



Der Bundesbeauftragte  
für den Datenschutz und  
die Informationsfreiheit

Deutscher Bundestag  
Innenausschuss

Ausschussdrucksache  
17(4)460 E

**Peter Schaar**

Bundesbeauftragter für den Datenschutz  
und die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit,  
Postfach 1468, 53004 Bonn

An den  
Vorsitzenden des Innenausschusses  
des Deutschen Bundestages  
Herrn Wolfgang Bosbach, MdB  
Platz der Republik 1  
11011 Berlin

HAUSANSCHRIFT Husarenstraße 30, 53117 Bonn  
VERBINDUNGSBÜRO Friedrichstraße 50, 10117 Berlin

TELEFON (0228) 997799-100  
TELEFAX (0228) 997799-550  
E-MAIL Ref5@bfdl.bund.de

INTERNET [www.datenschutz.bund.de](http://www.datenschutz.bund.de)

DATUM Bonn, 15.03.2012

[innenausschuss@bundestag.de](mailto:innenausschuss@bundestag.de)

BETREFF **68. Sitzung des Innenausschusses des Deutschen Bundestages am 19. März 2012**

HIER Öffentliche Anhörung von Sachverständigen zum Gesetzentwurf der  
Bundesregierung zur Verbesserung der Bekämpfung des Rechtsextremismus - BT-  
Drs. 17/8672

BEZUG Schreiben des Sekretariats des Innenausschusses des Deutschen Bundestages vom  
6. März 2012

Sehr geehrter Herr Bosbach,

anliegend übersende ich die mit Schreiben vom 6. März 2012 (Bezug) erbetene Stellungnahme.

Aufgrund der Eilbedürftigkeit erfolgt die Übersendung wunschgemäß per E-Mail.

Mit freundlichen Grüßen  
gez.

Schaar



**Stellungnahme**  
**des**  
**Bundesbeauftragten für den Datenschutz**  
**und die Informationsfreiheit**

Öffentliche Anhörung  
des Innenausschusses des Deutschen Bundestages  
am 19. März 2012

Gesetzentwurf der Bundesregierung  
Entwurf eines Gesetzes zur Verbesserung der Bekämpfung des Rechtsextremismus  
**BT-Drucksache 17/8672**



## Zusammenfassung

1. Trotz einzelner Verbesserungen besteht noch dringender gesetzgeberischer Handlungsbedarf.
2. Insbesondere die Regelungen zur Protokollierung und zur Nutzung der Protokolldaten sind gesetzlich klarstellungs- bzw. ergänzungsbedürftig. Dies bestätigen meine Kontrollen der inhaltsgleichen Bestimmungen des Antiterrordateigesetzes. Ohne diese Anpassungen ist eine effektive, umfassende Datenschutzkontrolle nicht möglich.
3. Zum Schutz unbescholtener Personen müssen bestimmte Tatbestände, insbesondere die Voraussetzungen für die Speicherung von Kontaktpersonen und die Befugnis zur Speicherung erweiterter Grunddaten zu dolosen Kontaktpersonen, enger bzw. hinreichend bestimmt und verhältnismäßig gefasst werden.
4. Einige Bestimmungen sind mit der eindeutigen gesetzlichen Zielsetzung, ausschließlich den gewaltbezogenen Rechtsextremismus zu regeln, nicht vereinbar.
5. Die Notwendigkeit des Gesetzgebungsvorhabens ist angesichts der geltenden Rechtslage kritisch zu hinterfragen. Derzeit sind bereits umfängliche Speicherungen, Übermittlungen und Nutzungen in diesem Bereich möglich. Vollzugsdefizite kann dieser Gesetzentwurf nicht beseitigen.



## A.

Ich begrüße, dass die Bundesregierung auf ursprünglich beabsichtigte Grundrechtseingriffe verzichtet hat, die ich in den Ressortberatungen besonders kritisch bewertet habe, insbesondere die generelle Verlängerung von Speicherfristen und die Normierung umfassender, unspezifischer Recherchemöglichkeiten in Dateien der Sicherheitsbehörden.

Positiv sehe ich auch, dass der Gesetzentwurf (GE) gegenüber dem Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz – ATDG) einige Verbesserungen enthält, z.B. durch die Aufnahme gegenüber dem ATDG erhöhter tatbestandlicher Eingriffsschwellen („Tatsachen“ anstelle von „tatsächlichen Anhaltspunkten“), einer qualifizierten Evaluierungsklausel (vgl. Artikel 3 Abs. 2 GE) sowie einer zeitlich befristeten Geltung der im Vergleich zum ATDG neu eingeführten Regelung des Artikel 1 § 7 des Gesetzes zur Errichtung einer standardisierten zentralen Datei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern zur Bekämpfung des gewaltbezogenen Rechtsextremismus (Rechtsextremismus-Dateigesetz – RED-G).

Gleichwohl sind durch die zwischenzeitlichen Änderungen nicht alle meine Bedenken ausgeräumt worden.

Zwei Punkte sind datenschutzrechtlich von herausragender Bedeutung und bedürfen dringend einer Klarstellung im vorliegenden Gesetzentwurf – auch im Lichte meiner Kontrollerfahrungen mit den inhaltsgleichen Regelungen des ATDG: Die Gewährleistung einer lückenlosen und effektiven Datenschutzkontrolle und einer qualifizierten, unabhängigen Evaluation.

### ▪ Artikel 1 § 10 Absatz 1 RED-G i.V.m. § 11 Absatz 1 RED-G

1. Gemäß Artikel 1 § 10 Absatz 1 RED-G hat das BKA bei jedem Zugriff für Zwecke der Datenschutzkontrolle den Zeitpunkt, die Angaben, die die Feststellung der aufgerufenen Datensätze ermöglichen, sowie die für den Zugriff verantwortliche Behörde und den Zugriffszweck nach § 5 Abs. 4 oder § 7 zu proto-



kollieren. Nach der Entwurfsbegründung zu dieser Norm umfasst diese Regelung „eine systemseitige Vollprotokollierung, d.h. eine automatisierte, beweis-sichere und lückenlose Protokollierung aller Datenbanktransaktionen auf der Grundlage von Auswerteprogrammen“ (GE-Begründung, S. 20). Hierzu zählen auch verdeckte Speicherungen im Sinne des Artikel 1 § 4 Abs. 1 Satz 1 RED-G sowie die durch eine Anfrage ausgelösten Treffer auf verdeckt gespeicherte Daten.

2. Die umfassende Protokollierung und Auswertbarkeit der Protokolldaten ist eine zentrale Verfahrenssicherung und damit ein adäquater Ausgleich zu dem mit dem ATDG erstmals gesetzlich legitimierten Informationspool von Polizeien und Nachrichtendiensten, der in besonders schwerwiegender Weise in das Recht der Betroffenen auf informationelle Selbstbestimmung eingreift und mit erheblichen verfassungsrechtlichen Risiken behaftet ist.

Im Rahmen meiner Kontrollen zur inhaltsgleichen Regelung des § 9 ATDG wurde mir kein umfassender Zugriff auf die ATD-Protokolldaten gewährt, obgleich das BKA, das die Protokolldaten in einem von der Antiterrordatei getrennten, d.h. gesonderten, Protokolldatenserver speichert und administriert, als Bundesbehörde meiner Kontrollkompetenz unterfällt. Begründet wurde dies u.a. damit, dass

- meine Berechtigung zur Einsichtnahme und Prüfung der Protokolldaten ausschließlich auf diejenigen Protokolldaten beschränkt sei, die in Folge einer Datenbanktransaktion einer an der ATD beteiligten Bundesbehörde generiert worden seien;
- ohne die Zustimmung der betroffenen Bundesbehörden deren Protokolldaten nicht eingesehen und ausgewertet werden dürften;
- mir kein unmittelbarer Zugriff auf verdeckt gespeicherte Daten der Bundesbehörden gewährt werden dürfe.

Infolgedessen war es mir beispielsweise nicht möglich, zu einem Betroffenen eine umfängliche Sachstandserhebung durchzuführen und Landesbeauftragte



für den Datenschutz über die in ihrem Zuständigkeitsbereich erfolgten Transaktionen zu informieren.

Auf Seiten der Sicherheitsbehörden erfolgt gemäß dem Prinzip „need to share“ durch die Errichtung der ATD und der Rechtsextremismus-Datei eine Zusammenführung der Informationen zur allseitigen Verfügbarkeit. Damit wird jedem Teilnehmer eine Gesamtschau ermöglicht. Den Datenschutzkontrollbehörden wird dies verweigert, obgleich diese Gesamtschau zur Gewährleistung einer adäquaten und effizienten datenschutzrechtlichen Kontrolle unerlässlich ist.

Bei der Auswertung von Protokolldaten zu einer bestimmten Person muss es auch möglich sein, erkennen zu können, welche Landesbehörden Daten zu dieser Person verarbeitet haben, um die zuständigen Landesdatenschutzbeauftragten entsprechend einbinden bzw. informieren zu können und gegebenenfalls dortige Folgeprüfungen zu initiieren.

Aus den bereichsspezifisch abschließenden Regelungen der Artikel 1 § 4 Abs. 1 Satz 1 RED-G und Artikel 1 § 10 Abs. 1 RED-G resultieren keine Beschränkungen meiner Kontrollkompetenz. Infolgedessen dürfen auch Protokolldaten zu verdeckten Speicherungen sowie zu Datenbanktransaktionen der an der Rechtsextremismus-Datei beteiligten Landesbehörden von mir uneingeschränkt und vorbehaltlos eingesehen und ausgewertet werden.

▪ **Artikel 3 Absatz 2**

Im Hinblick auf die Umsetzung der in dieser Regelung enthaltenen qualifizierten Evaluierungsklausel weise ich darauf hin, dass ich beim „Institut für Gesetzesfolgenabschätzung und Evaluation“ einen

**„Leitfaden zur Durchführung von ex-post-Gesetzesevaluationen unter besonderer Berücksichtigung der datenschutzrechtlichen Folgen“**

in Auftrag gegeben habe. Ich gehe davon aus, dass dieser bald veröffentlicht werden kann. Dort werden detailliert Evaluationsinstrumente und –methoden dar-



gelegt. Ich rege an, die Evaluierung auf der Grundlage dieses Leitfadens durchzuführen.

## I.

Ich verkenne nicht die zur Begründung des Gesetzentwurfs (GE) geltend gemachte Bedrohung durch den gewaltbezogenen Rechtsextremismus.

Auch insoweit ist die Vorgabe des Bundesverfassungsgerichts zu beachten, wonach sich der Staat auf rechtsstaatliche Mittel beschränken muss (vgl. BVerfG, 1 BvR 518/02 vom 04.04.2006, Rdn. 126 m.w.N.). „Das gilt auch für die Verfolgung der fundamentalen Staatszwecke der Sicherheit und des Schutzes der Bevölkerung. Die Verfassung verlangt vom Gesetzgeber, eine angemessene Balance zwischen Freiheit und Sicherheit herzustellen“ (BVerfG, 1 BvR 518/02 vom 04.04.2006, Rdn. 128). Insbesondere der aus dem Rechtsstaatsgebot folgende Verhältnismäßigkeitsgrundsatz ist strikt zu beachten. Demnach muss jeder Grundrechtseingriff zur Erreichung eines legitimen Ziels objektiv geeignet, erforderlich und angemessen sein (vgl. BVerfG, 1 BvR 518/02, Rdn. 82 m.w.N.).

In ihrer Entschließung zur Antiterrordatei (ATD) vom 27. Oktober 2006 hatte die 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont, dass jede Intensivierung der informationellen Zusammenarbeit zwischen Polizeibehörden und Nachrichtendiensten den verfassungsrechtlichen Vorgaben, insbesondere dem Recht auf informationelle Selbstbestimmung, dem Grundsatz der Verhältnismäßigkeit und dem - in einigen Landesverfassungen ausdrücklich genannten - Trennungsgebot von Polizei und Nachrichtendiensten entsprechen muss. Dies gilt auch für die gemeinsame Datei zur Bekämpfung des gewaltbezogenen Rechtsextremismus (im Folgenden kurz: Rechtsextremismus-Datei) von Polizeien und Nachrichtendiensten, die weitgehend „analog“ (GE-Begründung, S. 10) zur Antiterrordatei (ATD) ausgestaltet worden ist.

Folglich müssen zur Beseitigung bestehender Defizite im Bereich der Aufklärung und Bekämpfung des gewaltbezogenen Rechtsextremismus Maßnahmen getroffen wer-



den, die geeignet, erforderlich und angemessen sind (vgl. BVerfG, 1 BvR 518/02, Rdn. 82 m.w.N.).

Dies setzt zunächst voraus, dass bestehende Defizite auf der Grundlage der bekannten Sachverhalte vollständig ermittelt und valide festgestellt worden sind. Dieser Ermittlungsprozess ist – insbesondere in Bezug auf die aktuellen Vorfälle rechtsextremistischer Gewalttatanwendungen – noch nicht abgeschlossen. Insofern ist die Validität der im Gesetzentwurf genannten Prämisse, wonach „regelmäßig nicht ein Defizit an der Informationsbeschaffung, sondern am Informationsfluss und der Informationsbewertung durch die einzelnen Sicherheitsbehörden von Bund und Ländern“ (GE-Begründung, S. 19) vorliegt, zu hinterfragen.

Gesetzgeberische Aktivitäten, die ohne vorherige Aufklärung und Bewertung eventueller Defizite erfolgen, könnten sogar Ursachen der Missstände unabsichtlich verdecken oder deren Beseitigung verzögern. Dessen muss sich der Gesetzgeber bewusst sein.

Insbesondere vor diesem Hintergrund halte ich es für sehr bedauerlich, dass die Bundesregierung meiner bereits vor mehr als einem Jahr geäußerten Anregung nicht gefolgt ist, im Rahmen der Evaluierungsaufträge nach dem Koalitionsvertrag auch die allgemeinen Vorschriften zur Datenübermittlung zwischen Nachrichtendiensten und Polizeibehörden einer umfassenden Evaluierung zu unterziehen. Wäre diesem Petitum entsprochen worden, ständen möglicherweise bereits weitergehende Kenntnisse zu etwaigen strukturellen (Vollzugs-)Defiziten der Zusammenarbeit zwischen Nachrichtendiensten und Polizeien zur Verfügung.

## II.

Der Gesetzentwurf soll den Informationsaustausch zwischen Polizeien und Nachrichtendiensten in Bezug auf den gewaltbezogenen Rechtsextremismus verbessern (vgl. GE-Begründung, S. 10). Ausweislich der Gesetzesbegründung (S. 10, 19) werden der Informationsfluss und die Informationsbewertung als optimierungsbedürftig erachtet, nicht jedoch die Informationsbeschaffung.

Diese Sichtweise ist zu hinterfragen. Sollten auf Seiten der Sicherheitsbehörden auf Bundes- und/oder Länderebene entgegen den geltenden gesetzlichen Regeln Infor-



mationen über den gewaltbezogenen Rechtsextremismus (dienst-)rechtswidrig nicht, nicht zeitnah oder nicht vollständig erhoben worden sein, bestehen gravierende Vollzugsdefizite bei der Informationsbeschaffung. Diese Defizite kann der vorliegende GE nicht beseitigen. Er ist hierfür objektiv nicht geeignet und auch nicht erforderlich.

1. Artikel 1 § 2 Satz 1 RDE-G verpflichtet die an der Rechtsextremismus-Datei beteiligten Behörden, bereits erhobene Daten in der Datei zu speichern. Daten, die von diesen Behörden nicht erhoben worden sind, würden aufgrund ihres fehlenden Vorhandenseins für die Rechtsextremismus-Datei nicht zur Verfügung stehen.
2. Bereits nach geltendem Recht bestehen weitreichende Übermittlungspflichten (und - darüber hinausgehende – Übermittlungsberechtigungen) sowohl innerhalb des Verfassungsschutzverbundes als auch wechselseitig im Verhältnis der Polizeien und Nachrichtendienste, so dass die Annahme der verfassungsrechtlichen Erforderlichkeit für den vorliegenden Gesetzentwurf zumindest zweifelhaft erscheint.
  - a. § 20 Abs. 1 Satz 1 BVerfSchG normiert eine Übermittlungspflicht des BfV gegenüber den Staatsanwaltschaften und Polizeien hinsichtlich „bekanntgewordener Informationen einschließlich personenbezogener Daten, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Übermittlung zur Verhinderung oder Verfolgung von Staatsschutzdelikten erforderlich ist“. Nach § 20 Abs. 1 Satz 2 BVerfSchG sind Delikte nach Satz 1 (d.h. die dort genannten Staatsschutzdelikte) nicht nur „die in §§ 74 a und 120 des Gerichtsverfassungsgesetzes genannten Straftaten“. Hierzu zählen auch alle „sonstigen Straftaten, bei denen auf Grund ihrer Zielsetzung, des Motivs des Täters oder dessen Verbindung zu einer Organisation tatsächliche Anhaltspunkte dafür vorliegen, dass sie gegen die in Artikel 73 Nr. 10 Buchstabe b oder c des Grundgesetzes genannten Schutzgüter gerichtet sind“ (§ 20 Abs. 1 Satz 2 BVerfSchG). Demnach besteht bereits nach geltendem Recht bei Vorliegen von „tatsächlichen Anhaltspunkten“ in Bezug auf den gewaltbezogenen Rechtsextremismus eine



- inhaltlich über den vorliegenden Gesetzentwurf hinausgehende - Übermittlungspflicht des BfV an die Polizeien und Staatsanwaltschaften.

Gemäß § 11 Abs. 2 des Gesetzes über den Militärischen Abschirmdienst (MADG) gilt diese Übermittlungspflicht auch für den MAD.

- b. Eine entsprechende Datenübermittlungspflicht besteht auch für die Polizeien und Staatsanwaltschaften im Verhältnis zum BfV und den LfV gemäß § 18 Abs. 1 Satz 1 BVerfSchG. Diese erstreckt sich u.a. auf alle dort „bekannt gewordenen Tatsachen“ (§ 18 Abs. 1 Satz 1 BVerfSchG), die „Bestrebungen im Geltungsbereich dieses Gesetzes erkennen lassen, die durch Anwendung von Gewalt oder darauf gerichteten Vorbereitungshandlungen gegen die in § 3 Abs. 1 Nr. 1, 3 und 4 genannten Schutzgüter gerichtet sind“ (a.a.O.). Der Tatbestand des § 3 Abs. 1 Nr. 1 BVerfSchG erfasst auch alle Bestrebungen, die gegen die freiheitlich demokratische Grundordnung, den Bestand des Staates oder die Sicherheit des Bundes oder eines Landes gerichtet sind. Rechtsextremistische Tätigkeiten sind hierunter subsumierbar.
- c. Innerhalb des Verfassungsschutzverbundes, d.h. im Verhältnis des BfV und der LfV, bestehen gemäß § 5 BVerfSchG i.V.m. den Richtlinien zur Koordinierung dieser Zusammenarbeit wechselseitige Unterrichtungspflichten auch in Bezug auf rechtsextremistische Erkenntnislagen.

Ergänzend zu den vorgenannten Übermittlungspflichten eröffnen weitere Regelungen den Sicherheitsbehörden - über die vorgenannten Tatbestände hinausgehende - Übermittlungsberechtigungen, z.B. § 18 Abs. 3 BVerfSchG, § 19 Abs. 1 BVerfSchG, § 11 Abs. 1 MADG.

### III.

Zur Begründung des Gesetzentwurfs verweist die Bundesregierung auf die „Erfahrungen mit der analog aufgebauten Antiterrordatei“ (GE-Begründung, S. 10), die derzeit evaluiert werde (vgl. a.a.O). Nach ihrer Auffassung legen diese Erfahrungen na-



he, dass eine gemeinsame elektronische Plattform ein sehr wirkungsvolles Instrument sein kann (a.a.O.).

Kritisch zu bewerten ist, dass die Begründung des Gesetzentwurfs auf Teilergebnisse eines erst begonnenen Evaluierungsverfahrens abstellt, ohne den Abschluss dieses Evaluierungsprozesses abzuwarten und damit auf einer hinreichend validen Erkenntnisgrundlage zu agieren.

Zudem ist zu berücksichtigen, dass gegen das Antiterrordateigesetz (ATDG), an das sich der vorliegende Gesetzentwurf inhaltlich anlehnt, schwerwiegende verfassungsrechtliche Bedenken erhoben wurden [u.a. in der 24. Sitzung des Innenausschusses des Deutschen Bundestages vom 6. November 2006 (öffentliche Sachverständigenanhörung zum ATDG); s. auch Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 2006]. Außerdem ist eine Verfassungsbeschwerde zum ATDG beim Bundesverfassungsgericht anhängig (1 BvR 1215/07). Der vorliegende Gesetzentwurf unterliegt demnach ebenfalls verfassungsrechtlichen Risiken. Daher ist es umso wichtiger, im laufenden Gesetzgebungsverfahren die verfassungsrechtlichen Anforderungen mit besonderer Sorgfalt zu berücksichtigen und dabei die Erkenntnisse der Evaluierung des ATDG zu berücksichtigen.

#### IV.

Datenschutzrechtlich begrüßenswert ist die Aufnahme einer qualifizierten Evaluierungsklausel in Artikel 3 Absatz 2 des Gesetzentwurfs.

Aufgrund der Erfahrungen aus anderen Gesetzesevaluierungen sollte der Gesetzgeber jedoch festlegen, dass den diese Evaluation durchführenden unabhängigen Experten die von ihnen für diese wissenschaftliche Auswertung benötigten Informationen (Rohdaten etc.) von den Sicherheitsbehörden aufforderungsgemäß, zeitnah und vollumfänglich zur Verfügung gestellt werden müssen.



## B.

Im Einzelnen merke ich Folgendes an:

### I. Artikel 1 § 1 Absatz 1 RED-G

Bereits die Speicherung von Grunddaten (vgl. Artikel 1 § 3 Absatz 1 Ziffer 1 Buchstabe a RED-G) in der Rechtsextremismusdatei ist ein erheblicher Eingriff in das Recht auf informationelle Selbstbestimmung mit potentiell weit reichenden Folgen (vgl. auch Geiger, schriftliche Stellungnahme anlässlich der öffentlichen Sachverständigenanhörung des Innenausschusses des Deutschen Bundestages zur „Anti-Terror-Datei und zum Terrorismusbekämpfungsergänzungsgesetz“ am 6. November 2006, BT-IA-Drs. 16(4)131, S. 7).

Mit der Rechtsextremismus-Datei soll ein im Online-Verbund nutzbarer Datenpool geschaffen werden, in dem möglichst umfassend die Erkenntnisse von Polizei und Nachrichtendiensten im Bereich des gewaltbezogenen Rechtsextremismus zusammengeführt werden. Die Intensität eines mit der Speicherung in der Datei verbundenen Eingriffs in das Recht auf informationelle Selbstbestimmung wird dadurch verstärkt, dass personenbezogene Daten zusammengeführt werden, die von verschiedenen Bundes- und Landesbehörden mit unterschiedlichen Befugnissen auf unterschiedlichen Rechtsgrundlagen zu unterschiedlichen Zwecken gesammelt worden sind.

Nach dem verfassungsrechtlichen Vorbehalt des Gesetzes und dem Gebot der hinreichenden Normenbestimmtheit obliegt dem Gesetzgeber die Verpflichtung, diesen Eingriffstatbestand in der jeweiligen Gesetzesnorm hinreichend trennscharf und normenklar zu definieren.

Artikel 1 § 1 Abs. 1 RED-G normiert als tatbestandliche Anwendungsvoraussetzung den Begriff des „gewaltbezogenen Rechtsextremismus“ und damit einen besonderen Phänomenbereich [vgl. Vorblatt GE, C]. Die Norm enthält keine Legaldefinition. Der Begriff wird weder durch andere gesetzliche Regelungen noch durch Entscheidungen der Judikative präzisiert bzw. spezifiziert.



Mit der Festlegung auf den „gewaltbezogenen Rechtsextremismus“ soll der Umfang der in der Datei zu speichernden Informationen begrenzt werden (GE-Begründung, S. 12), da die Rechtsextremismus-Datei „keine Gesinnungsdatei“ (a.a.O., S. 13) sein soll. Ausweislich der Gesetzesbegründung erfordert der Gewaltbezug „neben einer subjektiven Komponente auch eine objektive Anknüpfung an ein gewalttätiges Verhalten und ist damit gegenüber der bloß subjektiven „Gewaltbereitschaft“ enger“ (a.a.O., S. 12). Das Tatbestandsmerkmal „gewaltbezogen“ ist demnach ein zentrales, die Dateispeicherung legitimierendes Kriterium.

Ausgehend von der Begründung des Gesetzentwurfs ist der Begriff „gewaltbezogen“ – zumindest in der Realität - nicht hinreichend trennscharf vom Begriff „gewaltfrei / nicht gewaltbezogen“ abzugrenzen (vgl. GE-Begründung, S. 22). Die Begründung attestiert ausdrücklich, dass „eine trennscharfe Unterscheidung zwischen dem gewaltfreien Rechtsextremismus und dem gewalttätigen (...) Rechtsextremismus nicht möglich“ (a.a.O.) sei.

Infolgedessen besteht die Gefahr, dass - insbesondere unter Berücksichtigung der gemäß § 2 Satz 1 Ziffer 3 RED-G speicherbaren Kontaktpersonen - in der Datei auch eine Vielzahl von Personen erfasst wird, die dem gesetzgeberisch intendierten Personenkreis nicht unterfallen.

Durch eine nicht hinreichend trennscharfe Begriffsbestimmung wird der Exekutive eine erhebliche Interpretationsmöglichkeit eröffnet. Dies entspricht nicht den verfassungsgerichtlichen Vorgaben, wonach z.B. die Polizei nicht ohne nähere gesetzliche Vorgaben über die Grenzen der Freiheit des Bürgers entscheiden und sich den Maßstab dafür selbst zurechtlegen darf [vgl. BVerfG, 1 BvR 668/04 vom 27.07.2005, Rdn. 127]. „Die Schaffung eingriffsbeschränkender Maßstäbe ist (...) Aufgabe des Gesetzgebers.“ [a.a.O.; vgl. auch Rdn. 132: „Hier muss der Gesetzgeber selbst Verantwortung übernehmen, (...)“].

## **II. Artikel 1 § 1 Absatz 2 Nr. 1 RED-G**

Durch diese Regelung wird der Kreis der an der Rechtsextremismus-Datei beteiligten Behörden über die in § 1 Abs. 1 RED-G abschließend aufgelisteten (Zentral-)Stellen



hinaus erheblich erweitert. Teilnahmeberechtigt sind demnach auch weitere Polizeivollzugsbehörden, soweit die in § 1 Abs. 2 Nr. 1 und 2 RED-G geregelten Voraussetzungen vorliegen. „Mit dieser Regelung soll verhindert werden, dass praktisch jede Polizeivollzugsbehörde, die im Rahmen der Gefahrenabwehr im Einzelfall auch Gefahren des gewaltbezogenen Rechtsextremismus abwehrt, angeschlossen werden kann“ (GE-Begründung, S. 12).

Im Hinblick auf das Gebot einer angemessenen und sachgerechten Beschränkung der Teilnahmeberechtigung sind diese Voraussetzungen kritisch zu bewerten. Die Beschränkung „nicht nur im Einzelfall besonders zugewiesen“ (§ 1 Abs. 1 Nr. 1 RED-G) ist durch entsprechende Organisationserlasse beliebig steuerbar.

### **III. Artikel 1 § 2 Nr. 3 RED-G**

Gegen diese Regelung bestehen Bedenken im Hinblick auf die Wahrung des Gebots hinreichender Normenklarheit und –bestimmtheit und des Verhältnismäßigkeitsgebots.

1. Im Gegensatz zu den in Artikel 1 § 2 Nr. 1 und 2 RED-G genannten Personen bedarf es für eine Speicherung von Kontaktpersonen in der Rechtsextremismus-Datei nach dem Wortlaut der Regelung nicht des Vorliegens von Tatsachen als materielle Erkenntnisschwelle. Eine entsprechende Konkretisierung erfolgt lediglich im Rahmen der Entwurfsbegründung (S. 13).

Diese qualifizierende Voraussetzung, d.h. das Vorliegen von Tatsachen, sollte in den Wortlaut der Regelung übernommen werden.

2. Nach der Gesetzesbegründung (S. 13) sind die vorgenannten konkreten Tatsachen „unter Berücksichtigung nachrichtendienstlicher bzw. polizeilicher Erfahrung zu würdigen. Kriterien für eine derartige Verbindung können beispielsweise die nähere persönliche Beziehung, (...) die Dauer der Verbindung (...) sein (...). Äußerlich flüchtige oder zufällige Alltagskontakte reichen nicht aus.“ (a.a.O.).

Demnach ist z.B. für eine entsprechende Qualifizierung als Kontaktperson eine – ggf. nur kurzfristige oder einmalige - “nähere persönliche Beziehung” (a.a.O.) von äußerlich flüchtigen oder zufälligen Alltagskontakten abzugrenzen.



Bei objektiv mehrdeutigen Sachverhalten ist diese Bewertung vielfach nicht (hinreichend) trennscharf zu gewährleisten, so dass auch unbescholtene Personen auf der Grundlage eines objektiv mehrdeutigen Sachverhalts als Kontaktpersonen in der Rechtsextremismus-Datei gespeichert werden könnten (vgl. auch Geiger, a.a.O., S. 7).

Zudem ist zu berücksichtigen, dass in der Rechtsextremismus-Datei gemäß Artikel 1 § 2 Satz 1 RED-G auch sensible weiche, d.h. auf ungesicherten Erkenntnissen beruhende, personenbezogene Daten der Nachrichtendienste (BfV, MAD, LfV) gespeichert werden müssen, die von den Diensten im Vorfeldbereich der Gefahrenabwehr auf der Grundlage bereichsspezifischer Eingriffsschwellen erhoben worden sind. Infolge der im Vorfeldbereich bestehenden hohen Ambivalenz der potentiellen Bedeutung einzelner Verhaltensumstände (vgl. BVerfG, 1 BvR 668/04 vom 27.07.2005, Rdn. 121) ist es die spezifische Aufgabe der Nachrichtendienste, auch Daten von Personen zu erheben, deren Verhalten nicht nur zum Erfassungszeitpunkt, sondern auch bei weiterer Beobachtung vollkommen legal sein kann. Insofern können auch Unbescholtene, d.h. sich rechtmäßig verhaltende Personen, in den Focus der Nachrichtendienste geraten. Dies ist eine zwangsläufige Folge der den Nachrichtendiensten gewährten Befugnis zur Datenerhebung im Vorfeldbereich.

#### **IV. Artikel 1 § 3 Abs. 1 Nr. 1 Buchstabe b RED-G**

Verfassungsrechtlich kritisch zu bewerten ist auch die in § 3 Abs. 1 Nr. 1 Buchstabe b) RED-G vorgesehene Speicherung erweiterter Grunddaten von sogenannten „dolos“ Kontaktpersonen. Im Eilfall wird auf diese Erkenntnisse unmittelbar zugegriffen (vgl. § 5 Abs. 2 Satz 1 RED-G).

Bereits die Speicherung von Grunddaten in der Rechtsextremismus-Datei ist ein erheblicher Eingriff in das Recht der Betroffenen auf informationelle Selbstbestimmung mit potentiell weit reichenden Folgen (s.o. B. I). Die Intensität dieses Eingriffs wird durch die Speicherung erweiterter Grunddaten verstärkt.



Die gemäß § 3 Abs. 1 Nr. 1 Buchstabe b RED-G zur Speicherung erweiterter Grunddaten notwendige Differenzierung zwischen Kontaktpersonen, „bei denen Tatsachen die Annahme rechtfertigen, dass sie von der Planung oder Begehung einer in § 2 Satz 1 Nr. 1 Buchstabe b RED-G genannten Straftat oder der Ausübung, Unterstützung oder Vorbereitung von rechtsextremistischer Gewalt im Sinne von § 2 Satz 1 Nr. 2 RED-G Kenntnis haben“ und Kontaktpersonen, die über diese Kenntnis nicht verfügen, ist in der Praxis oftmals nicht (hinreichend) trennscharf umsetzbar. Dies ist insbesondere der Fall, wenn lediglich aufgrund objektiv mehrdeutiger (Verhaltens-)Umstände auf das vermeintliche Vorliegen dieser Kenntnis geschlossen werden kann.

Meine Kontrollerfahrungen in Bezug auf die praktische Umsetzung des ATDG bestätigen dies. Es besteht die erhebliche Gefahr, dass in derartigen Fällen - gemäß der Maxime „in dubio pro Speicherung“ - auch erweiterte Daten zu Kontaktpersonen gespeichert werden, die über keine entsprechende Kenntnis im Sinne des § 3 Abs. 1 Nr. 1 Buchstabe b RED-G verfügen (vgl. auch Geiger, a.a.O., S. 7).

## **V. Artikel 1 § 7 RED-G**

Abweichend von der Konzeption des ATDG gewährt § 7 Abs. 1 Satz 1 RED-G den an der Rechtsextremismus-Datei beteiligten Behörden die Befugnis zur erweiterten Nutzung der in dieser Datei gespeicherten Daten zum Zweck der Erfüllung ihrer jeweiligen gesetzlichen Aufgaben.

Nach der Entwurfsbegründung (S. 19) ist diese systematische Datennutzung „angesichts der Bedrohungen durch den gewaltbezogenen Rechtsextremismus“ (a.a.O.) notwendig. Zur Begründung wird u.a. auf die „Nachbereitung von Vorfällen (wie z.B. der „Ceska“-Morde bzw. der Morde des „Zwickauer Trios““ (a.a.O.) verwiesen.

Inwieweit diese behauptete Notwendigkeit besteht und ob sie einen derart weitgehenden, intensiven Grundrechtseingriff zu legitimieren vermag, ist – auch aufgrund der noch nicht abgeschlossenen detaillierten Untersuchungen der (aktuellen) Vorgänge - nicht verifizierbar.

Zum Ausgleich der behaupteten Defizite sollen die Daten „für eng umgrenzte Projekte befristet genutzt werden können. Der Projektcharakter ist dabei wesentliches



rechtsstaatliches Element“ (GE-Begründung, S. 19). Ausgehend von dieser Prämisse habe ich Zweifel an der Erforderlichkeit dieser Regelung.

Seit dem Inkrafttreten des Gesetzes zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz) vom 22. Dezember 2006 besteht die Befugnis zur Errichtung zeitlich befristeter gemeinsamer Projektdateien unter Federführung des Bundesamtes für Verfassungsschutz (BfV), des Bundesnachrichtendienstes (BND) oder des Bundeskriminalamtes (BKA) (vgl. Artikel 2 bis 4 Gemeinsame-Dateien-Gesetz). In diesen Projektdateien dürfen auch über den Anwendungsbereich des RED-G hinausgehende Daten verarbeitet werden (vgl. § 22 Buchstabe a BVerfSchG; § 9 Buchstabe a BNDG; § 9 Buchstabe a BKAG).

Zur Wahrung der Verfassungsmäßigkeit einer derart projektbezogenen Zusammenarbeit zwischen Polizeien und Nachrichtendiensten hat der Gesetzgeber im Gemeinsame-Dateien-Gesetz festgelegt, dass für die Eingabe personenbezogener Daten in derartige Projektdateien die jeweiligen Übermittlungsvorschriften zugunsten der an der Zusammenarbeit beteiligten Behörden entsprechend gelten mit der Maßgabe, dass die Eingabe eines personenbezogenen Datums nur zulässig ist, wenn die Daten allen an der projektbezogenen Zusammenarbeit teilnehmenden Behörden übermittelt werden dürfen (vgl. z.B. § 22 Buchstabe a Abs. 2 Satz 1 BVerfSchG).

Der vorliegende Entwurf des RED-G enthält keine entsprechende Beschränkung.

#### **VI. Artikel 1 § 11 Abs. 2 Satz 2 RED-G**

Nach Artikel 1 § 11 Abs. 2 Satz 2 RED-G richtet sich die Auskunft zu verdeckt gespeicherten Daten nach den für die Behörde, die die Daten eingegeben hat, geltenden Rechtsvorschriften.

In der Entwurfsbegründung wird die Anwendung dieser Regelung wie folgt konkretisiert: „Wendet sich der Betroffene mit seinem Auskunftersuchen zunächst an das BKA, hat es in seiner Auskunftserteilung darauf hinzuweisen, dass sich diese nur auf nicht verdeckt gespeicherte Daten bezieht. Zusätzlich nennt das BKA bei der Auskunftserteilung die an der Datei beteiligten Behörden, die die Betroffenen um Auskunft zu einer etwaigen verdeckten Speicherung ersuchen können.“ (GE-Begründung, S. 21).



Demnach muss ein Betroffener in diesen Fällen sein Auskunftersuchen entgegen dem in § 11 Abs. 2 Satz 1 RED-G für nicht verdeckte Datenspeicherungen geregelten Verfahren nicht an das die Rechtsextremismus-Datei führende und im Außenverhältnis handelnde BKA, sondern an alle an der Rechtsextremismus-Datei teilnehmenden Behörden richten (vgl. GE-Begründung, S. 21). Entsprechendes gilt auch für die ATD. An dieser sind derzeit (Stand: 13. März 2012) achtunddreißig Behörden beteiligt.

Angesichts der Bedeutung des Auskunftsanspruchs zur Gewährleistung des durch Art. 19 Abs. 4 GG garantierten Rechtsschutzes bestehen hiergegen erhebliche verfassungsrechtliche Bedenken im Hinblick auf die Effektivität der Rechtsschutzgewährung.

Ein hinreichend effektiver Rechtsschutz gegen Eingriffe in das Recht auf informationelle Selbstbestimmung setzt voraus, dass ein Betroffener von diesen Eingriffen überhaupt Kenntnis erlangen kann (vgl. BvR 1550/03 vom 13.06.2007, Rdn. 168 m.w.N.).

Vorliegend ist diese Kenntniserlangung nur möglich, sofern sich der Betroffene an alle an der Rechtsextremismus-Datei beteiligte Stellen wendet und dort Auskunftersuchen stellt. Im Falle von Auskunftsverweigerungen bzw. unzureichenden Auskunftserteilungen müsste er gegebenenfalls eine Vielzahl entsprechender Bescheide im Widerspruchs- und Klageverfahren überprüfen lassen.

Angesichts der Vielzahl der an der Antiterrordatei beteiligten Behörden, deren Anzahl gemäß § 1 Abs. 2 ATDG zukünftig weiter anwachsen kann, ist diese Vorgehensweise für den Betroffenen mit einem erheblichen - auch finanziellen - Aufwand verbunden und daher im Hinblick auf eine effektive Rechtsschutzgewährung unangemessen.

Sofern Auskunftsansprüche den Rechten eines Betroffenen nicht angemessen Rechnung tragen, besteht im Falle einer heimlichen Datenerhebung die Pflicht zur Benachrichtigung des Betroffenen (vgl. 1 BvR 1550/03, Rdn. 170 m.w.N.; BVerfGE 65, 1 (70)). Eine entsprechende Benachrichtigungsregelung sieht der Entwurf des RED-G nicht vor.



Infolgedessen sollte das BKA auch für Auskunftersuchen zu verdeckt gespeicherten Daten im Zusammenwirken mit den beteiligten Behörden zumindest in der Weise als zentrale Auskunftsstelle fungieren, dass ein Auskunftersuchen auch zu verdeckten Speicherungen nur beim BKA gestellt werden muss und dieses das Ersuchen allen beteiligten Stellen mit der Bitte um Rückmeldung etwaiger zu beauskunftender Informationen zuleitet und gegenüber dem Betroffenen im Außenverhältnis als alleiniger Ansprechpartner fungiert.

## VII. Artikel 2

Ziel des Gesetzentwurfs ist die Bekämpfung des „gewaltbezogenen“ Rechtsextremismus. Die „Besonderheiten dieses Phänomenbereichs“ (Punkt C des Vorblattes) „fordern“ (a.a.O) ein Handeln des Gesetzgebers.

1. Bereits nach geltendem Recht (vgl. § 6 Satz 8 BVerfSchG) ist dieser besondere Phänomenbereich im Nachrichtendienstlichen Informationssystem (NADIS) umfassend speicherbar.

Der Begriff „Bestrebungen“ (§ 6 Satz 8 BVerfSchG) wird in § 4 Abs. 1 Satz 1 BVerfSchG konkretisiert. Danach ist nicht nur das Handeln für einen Personenzusammenschluss, sondern auch das Verhalten von Einzelpersonen NADIS-relevant. Erforderlich ist, dass dieses Verhalten auf die Anwendung von Gewalt gerichtet oder aufgrund seiner Wirkungsweise geeignet ist, ein in dieser Norm genanntes Schutzgut erheblich zu beschädigen.

2. Begründet wird die Novellierung mit einer „sich in der Realität nicht widerspiegelnden trennscharfen Unterscheidung zwischen gewaltfreien und gewaltbezogenen Bestrebungen“ (GE-Begründung, S. 22). Diese Behauptung steht in Widerspruch zur vorgenannten Zielsetzung und Prämisse, nur den besonderen Phänomenbereich des „gewaltbezogenen“ Rechtsextremismus gesetzlichen Neuregelungen zu unterwerfen. Zudem fehlen für diese Behauptung valide, überprüfbare Erkenntnisgrundlagen.

Ergänzende Ausführungen im Rahmen der mündlichen Anhörung behalte ich mir vor.