referenzdatei wurde auf Drängen von Datenschutzorganisationen nicht eingerichtet. Mit der Terrorismusbekämpfung hat diese Regelung unmittelbar nicht zu tun. Sie dient nur als Legitimation für die zur Verbesserung der Terrorismusbekämpfung vorgenommener Verschärfung des Ausländerrechts. Ob dies zur Terrorismusbekämpfung beiträgt, hat mein Hessischer Amtvorgänger angezweifelt, da die Fälschungssicherheit durch biometrische Merkmale kaum zu erhöhen sei. Als negative Begleiterscheinung monierte er, dass biometrische Merkmale stets Zusatzinformationen (z.B. Krankheitsindikatoren) enthielten[115]. Beides reicht jedoch m.E. nicht aus, um den Einsatz biometrischer Daten generell abzulehnen.

8. Eingriffe in die informationelle Selbstbestimmung von Ausländern reichen von der Befugnis des Bundesamtes für Migration und Flüchtlinge bzw. der Ausländerbehörden, Daten unter bestimmten Voraussetzungen an das Bundesamt für Verfassungsschutz zu übermitteln[116] über die Einführung gesonderter Ausweise mit biometri-

---

[111] *Bausback,* NJW 2006, 1922ff.
[112] VG Mainz, DuD 2002, 303 (305).
[113] § 4 Abs. 3 PassG; § 1 Abs. 4 PAG.
[114] § 16 Abs. 6 PassG; §3 Abs. 5 PAG.
[115] HDSB, 30. Tätigkeitsbericht, 2001, S. 21 f.
[116] § 18 Abs.1 a BVerfSchG,

schen Merkmalen,[117] und die Einführung der Regelanfrage bei Nachrichtendiensten und Sicherheitsbehörden vor der Erteilung eines Visums an terrorverdächtige Ausländer[118] bis zu einem erleichterten Zugriff der Nachrichtendienste auf die Datenbestände des Ausländerzentralregisters[119], das freiwillige Angaben über die Religionszugehörigkeit enthalten kann[120]. Über die Effektivität solcher Maßnahmen kann nur spekuliert werden. **Generell** dürften die gesetzlichen Eingriffsmöglichkeiten in die informationelle Selbstbestimmung der Ausländer verhältnismäßig sein. Der Datenschutz muss sich beim Gesetzesvollzug bewähren.

**9 Neben** den mit dem Terrorismusbekämpfungsgesetz gezielt eingeführten Maßnahmen gibt es noch zahlreiche datenschutzrechtlich relevante Maßnahmen wie die Videoüberwachung,[121] die zur Gefahrenabwehr eingesetzt werden können. Ob die geschilderten Maßnahmen zur effektiven Terrorismusbekämpfung ausreichen, wird die Zukunft zeigen. Den nach Perfektion strebenden, für die öffentliche Sicherheit verantwortlichen Organen reichen die polizeilichen Instrumentarien – aus ihrer Perspektive – verständlich, niemals aus. So fordert Minister *Schäuble* in dem erwähnten Verfassungsschutzbericht die Einrichtung einer gemeinsamen Terrorismusdatei der Sicherheitsbehörden[122] und Erweiterungen der Befugnisse des Bundeskriminalamts[123]. Die Erforderlichkeit ist jedoch **nicht** dargetan.

VI.

Die Bundesrepublik Deutschland und der europäische Staatenverbund sind Freiheitsordnungen. Freiheit erfordert Garantien vor hoheitlichen Eingriffen, aber zugleich Sicherheit und Schutz vor Eingriffen Dritter. Vor allem mit Blick auf den internationalen Terrorismus steht in jüngster Zeit der Sicherheitsaspekt im Vordergrund. Weltweit und auch in Europa hat sich die Sicherheitslage verändert. Für die Bekämpfung des

---

[117] § 49 Abs. 4 AufenthG.
[118] § 73 Abs. 3 i.V.m. § 5 Abs. 4 AufenthG.
[119] § 22 AZRG.
[120] § 3 Nr. 5 AZRG
[121] Zur Video-Überwachung als Personen- und Objektschutzmaßnahme OVG Rheinland-Pfalz, Urteil vom 8.12.2005 – 12 A 1095/04 -, NJW 2006, 1830.
[122] Vgl. Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz – ATDG) v.22.12.2006 (BGBl. I S.3409. Hiergegen wurde Verfassungsbeschwerde eingelegt (BvR 1215/07).
[123] FAZ 119/23.5.2006, S. 1.

Terrorismus wird der Datenschutz als Problem empfunden. Das Problem darf nicht zum **Dilemma** werden, bei dem wir zwischen zwei Übeln entscheiden müssen: Entweder Preisgabe des Datenschutzes oder Hinnahme terroristischer Anschläge.

Bei der Abwehr des islamischen Terrorismus, im Krieg gegen den Terrorismus, geht es um den Erhalt unserer freiheitlichen Rechtsordnung, zu der als wesentlicher Gesichtspunkt die informationelle Selbstbestimmung zählt. Vorhandene Daten wecken die Begehrlichkeit nach Datenzugriff. Sind Zugriffsmöglichkeiten einmal geschaffen, verselbständigen sie sich leicht gegenüber ihrem ursprünglichen Zweck. Das gilt insbesondere, wenn der Datenschutz zugunsten der Terrorismusbekämpfung abgebaut wird. Der Begriff des Terrorismus ist so unbestimmt, dass einem schnell das Etikett des Terroristen angehängt ist. Die Instrumentarien, die gegen Dschihadisten eingesetzt werden, eignen sich auch gegen andere Gegner und Feinde der jeweiligen Machthaber. Wenn wir im Krieg gegen den Terrorismus überzogene Freiheitseingriffe vornehmen, haben die Terroristen ihr Ziel erreicht. Im elektronischen Spitzelstaat schlägt die Terrorismusabwehr in Staatsterror um. Staatsterror nach innen ist niemals gerechtfertigt. Auch im Krieg gegen den internationalen Terrorismus ist er bedenklich. Ein Feind, der sich an keine Regeln hält, muss gleichwohl regelgerecht zur Strecke gebracht werden. Die Mission für Freiheit und Demokratie, die eine Aufgabe aller zivilisierter Staaten ist, und die wir nicht allein den USA überlassen dürfen, schlägt fehl, wenn wir versuchen, im Kampf gegen Terroristen diese mit ihren eigenen Waffen zu schlagen. Die Jagd der Terroristen muss wie jede Jagd rechtlich geregelt erfolgen, auch wenn sich die Gejagten an keine Regeln halten. **Fazit:** Der Slogan „Datenschutz **oder** Terrorismus“ ist verfehlt. Auch im Krieg gegen den Terrorismus sind die Datenschutzgrundsätze zu beachten und können beachtet werden, ohne das Ziel zu gefährden, die freiheitliche und demokratische Staatsordnung zu erhalten.