DVD Deutsche Vereinigung für Datenschutz e. V.

Bonner Talweg 33-35
53113 Bonn

Telefon: 0228/22 24 98
Telefax: 0228/24 38 470

dvd@datenschutzverein.de
www.datenschutzverein.de

Bonn, den 6.November 2006

Stellungnahme

anlässlich der öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages am 6. November 2006 zu den Bundestagsdrucksachen 16/2950 (Entwurf Gemeinsame– Dateien- Gesetz) und 16/2921 (Entwurf Terrorismusbekämpfungsergänzungsgesetz) u.a..

I. Das **Terrorismusbekämpfungsergänzungsgesetz** schreibt im Wesentlichen mit dem Terrorismusbekämpfungsgesetz begonnene Fehlentwicklungen fort:

1. Im Widerspruch zu Art. 22 Terrorismusbekämpfungsgesetz wurde eine **Evaluation** zentraler neu eingeführter behördlicher Befugnisse gerade verzichtet. Der Bericht der Bundesregierung zu den Auswirkungen der mit dem Terrorismusbekämpfungsgesetz befristeten Änderungen verschiedener Sicherheitsgesetze untertrifft die an eine seriöse Evaluation zu stellenden Bedingungen. Nicht unwesentliche empirische Daten werden der Öffentlichkeit vorenthalten, in der Regel lediglich behördliche statistische Daten einer quantitativen Bewertung zugeführt und eine qualitative Bewertung von Umfang und Erfolg der zu bewertenden Maßnahmen in der Regel unterlassen. Der Beobachtungszeitraum des Mitte 2006 vorgelegten Berichts endet bereits mit dem Jahr 2004. Eine unabhängige wissenschaftliche Bewertung der gesammelten Daten ist unterblieben, obwohl in den letzten Jahren zwei wissenschaftliche Evaluationsprojekte im Bereich des Strafverfahrensrechts mit Erfolg und hohem Erkenntnisgewinn durchgeführt worden sind. Die Behauptung, dass die Fortschreibung von Maßnahmen nach dem Terrorismusbekämpfungsgesetz die notwendige Fortschreibung einer Erfolgsgeschichte sei, ist und bleibt mit der von der Bundesregierung betriebenen Evaluation nicht belegbar.

Die nunmehr in den Entwürfen vorgesehene **erneute Befristung und die Aufwertung der Evaluation** zielen auf eine Korrektur der bisherigen Regierungspraxis. Dagegen ist nichts einzuwenden, hätte doch schon das Terrorismusbekämpfungsgesetz 2002 einer qualifizierten Evaluation dringend bedurft. Um sicherzustellen, dass eine unabhängige wissenschaftliche Evaluation auf die gebotene Kooperationsbereitschaft der Behörden trifft, sollte aber insoweit **nachgebessert und eine Kooperationspflicht der Behörden** festgeschrieben werden.

2. Die **Erweiterung der Anfragebefugnisse der Nachrichtendienste** gegenüber Finanz-, Post-, Luftfahrt- und Telekommunikationsdienstleistern schreibt die mit dem Terrorismusbekämpfungsgesetz eingeschlagene Linie fort und stellt Datenspuren des Alltags zu erneut erleichterten Bedingungen den Nachrichtendiensten zur Verfügung. Wie im Gesetzgebungsverfahren zum Terrorismusbekämpfungsgesetz ausführlich erörtert handelt es sich dabei nicht um belanglose Eingriffe, sondern um Daten von potentiell hohem Erkenntnisgewinn und entsprechender Sensibilität. Der teilweise Wegfall der Kontrollkompetenzen der G10-Kommission, die blankettartige Beschreibung des betroffnen Personenkreises (§ 8 a Abs. 2 S. 2 Nr. 1 und 2 BVerfSchG) und schließlich das durch zahlreiche Querverweise und Bezugnahmen zunehmend unlesbar werdende Regelungsgeflecht entziehen den praktischen Gebrauch der erweiterten Befugnisse sowohl der parlamentarischen als auch der justiziellen Kontrolle sowie der Kalkulierbarkeit für potentiell Betroffene. Die Erweiterung des Zweckprogramms dieser Befugnisse auf sog. einfachen Extremismus mit Gewaltbezug lassen die Terrorismusbekämpfung hinter sich und überführt befristete Sondermaßnahmen nach dem 11. September 2001 in das Standardarsenal der Nachrichtendienste.

3. Daneben setzt sich die neu hinzutretende Indienststellung des originär polizeilichen Schengener Informationssystems (SIS) für gezielte **europaweite nachrichtendienstliche Registrierungen** (§ 17 Abs. 3 BVerfSchG [neu]) dem Einwand der Gemeinschaftsrechtswidrigkeit aus, da nur Gefahrenabwehr im polizeirechtlichen Sinne vom Wortlaut des Art. 99 SDÜ erfasst wird. Wie wenig Sensibilität für die Abgrenzung von Polizei und Geheimdiensten in dem Entwurf des Terrorismusbekämpfungsergänzungsgesetz überhaupt noch vorausgesetzt werden kann, wird schließlich daran erkennbar, dass nach der Entwurfsbegründung für eine SIS- Ausschreibung durch das Bundesamt für Verfassungsschutz zwingend auch eine Ausschreibung im nationalen polizeilichen Informationssystem INPOL sein soll. Dies mag technisch zutreffen, legitimiert aber eine Überwindung des Gebots der Trennung von Polizei und Geheimdiensten nicht.

II. Der Entwurf für das **Gemeinsame- Dateien- Gesetz** kollidiert mit dem Trennungsgebot für Polizei und Geheimdienste, versagt bei der verfassungsgemäßen Programmierung der angestrebten Grundrechtseingriffe und stellt diesen auch keine hinreichenden verfahrensrechtlichen Sicherungen entgegen:

1. Anders als in historischer Zeit steht das **Trennungsgebot** heute vor der Aufgabe, ein Strukturprinzip für das Verhältnis von ca. 40 bundesrepublikanische Polizei- und Nachrichtendienstbehörden im Zeitalter unbegrenzter elektronischer Kommunikations-, Speicherungs- und Auswertungskapazitäten abzubilden. Das Trennungsgebot nachrichtendienstlicher Aufgaben und polizeilicher Methoden versteht sich in einer freiheitlichen Demokratie nicht als Anachronismus, sondern als lebendes Instrument und rechtsstaatliches Optimierungsgebot. Das bedeutet auch, wie zuletzt der sächsische Verfassungsgerichtshof festgestellt hat, dass das Trennungsgebot auch die informationelle Kooperation von Behörden einschränkt, mithin eine besondere Ausprägung informationeller Gewaltenteilung einschließt. Die dem Trennungsgebot im Zeichen der inneren Sicherheit entgegengehaltene Formel von einem sog. ganzheitlichen Ansatz zur Bekämpfung terroristischer Gefahren und spitzfindige Differenzierungen von institutionellem und informationellem Trennungsgebot werden der rechtsstaatlichen Funktion des Trennungsgebots nicht gerecht und werfen die Frage nach der Beherzigung des mentalen Trennungsgebots auf. Ebensowenig kann aus dem Wegfall des Besatzungsstatuts geschlossen werden, dass das ursprünglich von den Westalliierten formulierte Trennungsgebot aus der Rechtswirklichkeit verschwunden ist. Denn mit der Wiederherstellung der Einheit Deutschlands war nach herrschender Auffassung ein Abbau von rechtsstaatlichen und bürgerrechtlichen Garantien nicht angestrebt.

2. Das Gemeinsame-Dateien-Gesetz ist Ausdruck der weiteren **Infiltration der Gefahrenabwehr durch nachrichtendienstliche Gesichtspunkte und Methodik**. Schon lange haben die Nachrichtendienste einen Wandel der Aufgabenstellung durchlaufen von der Information der politischen Führung über besondere Entwicklungen im Bereich der Staatssicherheit hin zur operativen Durchdringung und zuweilen Mitgestaltung gesellschaftlicher Prozesse weit im Vorfeld exekutiven Handlungsbedarfs. Nachrichtendienstlicher Tätigkeit ist zunehmend die Rolle der Gefahrenfrüherkennung und - bekämpfungsvorsorge zugewiesen. Umgekehrt dringt polizeiliche Informationsbeschaffung zunehmend in das Gefahrenvorfeld vor. Praktische Konsequenz dieser Parallelbefassung sind die organisatorische und informationelle Verzahnung und die operative Abstimmung von Polizei und Nachrichtendiensten. An genau dieser Schnittstelle platziert, werden die Antiterrordatei und gemeinsame Projektdateien (§§ 22a BVerfSchG [neu] u.a.) zum Katalysator der

massenhaften Überwindung der gesetzlich bereits heute bedenklich nebulös geratenen Aufgabendifferenzierung von Polizei und Geheimdiensten. Das Trennungsgebot erträgt, auch und insbesondere angesichts der modernen Übermittlungsbefugnisse, den automatisierten „runden Tisch" der beteiligten Behörden nicht. Informationelle Gewaltenteilung, wie das Bundesverfassungsgericht sie aus den notwendig klar und eng zu beschreibenden und voneinander trennscharf zu differenzierenden Zwecken staatlicher Datenerhebung folgert, wird mit dem Gemeinsame-Dateien-Gesetz systematisch in Frage gestellt.

3. Die Antiterrordatei zielt auch nicht auf lediglich belanglose **Grundrechtseingriffe**. Schon die rechtliche Möglichkeit einer Datenübermittlung und damit verbunden einer Zweckänderung vertieft den primären Eingriff der Datenerhebung. Die Anti-Terror-Datei ist dagegen ein Instrument zur systematischen Perpetuierung von Grundrechtseingriffen durch Entfremdung der erhobenen Information sowohl von ihrer rechtlichen Umgebung als auch von dem Sinnzusammenhang des Primäreingriffs. Ungeachtet des weitestgehend standardisierten Datensatzes aus Grunddaten und erweiterten Grunddaten handelt es sich insbesondere bei nachrichtendienstlichen Daten aus dem Gefahrenvorfeld um sogenannte weiche Daten. Deren Validität kann anhand der Datei keinesfalls beurteilt werden. Erstrecht erlaubt auch der erweiterte Grunddatensatz nicht – wie die Entwurfsverfasser hoffen – eine Gefährdungseinschätzung. In der Sache ist die Datei kein Gefahrenbeurteilungs-, sondern nicht mehr als ein Verdachtsgewinnungsinstrument. Mehr ist von einer Indexdatei auch nicht zu erwarten. Dass, wie die Entwurfsbegründung meint, ggf. auch operative Konsequenzen aufgrund eines Treffers in der Antiterrordatei gezogen werden sollen, lässt eine sinkende Hemmschwelle im Umgang mit weichen Daten befürchten, die in dem durch tatsächliche Unsicherheiten besonders geprägten Gefahrenvorfeld unverantwortbar ist.

4. Bedauerlicherweise zieht der Entwurf auch aus vergangenen gesetzgeberischen Fehlleistungen keine Konsequenz. So ist das durch das Bundesverfassungsgericht mit der Entscheidung vom 27.07.2006 als nicht hinreichend präzise verworfene Konzept der **Kontaktperson** unkritisch in den Entwurf übernommen worden und wird in der Praxis seine Wirkung als Blankettbegriff zur Erfassung und Verdächtigung des sozialen Umfelds von Zielpersonen nachrichtendienstlicher Überwachung entfalten können.

5. Wie für die jüngere Sicherheitsgesetzgebung typisch erscheint der **Datenschutz** im Gesetzentwurf nur in vernachlässigungswertem Umfang. Dies ist nicht nur der Regelungstechnik geschuldet. Auch der Wille fehlt, wie sich daran ablesen lässt, dass sich gleichzeitig Geheimhaltungsbedürfnisse insbesondere der Nachrichtendienste ohne weiteres Geltung verschaffen können. Während also bei der Antiterrordatei die Kooperationspflicht der Behörden durch behördliche Geheimhaltungsinteressen suspendiert werden kann, wird den Betroffenen allenfalls durch die – verfassungsrechtlich selbstverständliche – Berücksichtigung „schutzwürdiger Belange" Rechnung getragen, womit keine effektive normative Unterscheidung von Verbotenem und Erlaubtem verbunden ist. Obgleich die **Protokollierung**spflicht für die Antiterrordatei zu begrüßen ist, bleibt das ohnehin spärliche Potential für rechtsstaatliche Kontrolle damit unausgeschöpft. Kooperationsformen wie die Antiterrordatei und die gemeinsamen Projektdateien bedürfen neben der Protokollierung zwecks Datenschutzkontrolle auch der Aktenkundigmachung von Grund und Ausmaß der Zugriffe und Übermittlungen, um die Entscheidungsträger in den beteiligten Stellen in die Lage zu versetzen, Rechtmäßigkeit und Zweckmäßigkeit rückschauend zu beurteilen.

III. Schlussbemerkung: Das Terrorismusbekämpfungsergänzungsgesetz und das Gemeinsame-Dateien-Gesetz bewegen sich als Fortsetzung des „Kampf gegen den Terrorismus" mit legislativen Mitteln bereits weit in aus rechtsstaatlicher Sicht unzugänglichem Terrain. Dies geschieht weitgehend ohne nachgewiesenes Bedürfnis und in Kollision mit dem Trennungsgebot und anderen Prinzipien des Grundrechtsschutzes.

Sönke Hilbrans
Rechtsanwalt und Fachanwalt für Strafrecht, Berlin
Vorsitzender der Deutschen Vereinigung für Datenschutz e.V., Bonn