Prof. Dr. Matthias Bäcker, LL.M.
Universität Mannheim
Abteilung Rechtswissenschaft
Schloss
68131 Mannheim

Mannheim, den 17. September 2014

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)144 B

Stellungnahme

zu dem Entwurf eines Gesetzes zur Änderung des Antiterrordateigesetzes
und anderer Gesetze

(BT-Drs. 18/1565)

Gliederung

Ergebnisse

1. Der Gesetzentwurf beseitigt nicht alle verfassungsrechtlichen Defizite des ATDG und des RED-G, die sich aus dem Urteil des Bundesverfassungsgerichts zum ATDG ergeben.

   a) Die vorgesehene Betroffenenregelung des § 2 Satz 1 Nr. 2 ATDG-E ist immer noch sehr weit gefasst und droht die kommunikative Privatsphäre zu verletzen, soweit sie an ein Befürworten von Gewalt anknüpft. Rechtstechnisch erscheint es darüber hinaus angezeigt, die Betroffenenregelungen in § 2 Satz 1 Nr. 2 ATDG sowie § 2 Satz 1 Nr. 1 und 2 RED-G hinsichtlich der Begriffe der „Gewalt“, der „rechtsextremistischen Gewalttat“ und des „vorsätzlichen Hervorrufens“ einzugrenzen und so die vom Bundesverfassungsgericht geforderte restriktive Auslegung dieser Begriffe ausdrücklich vorzugeben.

   b) Der Entwurf belässt in § 3 Abs. 1 Nr. 1 RED-G mehrere Kategorien zu speichernder Daten, die so weit und offen gefasst sind, dass Grundrechte der Betroffenen verletzt werden.

   c) Die vorgesehenen Regelungen in § 4 Abs. 3 ATDG-E und § 4 Abs. 3 RED-G-E zum Schutz von Daten, die durch besonders eingriffsintensive Datenerhebungsmaßnahmen gewonnen wurden, sind zu eng. Sie müssen auch Daten erfassen, die aus einer Erhebung von Telekommunikations-Verkehrsdaten stammen.

2. Die vorgesehenen Ermächtigungen zu erweiterten Datennutzungen in § 6a ATDG-E und § 7 RED-G-E sind zu weit gefasst und stehen mit den Grundrechten der Betroffenen nicht in Einklang.

3. Der Gesetzentwurf zieht nur unvollständige Schlüsse aus dem Urteil des Bundesverfassungsgerichts, da er allein das ATDG und das RED-G behandelt. Dringend reformbedürftig sind nach dem Urteil insbesondere die viel zu weitreichenden und zu unbestimmten Datenübermittlungsvorschriften des Nachrichtendienstrechts. Darüber hinaus liegt es aufgrund des Urteils zumindest nahe, die Tätigkeit der Gemeinsamen Zentren mehrerer Sicherheitsbehörden von Bund und Ländern ausdrücklich gesetzlich zu regeln.

Der Gesetzentwurf verfolgt zwei Regelungsziele, die ich im Folgenden getrennt voneinander behandle: Zum einen sollen die verfassungsrechtlichen Defizite von ATDG und RED-G behoben werden, die sich aus dem Urteil des Bundesverfassungsgerichts zum ATDG ergeben (unten I.). Zum anderen soll eine erweiterte Datennutzung auch für die Antiterrordatei eingeführt werden; für die Rechtsextremismus-Datei werden die Voraussetzungen einer erweiterten Datennutzung modifiziert (unten II.).

Daneben fällt auf, dass der Entwurf in seinem Gegenstand sehr eng zugeschnitten ist und sich auf das ATDG sowie das RED-G begrenzt. Dabei hätte sich nach dem Urteil des Bundesverfassungsgerichts aufgedrängt, auch bestimmte Regelungen außerhalb dieser beiden Gesetze zu überarbeiten beziehungsweise bestimmte Fragen überhaupt erstmals gesetzlich zu regeln (unten III.).

I. Behebung verfassungsrechtlicher Mängel von ATDG und RED-G

Die meisten der vorgesehenen Regelungen zielen darauf ab, die verfassungsrechtlichen Mängel zu beheben, die das Bundesverfassungsgericht in seinem Urteil vom 24. April 2013[1] für das ATDG festgestellt hat und die sich weitgehend auch im RED-G finden. Dieses Ziel wird überwiegend erreicht. Allerdings verblieben auch nach Inkrafttreten des Gesetzentwurfs noch einzelne verfassungsrechtliche Mängel sowie weitere Unstimmigkeiten, die zwar nicht zu Verfassungsverstößen führen, aber unter rechtstechnischen Gesichtspunkten ausgeräumt werden sollten. Diese Defizite des Entwurfs führe ich im Folgenden aus.

1. Betroffene Personen, § 2 ATDG-E und § 2 RED-G

Der Entwurf sieht vor, § 2 Satz 1 Nr. 2 ATDG insoweit zu ändern, als Personen in die Antiterrordatei aufgenommen werden konnten, die eine rechtswidrige Gewaltanwendung zu bestimmten Zielen befürworten. Denn nach dem Urteil des Bundesverfassungsgerichts reicht eine bloße innere Haltung nicht aus, um eine Datenspeicherung zu legitimieren. Demgegenüber bestünden keine grundsätzlichen Bedenken dagegen, „Hassprediger“ in die Datei aufzunehmen, die öffentlich zu Hass und Gewalt anstachelten.[2]

§ 2 Satz 1 Nr. 2 ATDG-E soll nunmehr eine Datenspeicherung daran knüpfen, dass der Betroffene voraussichtlich eine Gewaltanwendung durch seine Tätigkeiten vorsätzlich hervorruft. Als Regelbeispiel für solche Tätigkeiten soll die Norm das „Befürworten solcher Gewaltanwendungen“ nennen.

Auch mit dieser Änderung verbliebe die Regelung verfassungsrechtlich zumindest problematisch. Die Speicherungsermächtigung beschränkte sich nach wie vor nicht auf „Hassprediger“. Sondern sie würde auch Personen umfassen, die sich lediglich privat im kleinen Kreis positiv über eine Gewaltanwendung zu bestimmten Zielen äußern. Zwar könnte eine Datenspeicherung so – anders als nach der bisherigen Normfassung – nicht mehr allein an das Forum Internum des Einzelnen anknüpfen. Die Speicherung könnte jedoch die staatsfreie kommunikative

[1] BVerfGE 133, 277.

[2] BVerfGE 133, 277 (347 f.).

Privatsphäre verletzen.[3] Insbesondere Gewalt befürwortende Äußerungen im Kreis enger Vertrauenspersonen mögen unerfreulich sein, rechtfertigen jedoch für sich genommen keine staatlichen Eingriffsmaßnahmen.

Allerdings müssten nach § 2 Satz 1 Nr. 2 ATDG-E auch tatsächliche Anhaltspunkte dafür sprechen, dass diese Äußerungen eine Gewaltanwendung hervorrufen werden und dass die Betroffenen dies wollen. Ob damit ein hinreichend enger Zurechnungszusammenhang zwischen Äußerungen und Gewaltanwendung formuliert wird, der ein staatliches Eindringen in die kommunikative Privatsphäre ausnahmsweise rechtfertigen könnte, erscheint jedoch fragwürdig. Denn es wäre nicht ausgeschlossen, ein solches Hervorrufen selbst bei komplexen Kausalverläufen zu bejahen, in deren Rahmen die Äußerungen nur eine untergeordnete Bedeutung für die drohende Gewaltanwendung haben. Zudem erforderten diese einschränkenden Tatbestandsmerkmale eine Prognose zukünftiger Entwicklungen und eine Einschätzung der Willensrichtung des Betroffenen, die beide auf sehr ungewisser Basis beruhten. Es ist zweifelhaft, ob der gesetzliche Ermächtigungstatbestand auf diese Weise zuverlässig begrenzt wird.

Um die Speicherungsermächtigung demgegenüber zuverlässig auf „Hassprediger“ zu begrenzen und so ihre Verfassungskonformität sicherzustellen, sollte die Regelung präziser gefasst werden. Verfassungsrechtlich tragfähig wäre es etwa zu fordern, dass nach den vorliegenden tatsächlichen Anhaltspunkten der Betroffene zu rechtswidriger Gewaltanwendung „öffentlich aufruft“.

Daneben erscheint es regelungstechnisch angezeigt, die Betroffenenregelungen in § 2 Satz 1 Nr. 2 ATDG und § 2 Satz 1 Nr. 1 und 2 RED-G zu präzisieren. Diese Normen enthalten mit den Begriffen der „Gewalt“, der „rechtsextremistischen Gewalttat“ und des „vorsätzlichen Hervorrufens“ rechtswidriger Gewaltanwendung Tatbestandsmerkmale, die sehr weit interpretiert werden könnten und dann das Übermaßverbot verletzten. Zwar hat das Bundesverfassungsgericht – bei Stimmengleichheit im Senat – die Tatbestandsmerkmale der „Gewalt“ und des „vorsätzlichen Hervorrufens“ in § 2 Satz 1 Nr. 2 ATDG gleichwohl nicht beanstandet. Es hat dazu jedoch jeweils eine verfassungskonforme Auslegung gefordert. Danach ist unter „Gewalt“ nur solche Gewalt zu verstehen, die „unmittelbar gegen Leib und Leben gerichtet oder durch den Einsatz gemeingefährlicher Mittel geprägt ist“. Ein „vorsätzliches Hervorrufen“ von Gewalt setzt ein willentliches Handeln voraus.[4] Es liegt nahe, diese Einengungen in den Gesetzestext aufzunehmen und so Rechtssicherheit zu schaffen. Ein Grund, die überschießend weiten bisherigen Tatbestandsfassungen beizubehalten, ist demgegenüber nicht ersichtlich.

2. Zu speichernde Datenkategorien, § 3 RED-G-E

Das Bundesverfassungsgericht hat die Kategorien der erweiterten Grunddaten in § 3 ATDG insoweit beanstandet, als einige davon in transparenter Weise näher bestimmt werden müssen.

---

[3] Vgl. zur Gewährleistung eines kommunikativen Privatbereichs mit Blick auf den Ehrschutz, aber im Ansatz verallgemeinerbar BVerfGE 90, 255 (259 ff.).

[4] BVerfGE 133, 277 (341 ff.).

Dies setzt zumindest voraus, dass konkretisierende Vorgaben der Verwaltung dokumentiert und veröffentlicht werden.[5]

Der Gesetzentwurf setzt dies für die vom Bundesverfassungsgericht aufgeführten Datenkategorien in § 3 Abs. 4 ATDG-E und § 3 Abs. 4 RED-G-E um. Damit stellt der Entwurf für die Antiterrordatei insoweit einen verfassungskonformen Zustand her.

Hingegen geht der Entwurf für die Rechtsextremismus-Datei nicht weit genug. Denn § 3 Abs. 1 Nr. 1 Buchstabe b RED-G ordnet die Speicherung mehrerer Datenkategorien an, die in § 3 Abs. 1 Nr. 1 Buchstabe b ATDG keine Gegenstücke haben. Hinsichtlich dieser Datenkategorien bestehen teils erhebliche Zweifel, ob die Norm den verfassungsrechtlichen Geboten der Bestimmtheit und Verhältnismäßigkeit genügt. Einige von ihnen sind sehr weit gefasst und könnten den Grundrechtsgebrauch der Betroffenen empfindlich treffen. Dies gilt insbesondere für § 3 Abs. 1 Nr. 1 Buchstaben b qq und rr RED-G, die eine Speicherung der Teilnahme an rechtsextremistischen Veranstaltungen und des Besitzes oder Erstellens rechtsextremistischer Medien in größeren Mengen vorsehen, ohne dass es nach dem Gesetzeswortlaut darauf ankäme, ob es sich hierbei um grundrechtlich besonders geschützte[6] rechtmäßige Tätigkeiten handelt.[7] Sehr offen gehalten sind auch § 3 Abs. 1 Nr. 1 Buchstaben b tt und uu RED-G, die praktisch jede Beteiligung an rechtsextremistischen Zusammenschlüssen erfassen. Wenn diese Regelungen überhaupt für verfassungsrechtlich tragfähig gehalten werden,[8] so müssen sie deutlich präzisiert und eingeengt werden. Daher ist wenigstens zu fordern, dass auch für diese Datenkategorien eine konkretisierende Verwaltungsvorschrift erstellt und veröffentlicht wird. Zumindest sollte daher der Anwendungsbereich von § 3 Abs. 4 RED-G-E auf diese Datenkategorien erstreckt werden.

3. Speicherung von Daten aus Eingriffen in Art. 10 GG, § 4 ATDG-E und § 4 RED-G-E

Das Bundesverfassungsgericht hat gefordert, Daten besonders zu schützen, die durch Eingriffe in die besonderen Vertraulichkeitsgarantien aus Art. 10 GG, Art. 13 GG und Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG in seiner Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gewonnen wurden.[9]

Der Gesetzentwurf zählt hierzu in § 4 Abs. 3 ATDG-E und § 4 Abs. 3 RED-G-E bundesrechtliche Befugnisregelungen auf, die zu verdeckten Eingriffen in diese Grundrechte ermächtigen. Daten, die durch Maßnahmen nach diesen Befugnisregelungen oder nach gleichartigen landesrechtlichen Regelungen gewonnen wurden, müssen i.S.v. § 4 Abs. 1 ATDG bzw. § 4 Abs. 1 RED-G verdeckt gespeichert werden.

---

[5] BVerfGE 133, 277 (354 ff.).

[6] Insbesondere durch Art. 5, Art. 8 und Art. 21 GG.

[7] Die Gesetzesbegründung zu § 3 RED-G führt ohne Stütze im Gesetzestext aus, das Tatbestandsmerkmal der „sonstigen Veranstaltungen“ in § 3 Abs. 1 Buchstabe b qq erfasse „nicht die Teilnahme an rechtmäßigen Versammlungen und Kundgebungen oder rechtmäßigen Parteiveranstaltungen“, BT-Drs. 17/8672, S. 16. Damit wird in der Sache bereits in dieser Begründung eine verfassungskonforme restriktive Auslegung der Norm propagiert, die angesichts der hohen Anforderungen des Bestimmtheitsgrundsatzes an Datenverarbeitungsermächtigungen zumindest fragwürdig erscheint.

[8] Zu § 3 Abs. 1 Nr. 1 Buchstaben b qq und rr RED-G sehr kritisch *Arzt*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014 (im Erscheinen), § 3 RED-G Rn. 22 f.

[9] BVerfGE 133, 277 (372 ff.).

Die Vorgabe einer verdeckten Speicherung ist ein verfassungsrechtlich tragfähiges Schutzkonzept.[10] Jedoch sind die Regelungskataloge in § 4 Abs. 3 ATDG-E und § 4 Abs. 3 RED-G-E zu eng gefasst, so dass Schutzdefizite verbleiben. Denn diese Kataloge führen nicht die bundesrechtlichen Ermächtigungen zu verdeckten Erhebungen von Telekommunikations-Verkehrsdaten auf, die sich in § 100g StPO, § 20m BKAG, § 23g ZFdG und § 8a Abs. 2 Satz 1 Nr. 4 BVerfSchG (ggfs. i.V.m. § 2a BNDG oder § 4a MADG) finden.[11]

Verkehrsdatenerhebungen greifen jedoch intensiv in das Grundrecht aus Art. 10 GG ein, da sie weitreichende Einblicke in Kommunikationsverhalten, soziale Kontakte und Lebensgestaltung der Betroffenen ermöglichen.[12] Insbesondere wenn Verkehrsdaten über einen längeren Zeitraum zusammengetragen und systematisch ausgewertet werden, bleibt die Eingriffsintensität hinter einer inhaltsbezogenen Telekommunikationsüberwachung allenfalls geringfügig zurück.

Die durch Verkehrsdatenerhebungen gewonnenen Daten sind auch mit Blick auf die Ausgestaltung der beiden Dateien ebenso schutzbedürftig wie Daten, die aus inhaltsbezogenen Überwachungen stammen. Das Bundesverfassungsgericht hat den bisherigen Rechtszustand mit Blick auf die Antiterrordatei deshalb beanstandet, weil danach Daten aus Eingriffen in besondere Vertraulichkeitsgarantien unter Umständen als Grunddaten i.S.v. § 3 Abs. 1 Nr. 1 Buchstabe a ATDG zu speichern waren und deshalb durch eine Suchabfrage ohne weiteres als Klartext recherchiert werden konnten.[13] Dieses Risiko besteht für Daten aus Verkehrsdatenerhebungen ebenso wie für Daten aus inhaltsbezogenen Überwachungsmaßnahmen.[14] Beispielsweise kann eine Verkehrsdatenerhebung dazu dienen, die sozialen Kontakte eines bekannten „Gefährders“ zu erschließen, um eine komplexe terroristische oder extremistische Struktur auszuleuchten. Hierdurch können weitere mutmaßliche Strukturangehörige bekannt werden, deren Daten dann gleichfalls in der Datei zu speichern sind. Die Grunddaten dieser weiteren Personen stammen aus der Verkehrsdatenerhebung und unterliegen besonderen verfassungsrechtlichen Schutzanforderungen.[15] Der Entwurf verfehlt diese Anforderungen derzeit.

---

[10] BVerfGE 133, 277 (374 f.).

[11] Mit der Gesetzesbegründung halte ich es hingegen für unbedenklich, dass die Schutzregelung keine Daten erfasst, die durch offene Ermittlungsmaßnahmen gewonnen wurden. Weiter müssen meines Erachtens auch Daten aus Telekommunikations-Bestandsdatenerhebungen nicht besonders geschützt werden. Bestandsdatenerhebungen greifen zwar nach der Rechtsprechung des Bundesverfassungsgerichts im Sonderfall der Zuordnung einer dynamischen IP-Adresse in das Grundrecht aus Art. 10 GG ein, so BVerfGE 130, 151 (181 f.). Dabei handelt es sich jedoch um einen Eingriff von deutlich geringerer Intensität als bei Telekommunikationsüberwachungen oder Verkehrsdatenabrufen, vgl. BVerfGE 125, 260 (340 ff.). Dieser Eingriff in das Fernmeldegeheimnis erzeugt im Vergleich zu Eingriffen in das Recht auf informationelle Selbstbestimmung keinen so herausgehobenen Schutzbedarf, dass zwingend eine verdeckte Speicherung der gewonnenen Daten angezeigt wäre.

[12] BVerfGE 107, 299 (318 ff.); 113, 348 (383); vgl. zur Bevorratung solcher Daten BVerfGE 125, 260 (318 ff.).

[13] Vgl. BVerfGE 133, 277 (374).

[14] Das Bundesverfassungsgericht nennt insoweit beispielhaft ein bei einer Abhörmaßnahme in Erfahrung gebrachtes besonderes körperliches Merkmal oder einen seltenen Dialekt, BVerfGE 133, 277 (374).

[15] Ohne Belang ist, ob es noch weiterer Maßnahmen – etwa Bestandsdatenerhebungen – bedarf, um die erhobenen Verkehrsdaten bestimmten Personen zuzuordnen. Der grundrechtliche Schutzbedarf besteht über solche Zwischenschritte hinaus fort. Dementsprechend sind alle Verarbeitungen von Daten, die einmal durch einen Eingriff in Art. 10 GG gewonnen wurden, nach der ständigen Rechtsprechung des Bundesverfassungsgerichts

II. Erweiterte Datennutzung nach § 6a ATDG-E und § 7 RED-G-E

Der Gesetzentwurf sieht vor, durch § 6a ATDG-E den Funktionsumfang der Antiterrordatei auszubauen, indem nach dem Vorbild von § 7 RED-G eine erweiterte Nutzung dieser Datei ermöglicht wird. Die materiellen und formellen Vorgaben für diese erweiterte Nutzung weichen in Details von dem bisherigen § 7 RED-G ab. Insoweit sieht der Entwurf vor, § 7 RED-G an den neuen § 6a ATDG-E anzupassen.

Jedoch stehen § 6a ATDG-E und § 7 RED-G-E – ebenso wie schon der bisherige § 7 RED-G[16] – mit dem Recht auf informationelle Selbstbestimmung nicht in Einklang. Eine erweiterte Dateinutzung ist insbesondere dann als besonders schwerer Eingriff in dieses Grundrecht anzusehen, wenn die Nutzung einem präventivpolizeilichen oder strafprozessualen Zweck dient. An Ermächtigungen zu einer solchen Nutzung bestehen hohe verfassungsrechtliche Anforderungen. Die Vorgaben, die § 6a Abs. 1 ATDG-E und der weitgehend damit übereinstimmende § 7 Abs. 1 RED-G-E errichten, verfehlen diese Anforderungen deutlich.

1. Verfassungsrechtliche Anforderungen an eine erweiterte Nutzungsermächtigung

Der Entwurf definiert den Begriff der erweiterten Nutzung in § 6a Abs. 2 ATDG-E wortlautgleich mit § 7 Abs. 2 RED-G. Danach handelt es sich um komplexere informationstechnische Auswertungen, mit denen eine teilnehmende Behörde aus den gespeicherten Daten neue Informationen etwa über geografische oder soziale Zusammenhänge gewinnen soll.[17]

Die erweiterte Dateinutzung geht in Ausmaß und Qualität deutlich über die Nutzungen hinaus, welche die beiden Gesetze ansonsten zulassen.

Die Dateien werden in diesem Rahmen nicht als bloße Indexdateien genutzt, wie es § 5 Abs. 1 ATDG und § 5 Abs. 1 RED-G grundsätzlich vorsehen. Sondern eine teilnehmende Behörde erhält unmittelbar Zugriff auf die gespeicherten Daten (mit Ausnahme verdeckter Speicherungen), um diese Daten zur Aufgabenwahrnehmung zu nutzen.

Zumindest mit Blick auf den gesetzlichen Normalfall übersteigt die Reichweite der Zugriffsbefugnis auch die Eilfallermächtigungen in § 5 Abs. 2 ATDG und § 5 Abs. 2 RED-G deutlich:

Die Eilfallermächtigungen dienen primär dazu, einer teilnehmenden Behörde bei einer punktuellen Suchanfrage nach einer Person unmittelbar Zugriff auf die erweiterten Grunddaten zu verschaffen. Insoweit bilden die Dateien technische Plattformen für vereinfachte und beschleunigte Datenübermittlungen zwischen den teilnehmenden Behörden. Daneben ist zwar auch eine Inverssuche möglich, die von einem gespeicherten Merkmal aus den erweiterten

---

gleichfalls an diesem Grundrecht zu messen, so BVerfGE 100, 313 (359); 110, 33 (68 f.); 113, 348 (365); 125, 260 (313).

[16] Kritisch zu dieser Norm haben sich bereits mehrere der seinerzeit von dem Innenausschuss des Deutschen Bundestags angehörten Sachverständigen geäußert, vgl. die Stellungnahmen von *Poscher*, BT-Ausschussdrs. 17(4)460 D, S. 11 f.; *Roggan*, BT-Ausschussdrs. 17(4)460 C, S. 7; *Wolff*, BT-Ausschussdrs. 17(4)460 B, S. 8 f.

[17] Die Begründung zu § 7 RED-G nennt beispielhaft „die kartenmäßige, grafische oder sonstige Darstellung von Tatorten sowie Aufenthaltsorten der Verdächtigen, die Darstellung von Beziehungsgeflechten der Verdächtigen, der räumlichen Verteilung sowie von Reiseaktivitäten des rechtsextremistischen Personenpotenzials“, BT-Drs. 17/8672, S. 19.

Grunddaten und nicht von einer bestimmten Person ausgeht.[18] Eine solche Suche setzt jedoch immerhin noch voraus, dass die suchende Behörde eine Vorstellung davon hat, auf welche Ausprägung welches Merkmals es ihr ankommt.

Hingegen sollen die Dateien im Rahmen erweiterter Nutzungen den teilnehmenden Behörden als Datenpools dienen, aus denen sie mit praktisch allen informationstechnisch möglichen Methoden weitreichende Erkenntnisse schöpfen können. Dies schließt etwa mehrstufige Analysen ein, die zunächst Verdachtsmomente überhaupt erst hervorbringen sollen, auf denen dann weitere Analyseschritte aufbauen. Eine teilnehmende Behörde kann so mittels einer erweiterten Nutzung Informationen erzeugen, die sie mit Hilfe gezielter Übermittlungsersuchen oder einzelner Suchabfragen nicht beschaffen könnte, weil sie im Voraus nicht genau angeben könnte, welche Daten sie benötigt.

Die Ermächtigungen zu erweiterten Nutzungen heben damit das von dem Bundesverfassungsgericht begründete informationelle Trennungsprinzip zwischen Nachrichtendiensten und Polizeibehörden[19] bereichsspezifisch auf und ersetzen es durch ein informationelles Verfügbarkeitsprinzip. Hierin liegt dann, wenn eine operativ tätige Polizeibehörde eine der beiden Dateien erweitert nutzt, ein besonders schwerer Grundrechtseingriff.[20] An die Eingriffsrechtfertigung sind daher gleichartige Anforderungen zu stellen wie bei anderen besonders schwerwiegenden Eingriffsmaßnahmen. Als Referenzmaßnahmen aus der bisherigen Rechtsprechung des Bundesverfassungsgerichts sind vor allem Wohnraumüberwachungen, „Online-Durchsuchungen“ und die Nutzung bevorrateter Telekommunikations-Verkehrsdaten zu nennen.

Eine erweiterte Dateinutzung zur Strafverfolgung setzt danach von Verfassungs wegen den Verdacht einer besonders schweren Straftat voraus, deren Gewicht den mittleren Kriminalitätsbereich deutlich übersteigt.[21] Eine präventivpolizeiliche Nutzung darf nur zur Abwehr einer konkreten Gefahr für ein überragend wichtiges Rechtsgut erlaubt werden.[22]

Weniger hohe Anforderungen bestehen hingegen dann, wenn ein Nachrichtendienst eine der Dateien erweitert nutzen soll. Denn das informationelle Trennungsprinzip ist primär auf Informationsflüsse von Nachrichtendiensten zu Polizeibehörden zugeschnitten. Solche Informationsflüsse sind grundrechtlich besonders riskant, da hier die weitreichenden informationellen Vorfeldbefugnisse der Nachrichtendienste mit den weitreichenden Zwangsbefugnissen der Polizeibehörden zusammentreffen.[23] Dementsprechend hat das Bundesverfassungsgericht

---

[18] Dies hält angesichts der hohen tatbestandlichen Voraussetzungen ausdrücklich für verfassungsgemäß BVerfGE 133, 277 (364).

[19] BVerfGE 133, 277 (329).

[20] Wie hier *Arzt*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014 (im Erscheinen), § 7 RED-G Rn. 4; ebenso bereits zu der weniger weitreichenden Eilfallermächtigung in § 5 Abs. 2 ATDG BVerfGE 133, 277 (332).

[21] Vgl. zur Wohnraumüberwachung BVerfGE 109, 279 (343 ff.).

[22] Vgl. zur „Online-Durchsuchung“ BVerfGE 120, 274 (326 ff.); zum Abruf bevorrateter Telekommunikations-Verkehrsdaten BVerfGE 125, 260 (330 f.); ferner zur Rasterfahndung, die aus informationstechnischer Sicht der erweiterten Nutzung ähnelt, BVerfGE 115, 320 (360 ff.).

[23] Vgl. BVerfGE 133, 277 (322 ff.).

hohe Anforderungen insbesondere an einen Datenaustausch zwischen diesen Behörden „für ein mögliches operatives Tätigwerden“, also für polizeiliche Zwecke, errichtet.[24]

Im umgekehrten Fall, dass ein Nachrichtendienst Zugriff auf polizeiliche Datenbestände erhält, stellt sich dieses besondere grundrechtliche Risiko nicht. Ein solcher Informationsfluss ist grundrechtlich nicht trivial, aber in weiterem Umfang rechtfertigungsfähig. Ausreichend erscheint hier, dass sich das nachrichtendienstliche Erkenntnisinteresse auf eine terroristische oder extremistische Struktur bezieht, von der hinreichend gewichtige Schäden zu besorgen sind.

2. Verfassungsrechtliche Defizite der vorgesehenen Ermächtigungen

Der Gesetzentwurf sieht in § 6a Abs. 1 ATDG-E und § 7 Abs. 1 RED-G-E jeweils drei weitgehend gleichlautende Ermächtigungstatbestände vor. Keiner von ihnen genügt den verfassungsrechtlichen Anforderungen. Denn sie setzen durchweg erheblich unterhalb der mindestens zu fordernden Eingriffsschwellen an.

a) Analyse gewaltbereiter Bestrebungen

Nach § 6a Abs. 1 Satz 1 Alt. 1 ATDG-E und § 7 Abs. 1 Satz 1 Alt. 1 RED-G-E soll eine erweiterte Dateinutzung erlaubt sein, um im Rahmen eines Analyseprojekts Informationen über einzelne Bestrebungen des internationalen Terrorismus bzw. gewaltbereite rechtsextremistische Bestrebungen zu sammeln und auszuwerten.

Diese Ermächtigungstatbestände sind weit im Vorfeld einer konkreten Gefahr oder eines strafprozessualen Anfangsverdachts angesiedelt: Zum einen ist Gegenstand des Analyseprojekts nicht eine konkrete drohende oder begangene Straftat. Die Analyse bezieht sich vielmehr auf eine Struktur, von der bestimmte Straftaten oder Gewalthandlungen erwartet werden. Zum anderen beschränkt sich das Analyseziel nicht darauf, einzelne Straftaten zu verhindern oder zu verfolgen. Vielmehr sollen Informationen über die Zielstruktur als solche beschafft werden, um diese Struktur weitwinklig auszuleuchten.

An dem Befund, dass die vorgesehenen Ermächtigungen Eingriffsanlass und Eingriffsziel weit ins Vorfeld von Gefahr und Anfangsverdacht verlagern, ändert es nichts, dass eine erweiterte Nutzung nur im Rahmen eines „einzelfallbezogenen Projekts“ zulässig sein soll.

Der Begriff des Einzelfalls verweist hier ersichtlich nicht auf eine konkret drohende oder begangene Straftat. Vielmehr liegt es in diesem Kontext nahe, diesen Begriff so zu verstehen, dass (immerhin) eine zumindest ansatzweise konturierte einzelne Struktur Ziel der Dateinutzung sein muss. Tauglicher Gegenstand eines Analyseprojekts ist danach beispielsweise nicht der islamistische oder rechtsextremistische Terrorismus als solcher, wohl aber eine bestimmte terroristische Gruppierung[25] unabhängig davon, ob von ihr bereits ein näher konkretisierter Anschlag zu erwarten ist.

[24] BVerfGE 133, 277 (329).

[25] So auch die Entwurfsbegründung, BT-Drs. 18/1565, S. 19.

Was ein Projekt ist, definieren die vorgesehenen Regelungen nicht.[26] Es liegt nahe, darunter lediglich den behördlichen Arbeitszusammenhang zu verstehen, der sachlich durch die Zielstruktur als Analysegegenstand und zeitlich durch die Befristungsregelungen in § 6a Abs. 3 Sätze 2 und 3 ATDG-E sowie § 7 Abs. 3 Sätze 2 und 3 RED-G(-E) definiert wird. In dieser Interpretation begrenzt der Projektbegriff die vorgesehenen Ermächtigungen nicht zusätzlich.

Diese Ermächtigungen ließen sich verfassungskonform gestalten, indem sie ausdrücklich den Nachrichtendiensten vorbehalten würden, auf die sie ohnehin primär zugeschnitten sein dürften. Hohe Anforderungen ergäben sich dann allerdings wiederum an die Übermittlung der Ergebnisse eines nachrichtendienstlichen Analyseprojekts an Polizeibehörden. Diese Datenübermittlung ist jedoch nicht Gegenstand des Entwurfs, sondern richtet sich gemäß § 6a Abs. 7 Satz 2 ATDG-E bzw. § 7 Abs. 7 Satz 2 RED-G-E nach den allgemeinen Übermittlungsermächtigungen.

b) Strafverfolgung

Nach § 6a Abs. 1 Satz 1 Alt. 2 ATDG-E und § 7 Abs. 1 Satz 1 Alt. 2 RED-G-E dürfen die Dateien auch zum Zweck der Strafverfolgung erweitert genutzt werden. Gegenstand des strafprozessualen Verfahrens muss dabei eine der in § 6a Abs. 1 Satz 3 ATDG-E bzw. § 7 Abs. 1 Satz 3 RED-G aufgezählten Straftaten sein. Diese Straftatkataloge sind jedoch zu weit gefasst und beschränken sich nicht auf besonders schwere Straftaten.

Für die Beurteilung, wie schwer eine Straftat wiegt, ist der gesetzliche Strafrahmen von maßgeblicher Bedeutung. Eine besonders schwere, den Bereich der mittleren Kriminalität eindeutig verlassende Straftat liegt nach der Systematik des StGB erst vor, wenn die Tat im Höchstmaß mit mehr als fünf Jahren Freiheitsstrafe bewehrt ist. Dies hat das Bundesverfassungsgericht in seinem Urteil zur akustischen Wohnraumüberwachung näher ausgeführt.[27]

Hingegen führen § 6a Abs. 1 Satz 3 ATDG-E und § 7 Abs. 1 Satz 3 RED-G sogar Straftatbestände auf, bei denen die Höchststrafe noch unter fünf Jahren verbleibt. Dies gilt für die in beiden Normen genannten § 89b und § 91 StGB sowie aus dem Katalog des § 7 Abs. 1 Satz 3 RED-G zusätzlich für § 126 und § 127 StGB. Selbst wenn für die strafprozessuale erweiterte Dateinutzung die Anforderungen an das Gewicht der Straftaten gegenüber der Wohnraumüberwachung abzusenken wären, wären zumindest diese Verweise verfassungsrechtlich nicht tragfähig.

c) Verhinderung von Straftaten

Schließlich ermöglichen § 6a Abs. 1 Satz 2 ATDG-E und § 7 Abs. 1 Satz 2 RED-G erweiterte Dateinutzungen auch zu dem präventivpolizeilichen Ziel, Straftaten aus den Katalogen von § 6a Abs. 1 Satz 3 ATDG-E bzw. § 7 Abs. 1 Satz 3 RED-G zu verhindern. Diese Ermächtigungen sind gleichfalls zu weit gefasst.

Es ist bereits zweifelhaft, ob diese Ermächtigungen die erweiterte Dateinutzung auf konkrete Gefahren begrenzen, wie dies verfassungsrechtlich geboten ist. Ausdrücklich verwenden bei-

---

[26] Kritisch *Arzt*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014 (im Erscheinen), § 7 RED-G Rn. 6.

[27] BVerfGE 109, 279 (343 ff.).

de Normen den Gefahrbegriff nicht. Stattdessen setzen sie als Nutzungsanlass voraus, dass „eine… Straftat begangen werden soll“, und erlauben die Nutzung „zur Verhinderung“ von „Straftaten“. Die Formulierung des Nutzungsanlasses im Singular („eine Straftat“) könnte zwar so verstanden werden, dass die Polizeibehörde eine Straftat im Einzelfall zu prognostizieren hat, deren Konturen sich bereits näher abzeichnen. In dieser Interpretation würden die Ermächtigungen den polizeirechtlichen Gefahrbegriff lediglich reformulieren. Jedoch passen hierzu nicht das auf den (bloßen) Willen der potenziellen Straftäter abzielende Verb „sollen“ sowie die Benennung des Nutzungsziels im Plural („Straftaten“). Die Ermächtigungen greifen damit Formulierungen auf, die für das präventivpolizeiliche Vorfeldrecht typisch sind, also üblicherweise gerade nicht das Erfordernis einer konkreten Gefahr errichten sollen.[28] Zumindest sind sie so missverständlich gefasst, dass gegen sie Bedenken aus dem rechtsstaatlichen Bestimmtheitsgrundsatz bestehen.

Selbst wenn § 6a Abs. 1 Satz 2 ATDG-E und § 7 Abs. 1 Satz 2 RED-G als reformulierte Gefahrtatbestände begriffen werden, gehen diese Ermächtigungen teilweise inhaltlich zu weit. Sie gewährleisten auch dann nicht durchgängig, dass die erweiterte Dateinutzung sich auf besonders schwerwiegende Gefahren beschränkt. Grund hierfür sind die in Bezug genommenen Straftatkataloge in § 6a Abs. 1 Satz 3 ATDG-E bzw. § 7 Abs. 1 Satz 3 RED-G. Oben wurde bereits ausgeführt, dass diese Kataloge auch auf Straftatbestände minderen Gewichts verweisen. Hinzu kommt ein spezifisch präventivpolizeiliches Regelungsdefizit: Die Straftatkataloge führen teilweise Straftatbestände auf, die ihrerseits Handlungen im Vorfeld der Verletzung oder konkreten Gefährdung eines Rechtsguts kriminalisieren.[29] Die Ermächtigungen in § 6a Abs. 1 Satz 2 ATDG-E und § 7 Abs. 1 Satz 2 RED-G erlauben die erweiterte Dateinutzung bereits, wenn lediglich eine solche Vorfeldhandlung droht. Zu einem solchen Zeitpunkt wird vielfach noch keine Gefahr für ein Rechtsgut vorliegen. Eine Anknüpfung an strafrechtliche Vorfeldtatbestände entgrenzt deshalb den Eingriffsanlass und ist für präventivpolizeiliche Ermächtigungen ein ungeeigneter und verfassungsrechtlich nicht tragfähiger Regelungsansatz.[30] Hiervon betroffen sind die in beiden Katalogen aufgeführten § 89a, § 89b, § 91 und § 129a StGB sowie aus dem Katalog von § 7 Abs. 1 Satz 3 RED-G darüber hinaus § 89, § 127, § 129 und § 310 StGB.

III. Fortbestehende verfassungsrechtliche Defizite außerhalb von ATDG und RED-G

Der Gesetzentwurf sieht allein Änderungen des ATDG und des RED-G vor. Solche Änderungen reichen jedoch nicht aus, um das geltende Recht den verfassungsrechtlichen Anforderungen anzupassen, die das Bundesverfassungsgericht in seinem Urteil zum ATDG aufgezeigt hat.

---

[28] Eingehend anhand der Eingriffstatbestände des BKAG zum Verhältnis von Gefahr und Gefahrvorfeld und zu den verschiedenen Formulierungsmöglichkeiten die Kommissionsmitglieder *Bäcker* und *Hirsch*, in: Bericht der Regierungskommission zur Überprüfung der Sicherheitsgesetzgebung in Deutschland, 2013, S. 60 ff.

[29] Näher zu Erscheinungsformen und Zwecken derartiger kriminalpräventiver Straftatbestände mit Blick auf das Terrorismusstrafrecht die Kommissionsmitglieder *Bäcker, Hirsch* und *Wolff*, in: Bericht der Regierungskommission zur Überprüfung der Sicherheitsgesetzgebung in Deutschland, 2013, S. 37 ff.

[30] Näher *Bäcker*, in: Festschrift für Schenke, 2011, S. 331 (343 ff.); noch weitergehend BVerfGE 125, 260 (329).

Insbesondere ist es dringend erforderlich, die Datenübermittlungsermächtigungen des Nachrichtendienstrechts zu überarbeiten. Diese Normen ermöglichen Informationsflüsse von Nachrichtendiensten zu operativ tätigen Polizei- und Strafverfolgungsbehörden in einem Ausmaß, das auf der Grundlage des Urteils des Bundesverfassungsgerichts offenkundig und erheblich über das verfassungsrechtlich Zulässige hinausgeht.[31] Die gravierenden Mängel des geltenden Rechts lassen sich beispielhaft an den Übermittlungsermächtigungen des BVerfSchG aufzeigen: § 19 BVerfSchG erlaubt eine Datenübermittlung unter anderem, sofern die Empfangsbehörde die Daten für „Zwecke der öffentlichen Sicherheit“ benötigt. Das Bundesverfassungsgericht hat demgegenüber in seinem Urteil zum ATDG ausgeführt, Übermittlungsermächtigungen dürften sich jedenfalls für Informationsflüsse von Nachrichtendiensten an Polizeibehörden „nicht mit… niederschwelligen Voraussetzungen wie… der Wahrung der öffentlichen Sicherheit begnügen“.[32] Zu weit geht auch § 20 BVerfSchG, der eine Übermittlungspflicht zur Verfolgung von Staatsschutzdelikten errichtet; hierunter können bei entsprechender (etwa rassistischer) Motivation auch Bagatellstraftaten wie eine Beleidigung oder eine Sachbeschädigung fallen.

Darüber hinaus liegt es aufgrund des Urteils zum ATDG zumindest nahe, die Tätigkeit der sogenannten Gemeinsamen Zentren ausdrücklich gesetzlich zu regeln. Diese Zentren sind organisatorische Plattformen für eine institutionell verfestigte informationelle Zusammenarbeit verschiedener Sicherheitsbehörden von Bund und Ländern.[33] Diese Zusammenarbeit stützt sich derzeit allein auf die Datenübermittlungsermächtigungen des jeweiligen behördlichen Fachrechts. Die informationelle Zusammenarbeit in den Zentren geht jedoch über einen punktuellen Informationsfluss, wie ihn diese Ermächtigungen im Blick haben, fundamental hinaus. Vielmehr bedarf eine derartige behördenübergreifende Analysetätigkeit einer gesetzlichen Grundlage, die diese Tätigkeit auf besonders schwerwiegende Bedrohungen begrenzt. Dabei ist auch eine wirksame Kontrolle der Zentren als solcher – und nicht allein der teilnehmenden Behörden – zu gewährleisten.[34]

---

[31] Näher zum Folgenden die Kommissionsmitglieder *Bäcker, Hirsch* und *Wolff*, in: Bericht der Regierungskommission zur Überprüfung der Sicherheitsgesetzgebung in Deutschland, 2013, S. 202 ff.; eingehend *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, 2014.

[32] BVerfGE 133, 277 (330 f.).

[33] Näher Bericht der Regierungskommission zur Überprüfung der Sicherheitsgesetzgebung in Deutschland, 2013, S. 165 ff.

[34] Näher die Kommissionsmitglieder *Bäcker, Giesler, Hirsch* und *Wolff*, in: Bericht der Regierungskommission zur Überprüfung der Sicherheitsgesetzgebung in Deutschland, 2013, S. 172 ff.