Innenausschuss
A-Drs. 16(4)131 B

Prof. Dr. Dr. Eric Hilgendorf

Ordinarius für Strafrecht, Strafprozessrecht und Rechtsphilosophie

Kurze Stellungnahme zum Entwurf eines „Gemeinsame-Dateien-Gesetzes“

(Vorläufige Fassung, Stand: 2.11.2006)

I. Grundsätzliche Überlegungen

Grundsätzliche Überlegungen zu den **Bürgerrechten** im Spannungsfeld von „Freiheit und Sicherheit“ gelten heute bei vielen als obsolet, praxisfern und allenfalls von akademischem Interesse. Den Skeptikern ist insoweit Recht zu geben, als man den am 11.9.2001 offenbar gewordenen neuen Dimensionen des Terrorismus allein mit abstrakten Freiheitsbegriffen und wirklichkeitsfremden Idealen nicht mehr beizukommen vermag. Solide gesetzliche Regelungen müssen in der Lage sein, auch den nächsten terroristischen Anschlag zu überstehen.

Andererseits ist zu beachten, dass durch das **Abschleifen rechtsstaatlicher Sicherungen** ein nicht wieder gut zu machender Schaden angerichtet werden kann. Die Erfahrung zeigt, dass staatliche Eingriffs- und Überwachungsrechte, einmal eingeführt, kaum je wieder rückgängig gemacht werden. Auch besteht die Gefahr, durch nicht hinreichend überlegte Maßnahmen ein gut bewährtes und rechtsstaatlich einwandfreies System von Zuständigkeitsregelungen, Kompetenzabgrenzungen und Abwehrmöglichkeiten der Bürgerinnen und Bürger zu stören, ohne dass die Praxistauglichkeit der neuen Instrumentarien wirklich dargetan ist. Mit dem Vorwurf der Verfassungswidrigkeit sollte man zurückhaltend umgehen. Aber auch Maßnahmen, die sich noch im Rahmen der Verfassung halten, können schweren und u.U. irreparablen politischen wie rechtlichen Schaden anrichten.

Der vorliegende Entwurf lässt erkennen, dass dem Gesetzgeber diese Gefahren bewusst sind. Ich halte das hier in Frage stehende „Gemeinsame-Dateien-Gesetz“ für gut durchdacht und im Grundsatz akzeptabel. Das Anliegen, angesichts der Bedrohungen durch den internationalen Terrorismus den Informationsaustausch zwischen Polizeien und Nachrichtendiensten weiter zu verbessern, verdient Zustimmung. In vielen Details scheinen mir jedoch Nachbesserungen wünschenswert und auch durchführbar zu sein, ohne die Effizienz des Gesetzes spürbar zu beeinträchtigen.

Universität Würzburg
Lehrstuhl für Strafrecht, Strafprozessrecht, Rechtstheorie, Informationsrecht und Rechtsinformatik
Domerschulstrasse 16 · 97070 Würzburg
Tel.: (0931) 31 2303 Fax: (0931) 31 2797
E-Mail: hilgendorf@jura.uni-wuerzburg.de
http://www.rechtstheorie.de

II. Kritische Anmerkungen

1. Trennungsgebot

In der kritischen Auseinandersetzung mit den neuen Sicherheitsgesetzen wird häufig auf das sog. Trennungsgebot rekurriert, also das Gebot der Trennung zwischen Polizei und Nachrichtendiensten. Die umfangreiche Literatur zum Trennungsgebot hat sich bisher vor allem mit seiner historischen Entstehung und der Frage beschäftigt, ob dem Trennungsgebot Verfassungsrang zukommt. Merkwürdigerweise scheint dem Inhalt des Trennungsgebots im öffentlich-rechtlichen Schrifttum weit weniger Aufmerksamkeit zuteil geworden zu sein. „Trennungsgebote" finden sich in der bundesdeutschen Staats- und Verwaltungsorganisation in großer Zahl. Aus dem Bereich des Strafrechts sei etwa auf die Unterscheidung zwischen Polizei, Staatsanwaltschaft und Strafgerichtsbarkeit hingewiesen. Derartige Differenzierungen ändern nichts daran, dass die an der Strafverfolgung und strafrechtlichen Rechtsprechung beteiligten Stellen eng zusammenarbeiten dürfen und müssen. Für Polizei und Geheimdienste gilt im Grundsatz nichts anderes. Von dem Gebot einer strikten, in allen Bereichen durchzuführenden Trennung oder gar dem Verbot jeglicher Kontakte und Kooperationen kann also keine Rede sein.

Allerdings haben Polizei und Geheimdienste unterschiedliche Aufgaben und unterschiedliche Kompetenzen. Es handelt sich um unterschiedliche Organisationen (Behörden) mit einem unterschiedlichen Mitarbeiterkreis. Diese in der Bundesrepublik Deutschland bewährte Trennung wird durch die Schaffung verbesserter wechselseitiger Informationsmöglichkeiten nicht aufgehoben, so dass das Gemeinsame-Dateien-Gesetz jedenfalls in seiner Zielsetzung nicht gegen das Trennungsgebot verstößt. Allerdings wird man aus der unterschiedlichen Aufgaben- und Kompetenzzuweisung der hier beteiligten Stellen zu folgern haben, dass auch ihre Kompetenz zur Datenerhebung, Datenverarbeitung und Datenspeicherung entsprechend beschränkt ist. Polizei und Geheimdienste dürften also keinen Zugriff auf Daten haben, die nicht in ihren Aufgaben- und Kompetenzbereich gehören.

Auch insofern scheint mir die Konzeption des hier in Frage stehenden Gesetzes jedoch im Grundsatz akzeptabel zu sein. Nach § 5 Abs. 1 a.E. muss die Übermittlung von erweiterten Grunddaten (die einfachen Grunddaten dürften in diesem Zusammenhang unproblematisch sein) im Rahmen der jeweils geltenden Übermittlungsvorschriften erfolgen. Damit sollte sichergestellt sein, dass Daten nicht an von vornherein unzuständige Behörden übermittelt werden. Zu bedenken ist auch, dass es dem Gesetzgeber grundsätzlich frei steht, den Zuständigkeitsbereich von Behörden zu erweitern. Im

Ergebnis lassen sich deshalb aus dem Gebot der Trennung von Polizei und Geheimdiensten im Grundsatz keine durchgreifenden Bedenken gegen das Gemeinsame-Dateien-Gesetz herleiten.

Probleme ergeben sich allerdings im Zusammenhang mit den sog. Eilfällen (§ 5 Abs. 2). Dazu näher unter 3.2.

2. Datenschutz

Auch im Hinblick auf den Datenschutz und das Recht auf informationelle Selbstbestimmung scheinen mir gegen das Gesetz keine durchgreifenden Bedenken zu bestehen. Dem Grundsatz der Datensparsamkeit ist gerade auch im Hinblick auf die – sicherlich problematische, hier aber doch noch akzeptable – Aufnahme der **Religionszugehörigkeit** in den Kreis der „erweiterten Grunddaten" (§ 3 Nr. 1 b hh) Genüge getan. Die Religionszugehörigkeit darf nämlich nur gespeichert werden, soweit dies im Einzelfall zur Aufklärung oder Bekämpfung des internationalen Terrorismus erforderlich ist. Der moderne Terrorismus, um dessen Bekämpfung es hier geht, ist nun einmal in erster Linie religiös bedingt. Die Religionszugehörigkeit ist deshalb ein wichtiges Datum, auf das der auf Prävention und Gefahrenabwehr bedachte Staat nicht von vornherein verzichten kann.

Das in § 3 Abs. 1 Nr. 1 b rr vorgesehene **Freitextfeld** könnte bei beliebigen Einträgen dazu führen, dass die Auflistung in den Buchstaben aa) bis qq) entwertet wird, weil die „wirklich relevanten" Informationen als Freitext untergebracht sind. Außerdem sollte besser dafür gesorgt werden, dass die im Freitextfeld niedergelegten Informationen zumindest einigermaßen gesichert sind. Bloße Vermutungen oder Bewertungen ohne sichere Faktengrundlage sollten anderen Behörden nicht auch noch über die Antiterrordatei zugänglich gemacht werden. Sofern ein Freitextfeld aus Sicht der Aufklärungs- und Verfolgungsbehörden tatsächlich unverzichtbar ist (was ich nicht zu beurteilen vermag), sollte das Feld von der dateneingebenden Stelle regelmäßig überprüft werden müssen, um zu gewährleisten, dass evtl. überflüssig gewordene Bemerkungen entfernt werden.

3. Unbestimmte Begriffe

An einigen Stellen verwendet das Gesetz Begriffe, die bedenklich unbestimmt sind und daher Ansatzpunkt problematischer, den Intentionen des Gesetzgebers möglicherweise entgegenstehender Interpretationen sein könnten:

3.1. Zu unbestimmt ist zunächst das Konzept der „**Kontaktperson**“ in § 2 Nr. 3. Als „Kontaktperson“ gilt, wer mit einer Person i.S.v. § 2 Nr. 1 a oder Nr. 2 „in Verbindung steht“ und über ihn (oder sie) terrorismusrelevante Hinweise gewonnen werden können. Dies bedeutet, dass etwa ein Professor, dessen Vorlesung regelmäßig ein terrorismusverdächtiger Student besucht, Kontaktperson ist, auch wenn er den Studenten gar nicht kennt und selbst keinerlei Bezug zum Terrorismus hat. Ähnliches gilt für Vermieter und Arbeitskollegen. Hier ließe sich daran denken, die verdächtigen Kontaktpersonen durch eine Klausel wie „tatsächliche Anhaltspunkte die Annahme begründen, dass sie … die Anwendung von Gewalt billigen und …“) näher zu umschreiben. In jedem Fall sollte sichergestellt werden, dass unverdächtige oder nur entfernt verdächtige Kontaktpersonen, wenn sie schon in die Antiterrordatei aufgenommen werden müssen, nicht mit „terrorismusnahen“ Personen in einen Topf geworfen werden. Zu denken wäre an eine Klarstellung in den erweiterten Grunddaten, besser noch an die Schaffung einer dritten Kategorie „Kontaktmöglichkeiten“ neben den einfachen und den erweiterten Grunddaten.

3.2 Zu unbestimmt ist ferner die Fassung des „**Eilfalls**“ in § 5 Abs. 2. Ein Eilfall soll dann vorliegen, wenn ein unmittelbarer Zugriff auf die erweiterten Daten zur „Abwehr einer gegenwärtigen Gefahr für Leib, Leben, Gesundheit oder Freiheit einer Person oder für Sachen von erheblichem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, unerlässlich ist und die Datenübermittlung aufgrund eines Ersuchens nicht rechtzeitig erfolgen kann“. Auffällig ist hier zunächst eine gewisse Redundanz bei den gefährdeten Schutzgütern: Gefahren für den „Leib“ lassen sich kaum von Gefahren für die „Gesundheit“ unterscheiden; es bietet sich an, statt dessen einfach von Gefahren für die „körperliche Unversehrtheit“ zu sprechen.

Zum anderen erweitert die Einbeziehung von Gefahren für die „Freiheit“ den Anwendungsbereich der Eilfallklausel erheblich, man denke nur an den weiten Anwendungsbereich des § 240 StGB, einer der wichtigsten freiheitsschützenden Normen. Ein Blick auf die Freiheitsberaubung selbst (§ 239 StGB) legt die Vermutung nahe, dass Freiheitsgefährdungen sich kaum je durch jene Dringlichkeit auszeichnen werden, wie sie Gefährdungen des Lebens oder der körperlichen Unversehrtheit zukommen kann. Man sollte deshalb prüfen, ob man nicht Gefährdungen der Freiheit aus dem Anwendungsbereich der Eilfallklausel ganz herausnehmen und sie auf die „Abwehr einer gegenwärtigen Gefahr für das Leben oder die körperliche Unversehrtheit einer Person … „ beschränken sollte. Die Einbeziehung der Gefahren für Sachen von erheblichem Wert usw. sollte m.E. bestehen bleiben, weil auch hier enorme irreparable Schäden möglich sind. Allerdings sollte klargestellt werden, dass nicht der „bedeutende

Schaden“ i.S.v. § 69 Abs. 2 StGB und auch nicht der „bedeutende Wert“ von § 315 c StGB gemeint sind, sondern wirtschaftliche Großschäden.

Die Regelung der Zuständigkeiten, Dokumentationspflichten und anderen Kontrollmechanismen in Art. 5 Abs. 2 ist ein gelungenes Beispiel für das Konzept „Sicherheit durch Verfahren“. Ein kleineres Problem könnte darin zu sehen sein, was mit Arbeitsergebnissen zu geschehen hat, die durch eine Datenabfrage erzielt wurden, die im Nachhinein als unzulässig qualifiziert wurde. Nach dem Gesetzeswortlaut ist nur die „weitere Verwendung der Daten“ unzulässig, nicht dagegen die weitere Verwendung der mittels der Daten erzielten Arbeitsergebnisse. Dies ist vom Gesetzgeber aber offenbar intendiert (vgl. auch die Gesetzesbegründung S. 25).

3.3. Ein weiteres Problem stellt sich bei der Frage, **welche Behörden** das Recht haben sollen, auf die Antiterrordatei zuzugreifen. Die Regelung des § 1 Abs. 2 lässt hier einen nicht unbeträchtlichen Entscheidungsspielraum, der nach § 12 Nr. 2 vom Bundeskriminalamt im Wege einer Errichtungsanordnung auszufüllen ist. Die Formulierungen in der Begründung zu § 1 Abs. 2 sind zu weich, um eine klare Abgrenzung zu erlauben. Da es im Hinblick auf das Recht auf informationelle Selbstbestimmung von großer Bedeutung ist, wer auf die Antiterrordatei zugreifen kann, sollten die beteiligten Behörden nach Möglichkeit schon im Gesetz selbst festgelegt werden.

3.4 Bedenklich ist schließlich auch die Fassung der Voraussetzungen für eine **weitergehende Verwendung der Daten** (§ 6). Eine Verwendung der Daten „zu einen anderen Zweck als zur Wahrnehmung ihrer jeweiligen Aufgabe zur Aufklärung oder Bekämpfung des internationalen Terrorismus“ soll zulässig sein, soweit dies „zur Verfolgung einer besonders schweren Straftat oder zur Abwehr einer Gefahr für Leib, Leben, Gesundheit oder Freiheit einer Person geboten ist, erforderlich ist“ (Nr. 1, nach BT-Drucksache 672/06, S. 7), und außerdem „die Behörde, die die Daten eingegeben hat, der Verwendung zustimmt“ (Nr. 2). Auch hier ist wieder das Trennungsgebot (II.1) zu beachten. Eine zu weitgehende Anwendung des § 6 könnte dazu führen, dass das Trennungsgebot ausgehöhlt wird. Deshalb sollte § 6 restriktiv interpretiert werden.

An der Formulierung des § 6 fällt zunächst wieder der redundante Schutz der körperlichen Unversehrtheit auf (vgl. schon oben 3.2). In der BT-Drucksache 672/06, S. 7 findet sich eine Doppelung von „geboten“ und „erforderlich“, die unnötig ist; sinnvoller wäre es, von „geeignet“ und „erforderlich“ oder auch (m.E. vorzugswürdig), nur von einer „erforderlichen“ Datenverwendung zu sprechen. Höchstwahrscheinlich handelt es sich aber nur um ein Redaktionsversehen: In der Begründung (BT-Drucksache 672/06, S. 42 f) heißt es, eine Verwendung von Daten zu anderen

Zwecken als nach Satz 1 sei „nur zulässig, wenn dies zur Verfolgung einer besonders schweren Straftat oder zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben, Gesundheit oder Freiheit einer Person *oder für Sachen von erheblichem Wert, deren Erhaltung im öffentlichen Interesse* geboten ist, erforderlich ist“. Legt man diesen Wortlaut zugrunde, so macht die Aufeinanderfolge von „“geboten ist“ und „erforderlich ist“ Sinn.

Des Weiteren ist fraglich, ob der Anwendungsbereich dieser Ausnahmeklausel nicht zu weit und zu unbestimmt ausfällt. Was ist eine „besonders schwere Straftat“? Vielleicht wäre eine Begrenzung auf die (in § 12 Abs. 1 StGB legaldefinierten) Verbrechen sinnvoll.

Auch bei § 6 Abs. 1 Nr. 1 stellt sich das schon behandelte Problem, dass Gefahren für die „Freiheit“ praktisch allgegenwärtig sind. Um den Anwendungsbereich von § 6 nicht uferlos werden zu lassen, sollte wieder eine Beschränkung auf „Leben und körperliche Unversehrtheit“ festgelegt werden (vgl. schon oben 3.2). Schließlich ist auch fraglich, ob sich durch § 6 Abs. 1 Nr. 2 (Zustimmungserfordernis der dateneingebenden Behörde) eine echte Einschränkung der Verwendung der Daten zu weitergehenden Zwecken erreichen lässt. Die geltenden Übermittlungsverbote sind auch hier einschlägig. Möglicherweise ließe sich eine noch restriktivere Anwendung der Klausel erzwingen, wenn man die Zustimmung einer Datenschutzbehörde (des Bundes oder - vorzugswürdig – eines Landes) verlangen würde.

4. Einfache Wortlautklarstellungen

An folgenden Stellen könnte der Gesetzeswortlaut leicht geändert werden, um das Gemeinte deutlicher werden zu lassen:

4.1. Zwischen § 1 Abs. 2 Nr. 1 und § 1 Abs. 2 Nr. 2 sollte zur Klarstellung ein „und“ eingefügt werden.

4.2. Die Unterscheidung von „Grunddaten“ und „erweiterten Grunddaten“ in § 3 ist missverständlich, weil auch „erweiterte Grunddaten“ begrifflich Grunddaten sind. Klarer wäre es, von „einfachen“ und „erweiterten“ Grunddaten zu sprechen.

4.3 In § 3 Abs. 1 Nr. 1 b hh ließe sich zur Klarstellung vor „erforderlich“ noch das Wort „unbedingt“ einfügen, um den Ausnahmecharakter der Speicherung von Daten über die Religionszugehörigkeit zu betonen.

4.4 In § 5 Abs. 2 Satz 1 und in § 6 Abs. 1 Nr. 1 ist die Nennung des Schutzgutes „Gesundheit“ nach dem Schutzgut „Leib“ überflüssig; für beide ließe sich der übergreifende Begriff „körperliche Unversehrtheit“ verwenden (vgl. 3.2. und 3.4).

4.5 In § 11 Abs. 1 und Abs. 2 sollte vor „zu berichtigen“ bzw. „zu löschen“ jeweils noch das Wort „unverzüglich“ eingefügt werden (das schon jetzt in § 8 Abs. 3 verwendet wird, ohne dass ein relevanter Unterscheid zu § 11 erkennbar wäre).

III. Weitere Maßnahmen

Es sei gestattet, abschließend in aller Kürze noch einige Hinweise auf zusätzliche Maßnahmen zu geben, die eine rechtsstaatsfreundliche Umsetzung des „Gemeinsame-Dateien-Gesetzes“ begleiten könnten:

1. Evaluierungen

Evaluierungen komplexer Gesetzesprojekte sind für eine effiziente Neu-Formulierung, Umsetzung, Kontrolle und Fortentwicklung der Gesetze außerordentlich wichtig. Es reicht nicht aus, Gesetze (wie jetzt im Fall des Terrorismusbekämpfungsgesetzes) regierungsintern zu evaluieren. Aber auch eine Evaluierung allein durch wissenschaftliche Analyse und Kritik ist ungenügend, so wichtig sie auch ist. Gerade für zentrale Gesetze aus dem Bereich der Inneren Sicherheit sollten bei der Evaluierung daher Vertreter der gesetzesanwendenden Stellen, also vor allem der Polizei und der Geheimdienste, gehört werden. Außerdem sollten unabhängige Vertreter der Wissenschaft sowie Vertreter von Bürgerrechtsgruppen einbezogen werden. Nur durch seriöse, unabhängige Evaluierungen lassen sich Probleme, etwa praktisch überflüssige oder unzweckmäßig formulierte Eingriffsbefugnisse oder bürokratische Fallstricke ohne praktischen Nutzen, erkennen. Zeitlich sollten Evaluierungen so angesetzt werden, dass ihre Ergebnisse bei Ablauf etwaiger Gesetzesbefristungen vorliegen. Gerade bei rechtsstaatlich heiklen Materien könnten Evaluierungen regelmäßig alle zwei oder drei Jahre durchgeführt werden, um Fehlentwicklungen rechtzeitig zu erkennen.

2. Kontrollen

Als flankierende Maßnahme zum Erlass des Gemeinsame-Dateien-Gesetzes und des Terrorismusbekämpfungsergänzungsgesetzes empfiehlt es sich, über bessere Kontrollen der beteiligten Stellen, insbesondere der Geheimdienste, nachzudenken und leistungsfähige Kontrollmechanismen einzuführen. Entsprechende Gesetzesvorschläge existieren bereits. Gerade der Bereich der inneren Sicherheit darf der demokratischen Kontrolle keinesfalls entzogen werden. Bei den Kontrollen im Zusammenhang mit dem „Gemeinsame-Dateien-Gesetz" sollte dem Bundesbeauftragten für den Datenschutz eine Schlüsselrolle zukommen (vgl. schon jetzt § 10 Abs. 1).

3. Bewusstseinsschaffende Maßnahmen

Ein weiterer aus meiner Sicht wichtiger Schritt ist die Einführung „bewusstseinschaffender Maßnahmen" für die an der Gesetzesumsetzung beteiligten Personen. Es muss sichergestellt sein, dass in den beteiligten Behörden nicht nur die Behördenleiter und Vorgesetzen, sondern alle Beamten in nicht ganz unwesentlichen Positionen für die besondere Bedeutung des Grundrechts- und zumal des Datenschutzes im Bereich der Inneren Sicherheit Verständnis aufbringen. Auch der Öffentlichkeit sollte noch deutlicher vermittelt werden, dass Datenschutz kein Luxus, sondern angesichts der rasant zunehmenden technischen Möglichkeiten zur Überwachung eine unverzichtbare Voraussetzung eines freiheitlichen demokratischen Rechtsstaats ist.

4. Rechtsschutz

Ein anderer Punkt, der im Zusammenhang mit dem „Gemeinsame-Dateien-Gesetz" besondere Aufmerksamkeit verdient, ist der Rechtsschutz. Wer zu Unrecht in die Antiterrordatei gelangt ist und dadurch Nachteile erleidet, muss die Möglichkeit haben, dagegen vorzugehen. Dies setzt aber voraus, dass dem Betroffenen die Speicherung überhaupt bekannt ist. Andererseits kann man, um das Gesetz nicht ad absurdum zu führen, Verdächtige nicht ohne weiteres darüber informieren, dass ihre Daten in der Antiterrordatei gespeichert wurden. Das Problem des Rechtsschutzes erweist sich so als eng verknüpft mit dem bereits oben (III. 2) angesprochenen Problem der Kontrolle.

5. Echte Zusammenführung der Terrorismusdateien

Nur am Rande sei darauf hingewiesen, dass es wünschenswert wäre, sämtliche Terrorismusdateien, vor allem die des Bundeskriminalamts und der Staatsschutzstellen der Landeskriminalämter, in die neue Antiterrordatei zu überführen. In dieselbe Richtung zielt die Speicherungspflicht nach § 2 (mit den Möglichkeiten der beschränkten und verdeckten Speicherung nach § 4). Problematisch und rechtsstaatlich bedenklich wäre es, ältere Terrorismusdateien ohne zwingenden Grund unabhängig von der Antiterrordatei fortzuführen.

6. Abschaffung obsolet gewordener Teile des Rechts der inneren Sicherheit („Rechtsbereinigung“)

Abschließend sei der Hinweis erlaubt, dass die inzwischen sehr unübersichtlich gewordene Gesetzgebung zur inneren Sicherheit seit den 70er Jahren einer kritischen Sichtung unterzogen werden sollte. Eingriffsrechte und sonstige Regelungen, die nicht mehr zeitgemäß sind oder keine praktische Bedeutung (mehr) haben, sollten außer Kraft gesetzt werden. In diesem Zusammenhang ist wieder auf die Bedeutung externer Evaluierungen hinzuweisen (s.o. III 1). Als besonders eindrucksvolles Beispiel für eine derartige Untersuchung im Bereich der Kriminalität verweise ich auf den „Ersten Periodischen Sicherheitsbericht“ (2001). Ein ähnlich angelegter Bericht könnte sich mit der Entwicklung der terroristischen Gefährdungslage seit den 70er Jahren und den Antworten des Gesetzgebers darauf befassen. Derartige Querschnittuntersuchungen sollten nicht allein der Wissenschaft vorbehalten bleiben, sondern unter aktiver Beteiligung der Politik und der zuständigen Behörden sowie der Vertreter von Bürgerrechtsgruppen erarbeitet werden.

IV. Ergebnis

Intention und Konzeption des „Gemeinsame-Dateien-Gesetzes“ verdienen im Grundsatz Zustimmung. An einzelnen Punkten sind jedoch Nachbesserungen angezeigt. Diese betreffen vor allem das Konzept der „Kontaktperson“, den Begriff des „Eilfalls“, den Kreis der zum Datenzugriff befugten Behörden sowie die Voraussetzungen für eine weitere Verwendung der Daten. Auch die Kontrollmöglichkeiten sollten verstärkt werden; dabei könnte über eine bessere Kontrolle der Geheimdienste insgesamt nachzudenken sein. Darüber hinaus sollte die Anwendung des Gesetzes von einer unabhängigen Stelle, etwa dem Bundesbeauftragten für den Datenschutz, regelmäßig überprüft werden. Erforderlich ist

schließlich eine ernsthafte, d.h. umfassende und durch unabhängige Personen vorzunehmende regelmäßige Evaluierung.