Prof. Dr. Matthias Bäcker, LL.M.

Karlsruher Institut für Technologie
Institut für Informations- und Wirtschaftsrecht
Vincenz-Prießnitz-Straße 3
76131 Karlsruhe

Karlsruhe, den 2. Juni 2015

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)328 A

Stellungnahme

zu dem Entwurf eines Gesetzes zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes

(BT-Drs. 18/4654)

Gliederung

Ergebnisse

I. Erweiterte Zuständigkeit des Bundesamts für Verfassungsschutz

II. Datenverbund der Verfassungsschutzbehörden

III. Einsatz nachrichtendienstlicher Mittel durch das Bundesamt für Verfassungsschutz

1. Die allgemeine Regelung in § 8 Abs. 2 Satz 2 BVerfSchG-E
2. Regelungen zu verdeckten Mitarbeitern und Vertrauensleuten in § 9a f. BVerfSchG-E

IV. Ausbau der strategischen Telekommunikationsüberwachung des Bundesnachrichtendienstes

V. Datenübermittlungen von Nachrichtendiensten an Polizei- und Strafverfolgungsbehörden

1. Übermittlungsermächtigungen im BVerfSchG
   a) Defizite von § 19 Abs. 1 BVerfSchG-E
   b) Fortbestehende Mängel von § 20 und § 23 BVerfSchG
2. Defizite von § 7 Abs. 4 Satz 1 Nr. 2, Satz 2 G 10-E

Ergebnisse

1. Die geplante Erweiterung des Zuständigkeitsbereichs des Bundesamts für Verfassungsschutz durch § 5 Abs. 1 Satz 2 Nr. 2 BVerfSchG-E steht mit der Kompetenzordnung des Grundgesetzes nicht in Einklang.

2. Durch § 6 BVerfSchG-E soll ein umfassender Datenverbund der Verfassungsschutzbehörden geschaffen werden. Der Entwurf sieht hierfür keine hinreichenden begrenzenden Regelungen vor. Die geplante Regelung steht daher mit den Grundrechten der Betroffenen nicht in Einklang.

3. Die vorgesehene allgemeine Regelung zum Einsatz nachrichtendienstlicher Mittel in § 8 Abs. 2 Satz 2 BVerfSchG-E ist verwirrend formuliert und trägt nichts dazu bei, diesen Einsatz rechtsstaatlich zu disziplinieren. Dabei ist es verfassungsrechtlich angezeigt, die Rechtsgrundlagen für den Einsatz nachrichtendienstlicher Mittel zu überarbeiten.

4. Die geplanten Ermächtigungen zum Einsatz von verdeckten Mitarbeitern und Vertrauensleuten in §§ 9a f. BVerfSchG enthalten für eingriffsintensivere Einsatzformen keine hinreichende tatbestandliche Eingriffsschwelle. Zudem fehlt es für solche Einsatzformen an den gebotenen verfahrensrechtlichen Sicherungen.

5. Die vorgesehene Ausdehnung der strategischen Telekommunikationsüberwachung durch den Bundesnachrichtendienst in § 5 Abs. 1 Satz 3 Nr. 8 G 10-E, um Angriffen auf IT-Systeme zu begegnen, steht mit dem grundrechtlichen Fernmeldegeheimnis nicht vollständig in Einklang.

6. Der Entwurf beseitigt die derzeitigen Mängel der Datenübermittlungsermächtigungen in §§ 19 ff. BVerfSchG nicht vollständig. § 19 Abs. 1 BVerfSchG-E geht teilweise immer noch zu weit und verletzt Grundrechte. Der ebenfalls teils verfassungswidrig zu weit, zudem teils zu eng gefasste § 20 BVerfSchG soll überhaupt nicht geändert werden. Kritikwürdig ist schließlich, dass § 23 BVerfSchG unverändert bleiben soll, obwohl gerade diese Norm die Gefahr birgt, dass Datenübermittlungen von Nachrichtendiensten an Polizei- und Strafverfolgungsbehörden auch bei schwerwiegenden Straftaten unterbleiben.

7. Die vorgesehenen Datenübermittlungsermächtigungen in § 7 Abs. 4 Satz 1 Nr. 2, Satz 2 G 10-E sind teilweise zu weit gefasst und stehen insoweit mit den Grundrechten der Betroffenen nicht in Einklang.

Eine umfassende Stellungnahme zu allen Rechtsfragen, die der Gesetzentwurf aufwirft, war mir in der eingeräumten Bearbeitungszeit nicht möglich. Meine Stellungnahme beschränkt sich daher auf ausgewählte verfassungsrechtliche Probleme der beabsichtigten Regelungen. Soweit ich mich zu dem Entwurf nicht äußere, ist daraus nicht zwangsläufig zu folgern, dass ich die betreffenden Normen für unbedenklich halte.

Der Entwurf weist in mehrfacher Hinsicht erhebliche verfassungsrechtliche Mängel auf: Er sieht vor, den Zuständigkeitsbereich des Bundesamts für Verfassungsschutz in einer Weise auszubauen, die der bundesstaatlichen Kompetenzordnung widerspricht (unten I). Zudem soll ein annähernd grenzenloser Datenverbund der Verfassungsschutzbehörden geschaffen werden, der mit den Grundrechten der Betroffenen nicht in Einklang steht (unten II). Grundrechtliche Mängel enthalten auch die vorgesehenen Regelungen zum Einsatz nachrichtendienstlicher Mittel durch das Bundesamt für Verfassungsschutz (unten III), zum Ausbau der strategischen Telekommunikationsüberwachung durch den Bundesnachrichtendienst (unten IV) und zu Datenübermittlungen von Nachrichtendiensten an Polizei- und Strafverfolgungsbehörden (unten V).

I. Erweiterte Zuständigkeit des Bundesamts für Verfassungsschutz

Die geplante Erweiterung des Zuständigkeitsbereichs des Bundesamts für Verfassungsschutz durch § 5 Abs. 1 Satz 2 Nr. 2 BVerfSchG-E steht mit der Kompetenzordnung des Grundgesetzes nicht in Einklang.

Kompetenzrechtlich ist es generell problematisch, dass das Bundesamt für Verfassungsschutz selbst und aufgrund eigener Erkenntnisinteressen Informationen über verfassungsfeindliche Bestrebungen erheben soll. Denn das Grundgesetz vermittelt dem Bund lediglich eine Gesetzgebungskompetenz für die Zusammenarbeit von Bund und Ländern im Verfassungsschutz[1] und eine Verwaltungskompetenz für eine Zentralstelle in diesem Bereich.[2] Zwar sind diese Begriffe und das Zusammenspiel beider Kompetenztitel schwierig zu bestimmen. Ihnen lässt sich aber doch entnehmen, dass das Grundgesetz den Bund gerade nicht ermächtigt, in redundanter Weise eine Bundesbehörde mit umfassenden Datenerhebungsbefugnissen neben die Verfassungsschutzbehörden der Länder treten zu lassen. Insbesondere der Zentralstellenbegriff gewinnt Konturen nur bei einer restriktiveren Interpretation. Die Aufgabe einer Zentralstelle besteht danach lediglich darin, die Landesbehörden zu vernetzen und ihre Tätigkeit zu koordinieren. Die Tätigkeit der Zentralstelle bleibt stets auf die Tätigkeit der Landesbehörden bezogen. Eigene Datenerhebungen führt sie allenfalls durch, um diese Servicefunktion erbringen zu können,[3] nicht aber aufgrund selbst gesetzter Erkenntnisziele.[4]

---

[1] Art. 73 Abs. 1 Nr. 10 Buchstaben b und c GG

[2] Art. 87 Abs. 1 Satz 2 GG.

[3] Vgl. in diesem Sinne die kompetenzrechtlich heiklen, aber noch zulässigen Ermächtigungen in § 7 Abs. 2 und 3 BKAG und näher dazu *Graulich*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, § 7 BKAG Rn. 24 ff.

[4] Näher mit Blick auf das G 10 *Bäcker*, DÖV 2011, S. 840 (843 f.), m.w.N. auch zu den anderen vertretenen Auffassungen.

Diese Interpretation des Zentralstellenbegriffs liegt in der Gesetzgebungspraxis dem BKAG zugrunde. Eigene Datenerhebungsbefugnisse hat das Bundeskriminalamt grundsätzlich[5] nicht in seiner Eigenschaft als Zentralstelle, sondern aufgrund anderer Aufgaben, die auf andere Kompetenztitel als Art. 87 Abs. 1 Satz 2 GG zu stützen sind.[6] Hingegen weist § 5 Abs. 2 (nach dem Entwurf zukünftig Abs. 1) BVerfSchG dem Bundesamt für Verfassungsschutz bereits heute auch die Zuständigkeit zu, eigenständig – wenngleich im Benehmen mit den Landesbehörden – Informationen zu erheben. §§ 8 ff. BVerfSchG enthalten die zugehörigen Datenerhebungsermächtigungen.

Immerhin beschränkt sich der Zuständigkeitsbereich des Bundesamts für Verfassungsschutz bislang jedoch auf Sachverhalte mit einem spezifischen Bundesbezug. Das Bundesamt ist danach insbesondere zuständig, wenn Bestrebungen über den Bereich eines Landes hinausgehen oder auswärtige Belange der Bundesrepublik berühren oder wenn eine Landesbehörde das Bundesamt um ein Tätigwerden ersucht. Die weitere Regelung, nach der es auch ausreicht, wenn sich eine Bestrebung gegen den Bund richtet, beschreibt einen spezifischen Bundesbezug dann, wenn sie restriktiv ausgelegt wird. Danach muss das Ziel der Bestrebung gerade darin bestehen, den Bestand der Bundesrepublik zu untergraben. Nicht ausreichend ist es etwa, wenn eine Bestrebung sich lediglich gegen bestimmte materielle Kernbestandteile der freiheitlich demokratischen Grundordnung richtet.[7]

Die kompetenzrechtlichen Begriffe der Zusammenarbeit von Bund und Ländern und der Zentralstelle mögen bei einer extensiven Interpretation so zu verstehen sein, dass eine eigenständige Datenerhebungstätigkeit des Bundesamts für Verfassungsschutz in solchen Sachverhalten mit einem spezifischen Bundesbezug noch von der Kompetenzordnung gedeckt ist. Damit werden die maßgeblichen Kompetenztitel allerdings bis zum äußersten Rand ausgereizt.

Die geplante Zuständigkeitsregelung des § 5 Abs. 1 Satz 2 Nr. 2 BVerfSchG-E überschreitet selbst diese Grenze. Sie ersetzt einen Bundesbezug durch die Gefährlichkeit der betreffenden Bestrebung, indem das Bundesamt für Verfassungsschutz pauschal zuständig sein soll, Informationen über gewaltbereite oder Gewalt befürwortende Bestrebungen zu erheben. Damit sind für Datenerhebungen über solche Bestrebungen stets mindestens zwei Verfassungsschutzbehörden zuständig, nämlich das Bundesamt für Verfassungsschutz und mindestens eine Landesverfassungsschutzbehörde. Eine derartige pauschale Verdoppelung des außenwirksamen Verfassungsschutzes wird von der Kompetenzordnung nicht mehr gedeckt.

Diesem Befund lässt sich nicht mit der Entwurfsbegründung entgegenhalten, gewaltorientierte Bestrebungen seien stets gesamtstaatlich bedeutsam.[8] Wenn eine gewaltorientierte Bestrebung

---

[5] Eine Ausnahme bilden die Ermächtigungen in § 7 BKAG, die allerdings lediglich darauf gerichtet sind, ergänzende Informationen zu beschaffen, s.o. bei Fußnote 3.

[6] Vgl. zu dem Gefüge von Kompetenztiteln, auf das sich die gegenwärtige Ausgestaltung des Bundeskriminalamts stützen kann, mit unterschiedlichen Positionen im Einzelnen etwa *Ibler*, in: Maunz/Dürig (Begr.), GG, Stand 2012, Art. 87 Rn. 128 ff.; *Bäcker*, Terrorismusabwehr durch das Bundeskriminalamt, 2009, S. 18 ff.

[7] A.A. anscheinend *Roth*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, § 5 BVerfSchG Rn. 12, der meint, dass sich „Bestrebungen im Sinne des § 3 Abs. 1 [BVerfSchG] so gut wie immer auch gegen den Bund richten". In dieser Auslegung ist bereits die geltende Zuständigkeitsregelung mit der Kompetenzordnung nicht zu vereinbaren.

[8] BT-Drs. 18/4654, S. 20.

einen spezifischen Bundesbezug aufweist, ist das Bundesamt für Verfassungsschutz bereits nach geltendem Recht zuständig, Informationen über sie aufgrund eigener Erkenntnisziele zu erheben. Einer neuen Zuständigkeitsregelung bedarf es insoweit nicht.[9] Im Übrigen ist ohne weiteres vorstellbar, dass sich eine extremistische Bestrebung regional auf ein kleines Gebiet beschränkt, auf diesem Gebiet aber äußerst aggressiv vorgeht. Eine gesamtstaatliche Relevanz ergibt sich in einem solchen Fall nicht schon daraus, dass von der Bestrebung erhebliche Schäden drohen mögen. Die bundesstaatliche Kompetenzordnung des Grundgesetzes beruht vielmehr auf der Annahme, dass die Länder in der Lage sind, auch erhebliche Gefahren abzuwehren; dies zeigt sich neben dem Verfassungsschutz etwa an der Gesetzgebungs- und Verwaltungskompetenz der Länder für die allgemeine polizeiliche Gefahrenabwehr. Ein Schluss von Schadenspotenzialen auf Bundeskompetenzen ist ohne Verfassungsänderung nicht statthaft.

II. Datenverbund der Verfassungsschutzbehörden

Nach dem derzeitigen § 5 BVerfSchG sind die Verfassungsschutzbehörden der Länder verpflichtet, den anderen Landesbehörden und dem Bundesamt für Verfassungsschutz Informationen zu übermitteln, soweit dies erforderlich ist, damit die Empfangsbehörde ihre Aufgaben erfüllen kann. Umgekehrt hat das Bundesamt die Landesbehörden über alle Unterlagen zu unterrichten, deren Kenntnis für das jeweilige Land zum Zweck des Verfassungsschutzes erforderlich ist. Diese Unterrichtungspflichten werden durch die Regelung zu gemeinsamen Dateien in § 6 BVerfSchG flankiert, die bei dem Bundesamt für Verfassungsschutz zu führen sind. Dabei handelt es sich gemäß Satz 2 dieser Vorschrift grundsätzlich[10] nur um Indexdateien, die dazu dienen, Akten aufzufinden und Personen zu identifizieren.

Der Gesetzentwurf sieht vor, den Datenverbund der Verfassungsschutzbehörden erheblich auszubauen. Dadurch intensiviert sich allerdings der Grundrechtseingriff erheblich, der darin liegt, dass personenbezogene Daten in einer zentralen, automatisiert auswertbaren Verbunddatei gespeichert werden. Diese Intensivierung müsste durch begrenzende materielle Vorgaben kompensiert werden, die in dem Entwurf jedoch fehlen.

Der Entwurf führt zunächst die wechselseitigen Unterrichtungspflichten der Verfassungsschutzbehörden in § 6 Abs. 1 BVerfSchG-E zusammen. Unklar ist, ob diese Pflichten inhaltlich weiterreichen als bislang. Der Entwurf ersetzt den Begriff der Erforderlichkeit für die Aufgabenerfüllung durch die Relevanz für die Aufgaben und begründet dies mit „Einschätzungsdivergenzen zur Erforderlichkeit…, aus denen auch Defizite beim Informationsaustausch resultierten“.[11] Allerdings kann es zu solchen Divergenzen bei jedem Rechtsbegriff kommen. Sprachlich erscheint es naheliegend, Relevanz als Nützlichkeit zu interpretieren.[12]

---

[9] In sich widersprüchlich ist insoweit die Entwurfsbegründung. Danach sollen gegenüber gewaltorientierten Bestrebungen zwar stets die Zuständigkeitsregelungen in § 5 Abs. 2 Satz 2 Nr. 1 und 2 BVerfSchG greifen. Gleichwohl werden „Beobachtungslücken“ befürchtet, denen die neue Zuständigkeitsregelung begegnen soll.

[10] Eine Ausnahme für besonders schadensträchtige Bestrebungen und für „eng umgrenzte Anwendungsgebiete“ sieht § 6 Satz 8 BVerfSchG vor.

[11] BT-Drs. 18/4654, S. 22.

[12] So wohl auch die Entwurfsbegründung, die allerdings zugleich terminologisch zweifelhaft ausführt, der Relevanzbegriff sei als „Präzisierung der Erforderlichkeit“ anzusehen, BT-Drs. 18/4654, S. 22.

Hierfür spricht mit Blick auf Übermittlungen an das Bundesamt für Verfassungsschutz auch die in § 5 Abs. 2 BVerfSchG-E vorgesehene Aufgabe des Bundesamts, *alle* Erkenntnisse über verfassungsfeindliche Bestrebungen auszuwerten. In dieser Interpretation ginge der neue Begriff deutlich weiter als der hergebrachte, im Datenschutzrecht gängige Begriff der Erforderlichkeit.[13]

Jedenfalls sieht der geplante § 6 Abs. 2 BVerfSchG-E vor, den Inhalt der gemeinsamen Dateien erheblich auszubauen. Die bisherige Beschränkung auf eine Indexfunktion soll wegfallen. Damit geht die geplante Regelung jedoch zu weit.

Um eine behördliche Datensammlung zu regulieren, kann der Gesetzgeber bei unterschiedlichen Parametern ansetzen. Im Einzelnen handelt es sich dabei um

1. den Inhalt der Datensammlung, der durch Art und Umfang der gespeicherten Daten bestimmt wird,

2. die Voraussetzungen, unter denen Daten in der Datensammlung gespeichert werden, sowie

3. die Voraussetzungen und die zulässigen Arten einer Nutzung der gespeicherten Daten.

Von diesen Parametern hängt auch ab, wie intensiv eine behördliche Datensammlung, die personenbezogene Daten enthält, in Grundrechte eingreift. Dabei stehen die Parameter in einem wechselseitigen Kompensationsverhältnis. Soll etwa eine Datensammlung Daten in großem Umfang enthalten, die ganz oder weitgehend anlasslos bevorratet werden und aus denen sich sensible Informationen gewinnen lassen, so sind an die Voraussetzungen der Datennutzung grundsätzlich hohe Anforderungen zu stellen.[14] Wird allerdings die Datennutzung der Art nach enger begrenzt, können die Voraussetzungen niedriger angesetzt werden.[15] Umgekehrt können großzügige Nutzungsvoraussetzungen gerechtfertigt werden, wenn die Datensammlung nach ihrem Inhalt nur begrenzte Risiken für die Betroffenen birgt oder wenn hohe Anforderungen an eine Datenspeicherung bestehen.

Die vorgesehene Regelung gibt hingegen für den Datenverbund der Verfassungsschutzbehörden alle Parameter weitgehend frei:

Erstens enthält § 6 Abs. 2 BVerfSchG-E keine begrenzenden Vorgaben für den Inhalt der gemeinsamen Dateien. Diese Dateien können daher aufgrund beliebig vieler Datenfelder mit jeglichen Daten befüllt werden. Dies schließt Daten ein, die mit eingriffsintensiven nachrichtendienstlichen Mitteln erhoben wurden und bereits deshalb sensibel sind. Zudem soll § 10 Abs. 2 BVerfSchG-E den Verfassungsschutzbehörden ermöglichen, zusätzlich zu den gespeicherten Daten auch Belegdokumente in den gemeinsamen Datenbanken abzulegen. Zusam-

---

[13] Allgemein zur datenschutzrechtlichen Erforderlichkeit *Albers*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. 2, 2. Aufl. 2012, § 22 Rn. 130 ff.

[14] Vgl. für die Bevorratung von Telekommunikations-Verkehrsdaten grundsätzlich BVerfGE 125, 260 (327 ff.); für die umfassende Auswertung der Antiterrordatei in Eilfällen BVerfGE 133, 277 (364 f.).

[15] Vgl. für die Auflösung einer dynamischen IP-Adresse mittels bevorrateter Verkehrsdaten BVerfGE 125, 260 (340 ff.); für die Nutzung der Antiterrordatei als Indexdatei BVerfGE 133, 277 (360 ff.), anders aber für eine merkmalbezogene Recherche ebd., S. 363 f.

men genommen ermöglichen die vorgesehenen Regelungen den Verfassungsschutzbehörden damit, praktisch ihren gesamten Informationsbestand in digitaler Form in den Datenverbund einzustellen.

Zweitens erlaubt das Gesetz, personenbezogene Daten fast ohne einschränkende Voraussetzungen in die gemeinsamen Dateien einzustellen. Wegen der Speicherungsvoraussetzungen verweist § 6 Abs. 2 Satz 2 BVerfSchG-E insbesondere auf § 10 Abs. 1 BVerfSchG. Eine Speicherung ist danach zulässig, wenn tatsächliche Anhaltspunkte für verfassungsfeindliche Bestrebungen oder Tätigkeiten vorliegen oder wenn sie für die Erforschung und Bewertung solcher Bestrebungen oder Tätigkeiten erforderlich ist. Damit fordert die Norm letztlich nur, dass sich die Speicherung im Rahmen der Aufgaben des Verfassungsschutzes hält. Weitere Restriktionen hinsichtlich des Gewichts der jeweiligen Bestrebungen und Tätigkeiten, hinsichtlich des konkreten Speicherungsanlasses oder hinsichtlich der betroffenen Personen enthält § 10 Abs. 1 BVerfSchG nicht. Die Behördenpraxis mag restriktiver sein und insbesondere die Speicherung an eine bestimmte Beziehung des Betroffenen zu der Bestrebung knüpfen.[16] Dem Wortlaut der Norm lässt sich eine solche Einschränkung jedoch nicht entnehmen. § 10 Abs. 1 BVerfSchG ermöglicht seinem Wortlaut nach im Zusammenwirken mit § 6 Abs. 2 Satz 2 BVerfSchG-E vielmehr ohne weiteres, Daten etwa von nicht-dolosen Helfern („nützlichen Idioten“), flüchtigen Kontaktpersonen oder potenziellen Opfern der Angehörigen verfassungsfeindlicher Bestrebungen in die vorgesehenen gemeinsamen Dateien aufzunehmen.

Drittens enthält die vorgesehene Regelung kaum Beschränkungen für die Nutzung der gespeicherten Daten. Die Art der Nutzung ist in § 6 Abs. 2 BVerfSchG-E überhaupt nicht vorgegeben. Die gemeinsamen Dateien können daher für komplexe IT-gestützte Analysen genutzt werden, mit denen etwa Sozialprofile gebildet oder persönliche Eigenschaften und Vorlieben erschlossen werden können.[17] Zudem setzt eine Nutzung nach § 6 Abs. 2 Satz 6 BVerfSchG-E lediglich voraus, dass sie für die Aufgabenerfüllung der nutzenden Behörde erforderlich ist. Ein besonderer Nutzungstatbestand wird damit nicht geregelt. Insbesondere muss weder ein konkreter Nutzungsanlass bestehen noch muss sich die Abfrage auf Personen beziehen, die in einem spezifischen Näheverhältnis zu einer verfassungsfeindlichen Bestrebung stehen. Die weiteren Regelungen über die Zugriffsberechtigung in § 6 Abs. 2 Sätze 7 und 8 BVerfSchG-E geben lediglich vor, welche Amtswalter innerhalb einer Behörde die Dateien inwieweit nutzen dürfen. Die weite Nutzungsbefugnis des § 6 Abs. 2 Satz 6 BVerfSchG-E wird damit nicht beschränkt, sondern nur nach Maßgabe der innerbehördlichen Zuständigkeitsordnung verteilt.

Insgesamt wahrt § 6 Abs. 2 BVerfSchG-E damit nicht mehr das Übermaßverbot. Um den Datenverbund der Verfassungsschutzbehörden verfassungsrechtlich tragfähig auszubauen, müssten begrenzende Regelungen gefunden werden, welche die verschiedenen Regulierungsparameter in ein ausgewogenes Verhältnis bringen. Soll eine inhaltlich derart weitreichende Datenbevorratung mit so weitgehenden Nutzungsmöglichkeiten verbunden werden, so müssten

---

[16] So implizit die Entwurfsbegründung, vgl. BT-Drs. 18/4654, S. 29; einen Vorschlag für eine restriktivere Interpretation von § 10 Abs. 1 BVerfSchG unterbreitet *Bergemann*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 5. Aufl. 2012, Rn. H 97.

[17] So deutlich auch die Entwurfsbegründung, BT-Drs. 18/4654, S. 23 f., in Abgrenzung zu „archaischen Arbeitsmitteln“.

zumindest die Voraussetzungen der Datenspeicherung und der Datennutzung enger gefasst werden.

III. Einsatz nachrichtendienstlicher Mittel durch das Bundesamt für Verfassungsschutz

Als nachrichtendienstliche Mittel werden Methoden und Gegenstände bezeichnet, mit denen sich der Verfassungsschutz heimlich Informationen beschafft. Die Rechtsgrundlagen für den Einsatz nachrichtendienstlicher Mittel sind auf mehrere Vorschriften verteilt: § 8 Abs. 2 Satz 1 BVerfSchG beschreibt allgemein die Befugnis zur heimlichen Informationsbeschaffung und zählt exemplarisch einzelne nachrichtendienstliche Mittel auf. Diese Norm ermächtigt das Bundesamt für Verfassungsschutz jedoch nicht dazu, mit nachrichtendienstlichen Mitteln personenbezogene Daten zu erheben.[18] Die zugehörige Ermächtigung enthält vielmehr § 9 Abs. 1 Satz 1 BVerfSchG. Daneben finden sich spezielle Eingriffsermächtigungen für bestimmte eingriffsintensivere Datenerhebungsmaßnahmen in § 8a BVerfSchG, § 8d BVerfSchG, § 9 Abs. 2 und 4 BVerfSchG und § 1, § 3 G 10.

Der Gesetzentwurf sieht vor, dieses Gefüge von Rechtsgrundlagen in zweierlei Hinsicht zu modifizieren. Erstens soll der allgemeinen Regelung des § 8 Abs. 2 Satz 1 BVerfSchG ein neuer Satz 2 hinzugefügt werden, der nach der Entwurfsbegründung für Rechtssicherheit sorgen soll. Die geplante Regelung wirkt jedoch verwirrend und verfehlt die Anforderungen des Bestimmtheitsgrundsatzes. Zudem ändert sie nichts an den rechtsstaatlichen Bedenken, die eine pauschale Ermächtigung aufwirft, personenbezogene Daten heimlich zu erheben. Zweitens soll der Einsatz von verdeckten Mitarbeitern und Vertrauensleuten in §§ 9a f. BVerfSchG erstmals besonders geregelt werden. Diese Regelungen können allerdings eingriffsintensivere Einsatzformen nicht rechtfertigen.

1. Die allgemeine Regelung in § 8 Abs. 2 Satz 2 BVerfSchG-E

Die geplante Regelung in § 8 Abs. 2 Satz 2 BVerfSchG-E soll nach der Entwurfsbegründung für Rechtssicherheit sorgen, indem sie den Gehalt von § 8 Abs. 2 Satz 1 BVerfSchG im Sinne der oben dargestellten hergebrachten Auffassung klärt.[19] Dieses Ziel verfehlt der Entwurf jedoch. Die geplante Regelung wirft vielmehr erhebliche Zweifelsfragen auf und trägt im Übrigen nichts dazu bei, den Einsatz nachrichtendienstlicher Mittel rechtsstaatlich zu disziplinieren.

§ 8 Abs. 2 Satz 2 BVerfSchG-E besagt, dass § 8 Abs. 2 Satz 1 BVerfSchG nicht dazu ermächtigt, in Individualrechte einzugreifen. Dem lässt sich im Umkehrschluss entnehmen, dass § 8 Abs. 2 Satz 1 BVerfSchG taugliche Rechtsgrundlage für den Einsatz solcher nachrichtendienstlicher Mittel sein soll, die nicht in Individualrechte eingreifen. Unklar ist dabei schon der – in Gesetzestexten sonst ungebräuchliche[20] – Begriff der Individualrechte: Handelt es sich dabei lediglich um Grundrechte[21] oder sollen diesem Begriff auch subjektive Rechte unterfallen, die lediglich durch das einfache Recht gewährleistet werden? Vor allem aber genügt

---

[18] *Roth*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, § 8 BVerfSchG Rn. 20.

[19] BT-Drs. 18/4654, S. 25.

[20] Eine Volltextsuche nach „Individualrecht“ auf der Plattform http://www.gesetze-im-internet.de, die nahezu das gesamte Bundesrecht bereitstellt, ergab am 2. Juni 2015 keinen Treffer.

[21] So wohl die Entwurfsbegründung, BT-Drs. 18/4654, S. 25.

die Regelungstechnik des § 8 Abs. 2 Satz 2 BVerfSchG-E nicht dem rechtsstaatlichen Bestimmtheitsgebot. Die vorgeschlagene Regelung macht die Frage, welche Rechtsgrundlage den Einsatz nachrichtendienstlicher Mittel anleitet, von einer behördlichen Eingriffsprüfung abhängig, die das Gesetz nicht näher anleitet. Diese Eingriffsprüfung ist jedoch primär Sache des Gesetzgebers, der mit den gesetzlichen Ermächtigungsregelungen die jeweils berührten Grundrechte zu konkretisieren hat. Er kann diese Konkretisierungsleistung nicht durch eine derartige salvatorische Regelung an die vollziehende Gewalt delegieren.[22]

Die geplante Regelung verwirrt zudem auch insoweit, als sie auf „besondere Befugnisse“ verweist. Insbesondere liegt es sprachlich und im Vergleich etwa mit der polizeirechtlichen Terminologie nahe, als besondere Befugnisregelungen nur Normen anzusehen sind, die eine bestimmte Eingriffsmaßnahme zum Gegenstand haben und spezifisch regulieren. Die generalklauselartige Ermächtigung des § 9 Abs. 1 Satz 1 BVerfSchG wäre dann nicht als besondere Befugnisregelung anzusehen. Bei restriktiver Interpretation könnte § 8 Abs. 2 Satz 2 BVerfSchG-E daher zur Folge haben, dass das Bundesamt für Verfassungsschutz nachrichtendienstliche Mittel nicht mehr einsetzen darf, die in Grundrechte eingreifen, aber nicht in spezifischen Ermächtigungen geregelt sind, wie sie sich etwa in § 8a oder § 9 Abs. 2 BVerfSchG finden. Dieses mögliche Ergebnis dürfte nicht im Sinne des Entwurfs sein.

Dabei erscheint es durchaus geboten, weitere spezifische Ermächtigungen für nachrichtendienstliche Mittel in das Gesetz aufzunehmen, wie der Entwurf es mit § 9a und § 9b BVerfSchG-E partiell auch vorsieht. Denn einige der Mittel, die in § 8 Abs. 2 Satz 1 BVerfSchG genannt werden, greifen erheblich in das Recht auf informationelle Selbstbestimmung ein. Dies gilt etwa für heimliche Tonaufzeichnungen und längerfristige Observationen. Solche Maßnahmen können nach dem Bestimmtheitsgrundsatz nicht auf eine pauschale Generalklausel wie § 9 Abs. 1 Satz 1 BVerfSchG gestützt werden.[23] Insbesondere reicht es nicht aus, dass die nachrichtendienstlichen Mittel, die das Bundesamt für Verfassungsschutz einsetzen darf, lediglich in einer (überdies geheimen) Dienstvorschrift zu benennen sind, wie es § 8 Abs. 2 Satz 4 BVerfSchG-E (derzeit: § 8 Abs. 2 Satz 3 BVerfSchG) vorsieht. Besondere Geheimhaltungsbedürfnisse können diese Regelungstechnik nicht rechtfertigen. Dass nachrichtendienstliche Mittel durchaus präziser gesetzlich reguliert werden können, zeigt sich bereits an den Landesverfassungsschutzgesetzen, welche diese Mittel abschließend aufzählen.[24] Gerade für heimliche Datenerhebungen durch Nachrichtendienste ist das abstrakt-generelle Gesetz andererseits ein unverzichtbares Mittel, um den Bürgerinnen und Bürgern zumindest ansatzweise eine Orientierung über die Befugnisse der Dienste zu ermöglichen[25] und um eine demokratische Öffentlichkeit über diese Befugnisse und ihre Grenzen herzustellen.[26]

---

[22] Vgl. zu einer vergleichbaren Regelung im nordrhein-westfälischen Verfassungsschutzrecht BVerfGE 120, 274 (317).

[23] Vgl. zur Videoüberwachung im öffentlichen Raum BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 23. Februar 2007 – 1 BvR 2368/06 –, Rn. 45 ff.

[24] § 6 Abs. 3 Satz 1 bbgVerfSchG; § 8 Abs. 1 bremVerfSchG; § 10 Abs. 1 Satz 1 mvVerfSchG; § 5 Abs. 2 nwVSG.

[25] Allgemein zu den rechtsstaatlichen Funktionen des Bestimmtheitsgrundsatzes bei sicherheitsbehördlichen Datenerhebungsermächtigungen BVerfGE 110, 33 (52 ff.); 113, 348 (375 ff.); 120, 378 (407 f.).

[26] Zur demokratischen Funktion des Bestimmtheitsgrundsatzes bei sicherheitsbehördlichen Datenverarbeitungen BVerfGE 133, 277 (336).

2. Regelungen zu verdeckten Mitarbeitern und Vertrauensleuten in § 9a f. BVerfSchG-E
Der Entwurf sieht erstmals besondere Ermächtigungen für den Einsatz von verdeckten Mitarbeitern und Vertrauensleuten vor. Dies ist aus verfassungsrechtlicher Sicht im Ansatz zu begrüßen. Allerdings können die gesetzlichen Eingriffstatbestände die geregelten Maßnahmen nicht vollständig rechtfertigen.

Der Eingriffstatbestand für den Einsatz von verdeckten Mitarbeitern und Vertrauensleuten findet sich in § 9a Abs. 1 BVerfSchG, der wiederum auf § 9 Abs. 1 BVerfSchG verweist. Danach ist ein Einsatz insbesondere zulässig, wenn Tatsachen die Annahme rechtfertigen, dass damit Erkenntnisse über verfassungsfeindliche Bestrebungen von erheblicher Bedeutung gewonnen werden können.

Dieser sehr offen gefasste Eingriffsanlass ist unbedenklich bei nachrichtendienstlichen Mitteln von geringerer Eingriffsintensität, mit denen der Verfassungsschutz in noch weitgehend diffusen Lagen Anhaltspunkte gewinnen soll, auf deren Grundlage gezieltere Maßnahmen eingesetzt werden sollen. Der Einsatz eines verdeckten Mitarbeiters oder einer Vertrauensperson mag als solches Mittel geringerer Eingriffsintensität in einer Frühphase angesehen werden, in der eher ungezielt erste Erkenntnisse über eine Bestrebung beschafft werden sollen.

Die Eingriffsintensität steigt jedoch erheblich, wenn ein verdeckter Mitarbeiter oder eine Vertrauensperson gezielt an einzelne Angehörige der Bestrebung herangeführt werden soll, um deren Rolle und Vernetzungen innerhalb der Bestrebung aufzuklären. Ein derartiger gezielter Einsatz kann sich auf einen erheblichen Anteil der Lebensgestaltung der Betroffenen erstrecken und sensible Informationen zum Gegenstand haben.[27] Hierfür bedarf es eines qualifizierten gesetzlichen Eingriffstatbestands. Dieser Eingriffstatbestand muss einen hinreichend gewichtigen Eingriffsanlass vorgeben und die möglichen Zielpersonen präzise und restriktiv beschreiben.[28] Da § 9a Abs. 1 BVerfSchG-E dies nicht leistet, taugt der vorgesehene Eingriffstatbestand nicht dazu, eingriffsintensivere Einsatzformen zu regeln. Hierfür bedürfte es eines zusätzlichen, restriktiver zu fassenden Tatbestands. Daneben sind – etwa in Anknüpfung an § 8b BVerfSchG – verfahrensrechtliche Sicherungen einzurichten, um solche Einsatzformen auch prozedural einzuhegen.[29]

Kritikwürdig ist zudem, dass der Gesetzentwurf keine spezifizierenden Vorgaben zu der Frage vorsieht, inwieweit das Bundesamt für Verfassungsschutz Erkenntnisse, die durch verdeckte Mitarbeiter und Vertrauensleute gewonnen wurden, aus Gründen des Quellenschutzes gegenüber anderen staatlichen Stellen – insbesondere Polizeibehörden und der Strafjustiz – zu-

---

[27] Nach Auffassung von *Bergemann*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 5. Aufl. 2012, Rn. H 85, handelt es sich bei dem Einsatz einer Vertrauensperson in dieser Phase um „[m]öglicherweise … (nach der akustischen Wohnraumüberwachung) das eingriffsintensivste Mittel überhaupt".

[28] Die verfassungsrechtlichen Anforderungen an den Eingriffsanlass steigen auch im Nachrichtendienstrecht mit der Eingriffsintensität. Bei besonders schwerwiegenden Eingriffen konvergieren sie mit den Anforderungen an präventivpolizeiliche Ermächtigungen, vgl. zu Wohnraumüberwachungen Art. 13 Abs. 4 GG, zu „Online-Durchsuchungen" BVerfGE 120, 274 (329 ff.), zum Abruf bevorrateter Telekommunikations-Verkehrsdaten BVerfGE 125, 260 (331 f.).

[29] Vgl. zu dem verfassungsrechtlichen Gebot, intensive Grundrechtseingriffe durch verfahrensrechtliche Sicherungen abzuschirmen, etwa BVerfGE 120, 274 (331 ff.); 125, 260 (337 ff.).

rückhalten darf. Es soll damit bei der sehr pauschalen und wenig befriedigenden Regelung des § 23 Nr. 2 BVerfSchG bleiben.[30]

IV. Ausbau der strategischen Telekommunikationsüberwachung des Bundesnachrichtendienstes

§ 5 Abs. 1 Satz 3 Nr. 8 G 10-E soll die Gefahrenbereiche, deretwegen der Bundesnachrichtendienst die internationale Telekommunikation strategisch überwachen darf, um internationale Angriffe auf IT-Systeme ergänzen. Die geplante Regelung steht jedoch mit dem Fernmeldegeheimnis des Art. 10 GG nicht vollständig in Einklang. Bedenklich ist sie vor allem insoweit, als sie auch Angriffe mit kriminellem Ziel erfassen soll.

Das Bundesverfassungsgericht hat zwar in seinem zweiten G 10-Urteil aus dem Jahr 1999 festgehalten, dass strategische Telekommunikationsüberwachungen auch dann verfassungsrechtlich gerechtfertigt werden können, wenn sie Erkenntnisse über die international operierende organisierte Kriminalität gewinnen sollen. Denn solche Kriminalität kann die außen- und sicherheitspolitischen Interessen der Bundesrepublik erheblich berühren.[31]

Jedoch hat das Bundesverfassungsgericht bereits damals deutlich gemacht, dass nicht jede Form internationaler organisierter Kriminalität hinreichend schwer wiegt, um strategische Telekommunikationsüberwachungen zu rechtfertigen. Das Gericht hat die damals angegriffene Ermächtigungsnorm des § 3 Abs. 1 Satz 2 Nr. 5 G 10-a.F. deshalb insoweit verworfen, als sie auch im Ausland begangene Geldfälschungen als Gefahrenbereich aufführte. Hierzu führte es aus, Geldfälschungen bildeten nicht zwingend eine erhebliche Gefahr für Bestand und Sicherheit der Bundesrepublik. Tragfähig wäre nach Auffassung des Bundesverfassungsgerichts hingegen eine Regelung, welche sich auf Geldfälschungen großen Stils beschränkt, durch welche die Geldwertstabilität und damit die Wirtschaftskraft der Bundesrepublik bedroht sind. Eine solche Eingrenzung enthielt die seinerzeit angegriffene Regelung jedoch nicht.[32]

Zudem ist davon auszugehen, dass sich die verfassungsrechtlichen Anforderungen an strategische Telekommunikationsüberwachungen seit dem Jahr 1999 verschärft haben.[33] Denn das Bundesverfassungsgericht hat in seiner damaligen Abwägung auf technische und rechtliche Begrenzungen der Überwachung abgestellt, die heute so nicht mehr bestehen. So lassen sich unter den gegenwärtigen technischen Bedingungen inländische und internationale Telekommunikationsverkehre nicht mehr trennscharf unterscheiden. Die strategische Überwachung erfasst zudem heute im Ansatz jedes Übertragungsmedium, während sie sich seinerzeit auf nicht-leitungsgebundene Verkehre beschränkte. Zwar begrenzt das Gesetz stattdessen die Überwachung auf einen bestimmten Höchstprozentsatz der Übertragungskapazität, die auf den überwachten Übertragungswegen zur Verfügung steht. Jedoch ist zumindest fragwürdig, ob diese Vorgabe die Überwachung tatsächlich wirksam einschränkt. Schließlich haben sich die Analysemöglichkeiten des Bundesnachrichtendienstes seit dem Jahr 1999 erheblich fortentwickelt. Insgesamt wiegt der Eingriff in das Fernmeldegeheimnis, der in einer strategi-

[30] Siehe zu dieser Norm noch unten V. 1. b).

[31] BVerfGE 100, 313 (381 ff.).

[32] BVerfGE 100, 313 (384 f.); vgl. hingegen nunmehr § 5 Abs. 1 Satz 3 Nr. 5 G 10.

[33] Näher zum Folgenden *Bäcker*, K&R 2014, S. 556 (557 ff.).

schen Telekommunikationsüberwachung liegt, heute noch schwerer als zur damaligen Zeit. Dementsprechend muss das Eingriffsziel noch höheres Gewicht haben, damit der Verhältnismäßigkeitsgrundsatz gewahrt wird.

Angesichts dessen verfehlt § 5 Abs. 1 Satz 3 Nr. 8 G 10-E insoweit die verfassungsrechtlichen Anforderungen, als der Bundesnachrichtendienst die strategische Überwachung auch einsetzen können soll, um kriminelle Angriffe auf IT-Systeme zu erkennen. Solche Angriffe weisen nicht durchweg ein Schadenspotenzial auf, das den auch heute noch anzuerkennenden Gefahrenbereichen wie Kriegsgefahr, Terrorismus oder Proliferation annähernd vergleichbar wäre. So zeugen etwa Angriffe mit dem Ziel, Betrugsstraftaten zu begehen, zwar von beträchtlicher krimineller Energie und können in der Summe erhebliche Schäden verursachen. Dies unterscheidet sie jedoch nicht von anderen Formen der organisierten Eigentums- oder Vermögenskriminalität, die gleichfalls keine strategischen Telekommunikationsüberwachungen rechtfertigen können. Die tatbestandliche Einschränkung, dass es sich um Fälle von erheblicher Bedeutung handeln muss, ändert hieran nichts, da sie zu unbestimmt und unspezifisch ausfällt. Hingegen finden sich in § 5 Abs. 1 Satz 3 Nr. 8 G 10-E keine näheren Vorgaben für die bedrohten IT-Systeme oder die drohenden Schäden. Nur mithilfe solcher Vorgaben ließe sich der Anwendungsbereich der strategischen Telekommunikationsüberwachung möglicherweise auf solche Erscheinungsformen von *cyber crime* zuschneiden, die hinreichend schwer wiegen, um einen so intensiven Grundrechtseingriff zu rechtfertigen.

V. Datenübermittlungen von Nachrichtendiensten an Polizei- und Strafverfolgungsbehörden

Das Bundesverfassungsgericht hat in seinem Urteil zum Antiterrordateigesetz aus dem Recht auf informationelle Selbstbestimmung ein informationelles Trennungsprinzip für das Verhältnis von Nachrichtendiensten und Polizei- und Strafverfolgungsbehörden abgeleitet. Der Grund hierfür liegt in den unterschiedlichen Aufgaben dieser Behörden, denen unterschiedliche Verteilungen von Datenerhebungs- und Zwangsbefugnissen zugrunde liegen. Verfassungsrechtlich problematisch sind insbesondere Datenübermittlungen von Nachrichtendiensten an operativ tätige Polizei- und Strafverfolgungsbehörden. Denn bei einer solchen Datenübermittlung wirken die weitreichenden Datenerhebungsbefugnisse der Nachrichtendienste mit den weitreichenden operativen Zwangsbefugnissen der Polizei- und Strafverfolgungsbehörden zusammen. Hierin liegt ein besonders schwerer Grundrechtseingriff. Dieser Eingriff genügt nur dann dem Verhältnismäßigkeitsgrundsatz, wenn er einem herausragenden öffentlichen Interesse dient. Dies muss durch eine hinreichend konkrete und qualifizierte Eingriffsschwelle gesichert sein.[34] Es ist dabei Aufgabe des Gesetzgebers der Übermittlungsermächtigung, eine Eingriffsschwelle festzulegen, die den verfassungsrechtlichen Anforderungen genügt. Denn dieser Gesetzgeber trägt eine grundrechtliche Regelungsverantwortung für den Umgang mit den Daten, die er zur Übermittlung freigibt.[35]

[34] BVerfGE 133, 277 (329).

[35] Vgl. BVerfGE 125, 260 (346); 130, 151 (201).

Das Urteil zum Antiterrordateigesetz erfordert es, die Datenübermittlungsregelungen des Nachrichtendienstrechts zu überarbeiten.[36] Der Gesetzentwurf wird dem nicht vollständig gerecht. Dies gilt sowohl für die vorgesehenen Regelungen im BVerfSchG als auch im G 10.

1. Übermittlungsermächtigungen im BVerfSchG

Der Entwurf sieht vor, § 19 Abs. 1 BVerfSchG neu zu fassen. Dies ist auch angezeigt, denn diese Norm weist momentan besonders schwere verfassungsrechtliche Mängel auf.[37] Jedoch begegnet die geplante Neufassung ihrerseits zum Teil verfassungsrechtlichen Bedenken. Zudem verfehlt auch § 20 BVerfSchG teils die verfassungsrechtlichen Anforderungen; diese Regelung soll nach dem Entwurf indes nicht geändert werden. Schließlich sind die Datenübermittlungsregelungen des BVerfSchG auch insoweit überarbeitungsbedürftig, als sie teilweise einen Informationsfluss von den Nachrichtendiensten selbst in gravierenden Fällen nicht zuverlässig gewährleisten. Diesem Defizit begegnet der Entwurf nicht, obwohl sein erklärtes Ziel darin besteht, die Kooperation der Sicherheitsbehörden zu verbessern.

a) Defizite von § 19 Abs. 1 BVerfSchG-E

§ 19 Abs. 1 BVerfSchG-E differenziert überzeugend zwischen Daten, die mit nachrichtendienstlichen Mitteln erhoben wurden, und sonstigen (insbesondere aus öffentlichen Quellen gewonnenen) Daten des Bundesamts für Verfassungsschutz.[38] Für die sensibleren Daten, die mit nachrichtendienstlichen Mitteln erhoben wurden, errichtet Satz 1 mehrere Übermittlungstatbestände mit unterschiedlichen Übermittlungszwecken. Überwiegend sind diese Tatbestände unbedenklich. Verfassungsrechtlichen Bedenken begegnet jedoch die vorgesehene Übermittlungsermächtigung in § 19 Abs. 1 Satz 1 Nr. 3 BVerfSchG-E, die eine Übermittlung zur Verhinderung oder sonstigen Verhütung von Straftaten von erheblicher Bedeutung vorsieht. Für diese Bedenken gibt es zwei Gründe:

Erstens droht der strafprozessuale Begriff der Straftat von erheblicher Bedeutung den präventivpolizeilichen Übermittlungstatbestand zu entgrenzen. Soweit durch eine Straftat Schäden für besonders bedeutsame Rechtsgüter drohen, ist bereits der Übermittlungstatbestand des § 19 Abs. 1 Satz 1 Nr. 2 BVerfSchG-E verwirklicht. Einer weiteren Übermittlungsermächtigung, die auf die Kriminalprävention zugeschnitten ist, bedarf es insoweit nicht. Allerdings finden sich im materiellen Strafrecht zahlreiche Deliktstatbestände, die Handlungen im Vorfeld strafbarer Rechtsgutsverletzungen bei Strafe verbieten. Insbesondere das Terrorismusstrafrecht zeichnet sich durch eine nahezu flächendeckende Vorfeldkriminalisierung aus.[39] Viele dieser Straftaten sind schon wegen hoher Strafandrohungen[40] ohne weiteres als Straftaten von erheblicher Bedeutung anzusehen, die im strafrechtlichen Ermittlungsverfahren ein-

---

[36] So etwa der Bericht der Regierungskommission zur Überprüfung der Sicherheitsgesetzgebung in Deutschland, 2013, S. 200 ff., mit unterschiedlichen Akzentuierungen durch die Kommissionsmitglieder.

[37] Eingehend zu diesen Mängeln *Gazeas,* Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, 2014, S. 409 ff.

[38] Näher zu der unterschiedlichen Eingriffsintensität in beiden Übermittlungskonstellationen *Gazeas,* Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, 2014, S. 249 ff.

[39] Näher die Kommissionsmitglieder *Bäcker, Hirsch* und *Wolff* im Bericht der Regierungskommission zur Überprüfung der Sicherheitsgesetzgebung in Deutschland, 2013, S. 37 ff.

[40] Vgl. beispielhaft § 89a StGB (Vorbereitung einer schweren staatsgefährdenden Gewalttat) – Freiheitsstrafe von sechs Monaten bis zu zehn Jahren; § 129a Abs. 1 und 2 StGB (Bildung einer terroristischen Vereinigung) – Freiheitsstrafe von einem Jahr bis zu zehn Jahren.

griffsintensive Überwachungsmaßnahmen rechtfertigen können, wenn ein Tatverdacht besteht. Allerdings führt der materiell-strafrechtliche Vorfeldansatz dazu, dass in beträchtlichem Umfang Handlungen weniger wegen ihres unmittelbaren Schadenspotenzials als deswegen verboten werden, weil sich in ihnen der Wille des Handelnden manifestiert, weitere Straftaten zu begehen. Wenn präventivpolizeiliche Ermächtigungen an solche Vorfeldtatbestände anknüpfen, dehnen sie die strafrechtliche Vorverlagerung noch aus. Sie ermöglichen dann Eingriffsmaßnahmen in weitgehend diffusen und zumeist höchst ambivalenten Bedrohungslagen, in denen Schäden für hochrangige Rechtsgüter allenfalls mittelbar und in geraumer Zeit zu besorgen sind. Mit den verfassungsrechtlichen Geboten der Bestimmtheit und Verhältnismäßigkeit ist dies nicht zu vereinbaren. Präventivpolizeiliche Eingriffsermächtigungen dürfen daher grundsätzlich nicht auf strafrechtliche Vorfeldtatbestände verweisen.[41] Für Übermittlungsermächtigungen zu präventivpolizeilichen Zwecken gilt dies ebenso. Soweit ein eigenständiger Übermittlungstatbestand für die polizeiliche Kriminalprävention in § 19 Abs. 1 Satz 1 BVerfSchG-E überhaupt erforderlich sein sollte, müssten die Straftaten, die eine Datenübermittlung rechtfertigen, nach spezifisch präventivpolizeilichen Kriterien ausgewählt und enumerativ aufgezählt werden.

Zweitens ermöglicht § 19 Abs. 1 Satz 1 Nr. 3 BVerfSchG-E Datenübermittlungen auch, um Straftaten zu verhüten. Der Begriff der Straftatverhütung soll nach der Gesetzesbegründung – die sich mit Teilen der Gesetzgebungspraxis, Rechtsprechung und Literatur zum Polizeirecht deckt[42] – auf Bedrohungslagen im Vorfeld konkreter Gefahren verweisen.[43] Angesichts der hohen Eingriffsintensität einer Datenübermittlung von einem Nachrichtendienst an eine Polizeibehörde bestehen jedoch erhebliche Zweifel, ob eine solche Übermittlung im Gefahrvorfeld überhaupt verfassungsrechtlich gerechtfertigt werden kann. Zumindest aber müsste die Übermittlungsermächtigung einschränkende Tatbestandsmerkmale enthalten, um den Übermittlungsanlass so zuzuschneiden, dass der Verhältnismäßigkeitsgrundsatz gewahrt bleibt.[44] § 19 Abs. 1 Satz 1 Nr. 3 BVerfSchG-E leistet dies nicht ansatzweise.

b) Fortbestehende Mängel von § 20 und § 23 BVerfSchG

Kritikwürdig ist weiter, dass der Entwurf sich darauf beschränkt, § 19 Abs. 1 BVerfSchG neu zu fassen. Denn auch die anderen Übermittlungsregelungen dieses Gesetzes begegnen teils verfassungsrechtlichen Bedenken. Zudem gewährleisten sie nicht hinreichend zuverlässig, dass das Bundesamt für Verfassungsschutz in schwerwiegenden Fällen die erforderlichen Daten an Polizei- und Strafverfolgungsbehörden übermittelt.

Gleichzeitig zu weit und zu eng gefasst ist die Übermittlungsermächtigung in § 20 Abs. 1 Satz 1 BVerfSchG. Diese Norm verpflichtet das Bundesamt für Verfassungsschutz, Daten an die Polizei- und Strafverfolgungsbehörden zu übermitteln, wenn die Daten benötigt werden, um Staatsschutzdelikte zu verhindern oder zu verfolgen. Einerseits reicht der Begriff des Staatsschutzdelikts, der in § 20 Abs. 1 Satz 2 BVerfSchG definiert wird, sehr weit und umfasst bei entsprechender Motivation auch Straftaten von geringem Gewicht wie eine rassisti-

---

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

[42] Vgl. etwa *Denninger*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 5. Aufl. 2012, Rn. D 1 ff.

[43] BT-Drs. 18/4654, S. 34.

[44] Vgl. zur präventivpolizeilichen Telekommunikationsüberwachung BVerfGE 113, 348 (385 ff.).

sche Beleidigung oder Sachbeschädigung. Andererseits besteht keine Übermittlungspflicht bei Straftaten ohne Staatsschutzbezug, selbst wenn es sich um schwerste Kriminalität handelt.[45] Diese in sich inkohärente und teils verfassungswidrige Norm sollte gleichfalls überarbeitet werden.

Korrekturbedürftig ist zudem § 23 Nr. 2 BVerfSchG, der eine Datenübermittlung verbietet, wenn überwiegende Sicherheitsinteressen der Übermittlung entgegenstehen.[46] Hierzu zählen insbesondere Anliegen des Quellen- und Methodenschutzes. Es spricht viel dafür, dass diese Regelung in der Vergangenheit teils vorschnell herangezogen wurde, um nachrichtendienstliche Informationsbestände auch in schwerwiegenden Fällen gegen Polizei- und Strafverfolgungsbehörden abzuschotten. Daher sollte das Übermittlungsverbot tatbestandlich spezifiziert[47] und ein Verfahren eingerichtet werden, um die Anwendung dieser Norm zu kontrollieren. Denkbar wäre etwa, die Entscheidung darüber, ob die Voraussetzungen des Übermittlungsverbots vorliegen, auf die oberste Dienstbehörde zu verlagern.[48]

2. Defizite von § 7 Abs. 4 Satz 1 Nr. 2, Satz 2 G 10-E

Die vorgesehene Ermächtigung des Bundesnachrichtendienstes, Daten aus strategischen Telekommunikationsüberwachungen zur Verhütung oder Verfolgung bestimmter Straftaten an Polizei- und Strafverfolgungsbehörden zu übermitteln, steht mit den Anforderungen von Art. 10 GG nicht in Einklang.

Der geregelte Übermittlungseingriff wiegt äußerst schwer. Zu dem ohnehin hohen Gewicht, das einer Datenübermittlung von einem Nachrichtendienst an eine operativ tätige Polizei- oder Strafverfolgungsbehörde zukommt, tritt hier noch die sehr hohe Eingriffsintensität der strategischen Telekommunikationsüberwachung hinzu, die das besonders gewährleistete Grundrecht aus Art. 10 GG beschränkt.[49]

Angesichts dessen erscheint eine solche Datenübermittlung zur Strafverfolgung nur angemessen, wenn der Verdacht einer schweren Straftat besteht. Sollen Daten zu präventivpolizeilichen Zwecken übermittelt werden, ist die Übermittlung an eine konkrete Gefahr für ein besonders bedeutsames Rechtsgut zu knüpfen.[50] Diese Anforderungen verfehlt die geplante Übermittlungsermächtigung deutlich.

---

[45] Eingehend *Gazeas,* Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, 2014, S. 318 ff.

[46] Näher *Gazeas,* Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, 2014, S. 361 ff.

[47] In Betracht kommen insbesondere Rückausnahmen von dem Übermittlungsverbot und präzisere Abwägungsregeln, vgl. beispielhaft den Regelungsvorschlag im Abschlussbericht der Bund-Länder-Kommission Rechtsterrorismus, 2013, Rn. 721.

[48] Hierfür *Gazeas,* Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, 2014, S. 594 ff., der insgesamt acht Regelungsmodelle für die Zuständigkeit erörtert.

[49] Zur erhöhten Eingriffsintensität einer Datenübermittlung, die Daten aus Telekommunikationsüberwachungen zum Gegenstand hat, BVerfGE 133, 277 (372 f.).

[50] Ansatzweise bereits wie hier, aber tendenziell großzügiger noch das zweite G 10-Urteil des Bundesverfassungsgerichts, BVerfGE 100, 313 (391 ff.). Die damaligen Ausführungen sind jedoch durch die später ergangene Rechtsprechung des Bundesverfassungsgerichts zum Sicherheitsrecht teils überholt. Zudem muss auf der Ebene der Datenübermittlung gleichfalls der zwischenzeitlich weiter gestiegenen Eingriffsintensität der strategischen Telekommunikationsüberwachung Rechnung getragen werden, siehe dazu oben IV.

Die vorgesehene Ermächtigung in § 7 Abs. 4 Satz 1 Nr. 2, Satz 2 G 10-E, Daten an Strafverfolgungsbehörden zu übermitteln, ist insoweit nicht zu beanstanden, als sie auf den Straftatenkatalog für die strafprozessuale Telekommunikationsüberwachung in § 100a Abs. 2 StPO verweist.[51] Daneben ermöglicht die Norm jedoch Datenübermittlungen auch zu dem Ziel, weitere Straftaten zu verfolgen, die in § 3 Abs. 1 Satz 1 Nr. 1, 2, 5 und 7, Satz 2 und Abs. 1a G 10 genannt sind. Dabei handelt es sich nicht durchweg um hinreichend gewichtige Straftaten. Beispielhaft seien die Bagatelldelikte des § 20 Abs. 1 Nr. 1 bis 4 VereinsG (aufgeführt in § 3 Abs. 1 Satz 1 Nr. 2 G 10) und des § 95 Abs. 1 Nr. 8 AufenthG (aufgeführt in § 3 Abs. 1 Satz 1 Nr. 7 G 10) genannt, die beide im Höchstmaß lediglich mit einer Freiheitsstrafe von einem Jahr bedroht sind.[52]

Die vorgesehene Ermächtigung in § 7 Abs. 4 Satz 1 Nr. 2 G 10-E, Daten zu präventivpolizeilichen Zwecken zu übermitteln, ist in noch größerem Ausmaß verfassungsrechtlich unzureichend. Dies gilt selbst dann, wenn davon ausgegangen wird, dass die tatbestandlich vorausgesetzte Planung einer Straftat stets eine konkrete Gefahr dieser Tat begründet.[53] Denn zur Verhinderung von wenig gewichtigen Straftaten, auf die § 3 G 10 zum Teil verweist, ist eine Datenübermittlung wiederum nicht angemessen. Zudem verweist die geplante Übermittlungsregelung über die angeführten Straftatkataloge auch auf materiell-strafrechtliche Vorfeldtatbestände,[54] die in einer präventivpolizeilich ausgerichteten Ermächtigung fehl am Platze sind.[55]

---

[51] Zur Verhältnismäßigkeit dieses Katalogs BVerfGE 129, 208 (243 f.).

[52] Zur indiziellen Bedeutung der Strafandrohung für das Gewicht des öffentlichen Interesses an einer wirksamen Strafverfolgung BVerfGE 129, 208 (243). Es würde den Rahmen dieser Stellungnahme sprengen zu erörtern, ob die Überwachungsermächtigung des § 3 Abs. 1 Satz 1 G 10 in jeder Hinsicht das grundrechtliche Fernmeldegeheimnis wahrt.

[53] Im Gefahrvorfeld verortet das Planungsstadium hingegen anscheinend BVerfGE 100, 313 (392).

[54] Etwa auf § 89a StGB (Katalogtat nach § 3 Abs. 1 Satz 1 Nr. 2 G 10) sowie auf § 129 StGB (Katalogtat nach § 100a Abs. 2 Nr. 1 Buchstabe d StPO).

[55] Siehe oben V. 1. a).