L e i t s ä t z e

zum Beschluss des Ersten Senats vom 28. September 2022

- 1 BvR 2354/13 -

(Bundesverfassungsschutzgesetz – Übermittlungsbefugnisse)

1. Die Gesetzgebungskompetenz des Bundes aus Art. 73 Abs. 1 Nr. 10 GG erstreckt sich nicht nur auf die Zusammenarbeit des Bundes und der Länder, sondern auch auf die der Länder untereinander. Sie umfasst hingegen nicht die Regelung der Zusammenarbeit zwischen Behörden desselben Landes.

2. Die Normenklarheit setzt der Verwendung gesetzlicher Verweisungsketten Grenzen, steht dieser aber nicht grundsätzlich entgegen. Bei der Normierung sicherheitsrechtlicher Datenverarbeitungen kann es zweckdienlich sein, auf Fachgesetze zu verweisen, in deren Kontext Auslegungsfragen – anders als bei heimlichen Maßnahmen – im Wechselspiel von Anwendungspraxis und gerichtlicher Kontrolle verbindlich geklärt werden können. Ob eine Verweisung mit dem Gebot der Normenklarheit vereinbar ist, hängt von einer wertenden Gesamtbetrachtung unter Berücksichtigung möglicher Regelungsalternativen ab. Das Erfassen des Normgehaltes wird insbesondere durch Verweisungsketten erleichtert, die die in Bezug genommenen Vorschriften vollständig aufführen.

3. Die Übermittlung mit nachrichtendienstlichen Mitteln erhobener personenbezogener Daten und Informationen durch den Verfassungsschutz zur Gefahrenabwehr kann als Übermittlungsschwelle grundsätzlich auch an die Gefahr der Begehung solcher Straftaten anknüpfen, bei denen die Strafbarkeitsschwelle durch die Pönalisierung von Vorbereitungshandlungen oder bloßen Rechtsgutgefährdungen in das Vorfeld von Gefahren verlagert wird. Der Gesetzgeber muss dann aber sicherstellen, dass in jedem Einzelfall eine konkrete oder konkretisierte Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegt. Diese ergibt sich nicht notwendiger Weise bereits aus der Gefahr der Tatbestandsverwirklichung selbst.

BUNDESVERFASSUNGSGERICHT

- 1 BvR 2354/13 -

IM NAMEN DES VOLKES

In dem Verfahren
über
die Verfassungsbeschwerde

des Herrn (…),

- Bevollmächtigter: (…) -

gegen § 19 Absatz 1 Satz 1, § 20 Absatz 1 Satz 1 und 2 sowie § 21 Absatz 1 Satz 1 des Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz – BVerfSchG)
– unter Bezugnahme auf das Rechtsextremismus-Datei-Gesetz (RED-G)

hat das Bundesverfassungsgericht – Erster Senat –
unter Mitwirkung der Richterinnen und Richter
Präsident Harbarth,
Baer,
Britz,
Ott,
Christ,
Radtke,
Härtel,
Wolff

am 28. September 2022 beschlossen:

1. § 20 Absatz 1 Satz 1 und 2 und § 21 Absatz 1 Satz 1 in Verbindung mit § 20 Absatz 1 Satz 1 und 2 des Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz) in der Fassung vom 20. Dezember 1990 (Bundesgesetzblatt I Seite 2954, 2970) sind mit Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes nicht vereinbar, soweit sie zur Übermittlung personenbezogener Daten verpflichten, die mit nachrichtendienstlichen Mitteln erhoben wurden.

2. Bis zu einer Neuregelung, längstens jedoch bis zum 31. Dezember 2023, gelten die für mit dem Grundgesetz unvereinbar erklärten Vorschriften mit der Maßgabe fort, dass eine Übermittlung von mit nachrichtendienstlichen Mitteln erhobenen personenbezogenen Daten nur zum Schutz eines Rechtsguts von herausragendem öffentlichem Interesse zulässig ist; dem entspricht eine Begrenzung auf besonders schwere Straftaten. Außerdem müssen die nach Maßgabe der Gründe an die jeweilige Übermittlungsschwelle zu stellenden Anforderungen erfüllt sein.

3. Im Übrigen wird die Verfassungsbeschwerde verworfen.

4. Die Bundesrepublik Deutschland hat dem Beschwerdeführer drei Viertel seiner notwendigen Auslagen aus dem Verfassungsbeschwerdeverfahren zu erstatten.

G r ü n d e :

A.

Die Verfassungsbeschwerde richtet sich gegen die allgemeinen Befugnisse des Bundesamtes für Verfassungsschutz sowie der Verfassungsschutzbehörden der Länder zur Übermittlung personenbezogener Daten und Informationen nach dem Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz – BVerfSchG), soweit die Vorschriften des Gesetzes zur Errichtung einer standardisierten zentralen Datei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern zur Bekämpfung des gewaltbezogenen Rechtsextremismus (Rechtsextremismus-Datei-Gesetz – RED-G) auf sie Bezug nehmen. 1

Der Beschwerdeführer wandte sich mit seiner im August 2013 erhobenen Verfassungsbeschwerde zunächst gegen § 19 Abs. 1 Satz 1 BVerfSchG in der Fassung vom 5. Januar 2007 (BGBl I S. 2), der eine Generalklausel zur ermessensabhängigen Übermittlung personenbezogener Daten durch das Bundesamt für Verfassungsschutz an inländische öffentliche Stellen enthielt. Weiter griff er § 20 Abs. 1 Satz 1 und 2 sowie § 21 Abs. 1 Satz 1 in Verbindung mit § 20 Abs. 1 Satz 1 und 2 BVerfSchG jeweils in der Fassung vom 20. Dezember 1990 (BGBl I S. 2954) an, die die Übermittlungspflicht des Bundesamtes für Verfassungsschutz und der Verfassungsschutzbehörden der Länder an Polizeien und Staatsanwaltschaften zur Verhinderung und Verfolgung von Staatsschutzdelikten normieren. 2

Die angegriffenen Vorschriften werden durch § 8 RED-G in der Fassung vom 20. August 2012 (BGBl I S. 1798) in Bezug genommen, der für die Übermittlungen von Erkenntnissen aufgrund eines Ersuchens nach § 6 Abs. 1 Satz 1 RED-G zwischen den beteiligten Behörden auf die jeweils geltenden Übermittlungsvorschriften der Fachgesetze verweist. 3

Nach Erhebung der Verfassungsbeschwerde wurde § 19 Abs. 1 Satz 1 BVerfSchG durch das am 21. November 2015 in Kraft getretene Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 17. November 2015 (BGBl I S. 1938) geändert. 4

I.

1. Die angegriffenen Regelungen betreffen die allgemeine Befugnis zur Übermittlung personenbezogener Daten durch das Bundesamt für Verfassungsschutz sowie die Übermittlungspflicht des Bundesamtes für Verfassungsschutz und der Verfassungsschutzbehörden der Länder an Strafverfolgungs- und Sicherheitsbehörden in Angelegenheiten des Staats- und Verfassungsschutzes. Daneben finden sich im Bundesverfassungsschutzgesetz und in anderen Fachgesetzen verschiedene auf spezifische Erhebungstatbestände abgestimmte Übermittlungsvorschriften, die nicht angegriffen wurden. 5

§ 19 Abs. 1 Satz 1 BVerfSchG ermöglichte in seiner ursprünglichen Fassung die Übermittlung personenbezogener Daten durch das Bundesamt für Verfassungsschutz an inländische öffentliche Stellen, wenn dies zur Erfüllung seiner Aufgaben erforderlich war oder der Empfänger die Daten zum Schutz der freiheitlichen demokratischen Grundordnung oder sonst für Zwecke der öffentlichen Sicherheit benötigte. 6

Mit dem Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 17. November 2015 wurde diese Übermittlungsbefugnis umgestaltet. Das Ziel der Novelle war insbesondere, den Vorgaben des Urteils des Bundesverfassungsgerichts vom 24. April 2013 zum Antiterrordateigesetz (BVerfGE 133, 277) Rechnung zu tragen. Deshalb sollten im Hinblick auf das informationelle Trennungsprinzip die Voraussetzungen klarstellend normiert werden, die für die Übermittlung von Erkenntnissen, die mit besonderen Mitteln nachrichtendienstlich gewonnen worden sind, an operativ tätige Behörden gelten (vgl. BTDrucks 18/4654, S. 32 f.). Die Übermittlung von mit nachrichtendienstlichen Mitteln nach § 8 Abs. 2 BVerfSchG erhobenen personenbezogenen Daten an diese Stellen wurde deshalb in § 19 Abs. 1 Satz 1 BVerfSchG neu geregelt, während die Datenübermittlung im Übrigen in § 19 Abs. 1 Satz 2 BVerfSchG n.F. verortet wurde. Zudem ergänzte der Gesetzgeber die Übermittlungsvariante „[wenn der Empfänger die Daten] sonst für Zwecke der öffentlichen Sicherheit benötigt“ um das Erfordernis „erheblicher“ Zwecke, um bagatellarische Sachverhalte auszuscheiden (vgl. BTDrucks 18/4654, S. 34). 7

§ 20 Abs. 1 Satz 1 BVerfSchG regelt als lex specialis (vgl. § 19 Abs. 1 Satz 1 a.E. BVerfSchG n.F.) die Übermittlung von Informationen einschließlich personenbezogener Daten durch das Bundesamt für Verfassungsschutz an die Staatsanwaltschaften und Polizeien in Angelegenheiten des Staats- und Verfassungs- 8

schutzes. Im Gegensatz zur ermessensabhängigen Übermittlungsbefugnis des § 19 BVerfSchG verpflichtet die Vorschrift das Bundesamt für Verfassungsschutz zur Informationsweitergabe. § 20 Abs. 1 Satz 2 BVerfSchG definiert die Staatsschutzdelikte unter Bezugnahme auf die Kataloge der §§ 74a und 120 des Gerichtsverfassungsgesetzes (GVG) und enthält eine Generalklausel für sonstige Straftaten, die gegen die in Art. 73 Abs. 1 Nr. 10 Buchstabe b oder c GG genannten Schutzgüter gerichtet sind. An deren Schutz bestehe – zumal vor kriminellen Angriffen – ein herausragendes öffentliches Interesse (vgl. BTDrucks 18/4654, S. 34). § 21 Abs. 1 Satz 1 BVerfSchG erstreckt die Übermittlungspflichten des § 20 Abs. 1 Satz 1 und 2 BVerfSchG entsprechend auf die Verfassungsschutzbehörden der Länder.

2. Auf diese Übermittlungsregelungen verweist das Rechtsextremismus-Datei-Gesetz, mit dem der Gesetzgeber bezweckte, angesichts der Bedrohung durch den gewaltbezogenen Rechtsextremismus den Informationsaustausch zwischen Polizeien und Nachrichtendiensten weiter zu verbessern (vgl. BTDrucks 17/8672, S. 1). Nach dem Vorbild der Antiterrordatei schuf der Gesetzgeber die Rechtsgrundlage für die Rechtsextremismus-Datei, eine der Bekämpfung des gewaltbezogenen Rechtsextremismus dienende Verbunddatei von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder. Die Datei erleichtert und beschleunigt den Informationsaustausch, indem bestimmte Erkenntnisse aus dem Zusammenhang der Bekämpfung des gewaltbezogenen Rechtsextremismus, über die einzelne Behörden verfügen, für alle beteiligten Behörden schneller auffindbar und leichter zugänglich werden (vgl. BTDrucks 17/8672, S. 10 f.; zur Antiterrordatei BVerfGE 133, 277 <280 Rn. 3>). 9

§ 2 RED-G bestimmt, dass und in Bezug auf welche Personen oder Objekte Behörden verpflichtet sind, bereits erhobene Daten in der Rechtsextremismus-Datei zu speichern. Voraussetzung einer Speicherung ist dabei, dass polizeiliche oder nachrichtendienstliche Erkenntnisse vorliegen, aus denen sich tatsächliche Anhaltspunkte dafür ergeben, dass sich die Daten auf die in § 2 Satz 1 Nr. 1 bis 3 RED-G genannten Personen oder Objekte beziehen und dass die Kenntnis der Daten für die Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus erforderlich ist. 10

Welche Daten zu speichern sind, ergibt sich aus § 3 Abs. 1 RED-G. Die Regelung unterscheidet zwischen den in § 3 Abs. 1 Nr. 1 Buchstabe a RED-G aufgeführten Grunddaten (unter anderem Name, Geschlecht, Alter, Anschrift) und den 11

in § 3 Abs. 1 Nr. 1 Buchstabe b RED-G aufgeführten erweiterten Grunddaten (beispielsweise Telefon-/Faxanschlüsse, Adressen für elektronische Post, Bankverbindungen).

Zugriff auf die Rechtsextremismus-Datei haben die in § 1 Abs. 1 RED-G benannten Behörden, also das Bundeskriminalamt, die in der Rechtsverordnung nach § 58 Abs. 1 des Bundespolizeigesetzes (BPolG) bestimmte Bundespolizeibehörde, die Landeskriminalämter, die Verfassungsschutzbehörden des Bundes und der Länder sowie der Militärische Abschirmdienst. Hinzu kommen nach § 1 Abs. 2 RED-G in Verbindung mit der Verordnung über die Benennung weiterer zur Teilnahme an der Rechtsextremismus-Datei berechtigter Polizeivollzugsbehörden vom 11. März 2015 (BGBl I S. 302, 303) einzelne Polizeivollzugsbehörden. § 6 Abs. 4 RED-G regelt, dass die Polizeibehörden den Staatsanwaltschaften die Daten zum Zwecke der Strafverfolgung übermitteln, auf die sie Zugriff erhalten haben, soweit sie die Rechtsextremismus-Datei auf Ersuchen oder im Auftrag der das strafrechtliche Ermittlungsverfahren führenden Staatsanwaltschaft nutzen. Diese Daten darf die Staatsanwaltschaft wiederum für eigene Ersuchen an die einspeichernden Behörden verwenden. 12

Im Regelfall erlaubt § 5 Abs. 1 Nr. 1 Buchstabe a RED-G den berechtigten Behörden bei einer Abfrage zu Personen einen unmittelbaren Zugriff lediglich auf die zu ihrer Identifizierung gespeicherten Grunddaten nach § 3 Abs. 1 Nr. 1 Buchstabe a RED-G. Nach § 6 Abs. 1 Satz 1 RED-G darf die abfragende Behörde die Daten, auf die sie gemäß § 5 Abs. 1 RED-G Zugriff erhalten hat, insbesondere zur Vorbereitung und Substantiierung eines Einzelübermittlungsersuchens verwenden. In § 8 RED-G ist festgelegt, dass sich die Übermittlung von Erkenntnissen aufgrund eines Ersuchens nach § 6 Abs. 1 Satz 1 RED-G nach den jeweils geltenden Übermittlungsvorschriften richtet. Dies sind – unter anderem – die vorliegend angegriffenen § 19 Abs. 1 Satz 1 BVerfSchG a.F. und § 20 Abs. 1 Satz 1 und 2 BVerfSchG sowie § 21 Abs. 1 Satz 1 in Verbindung mit § 20 Abs. 1 Satz 1 und 2 BVerfSchG. 13

3. Die für das Verfahren relevanten Normen des Bundesverfassungsschutzgesetzes und des Rechtsextremismus-Datei-Gesetzes haben in den hier maßgeblichen Fassungen auszugsweise den folgenden Wortlaut: 14

§ 19 BVerfSchG in der Fassung vom 5. Januar 2007 (BGBl I S. 2) – Übermittlung personenbezogener Daten durch das Bundesamt für Verfassungsschutz

(1) [1]Das Bundesamt für Verfassungsschutz darf personenbezogene Daten an inländische öffentliche Stellen übermitteln, wenn dies zur Erfüllung seiner Aufgaben erforderlich ist oder der Empfänger die Daten zum Schutz der freiheitlichen demokratischen Grundordnung oder sonst für Zwecke der öffentlichen Sicherheit benötigt. [2]Der Empfänger darf die übermittelten Daten, soweit gesetzlich nichts anderes bestimmt ist, nur zu dem Zweck verwenden, zu dem sie ihm übermittelt wurden.

[…]

§ 19 BVerfSchG in der Fassung vom 17. November 2015 (BGBl I S. 1938) – Übermittlung personenbezogener Daten durch das Bundesamt für Verfassungsschutz

(1) [1]Das Bundesamt für Verfassungsschutz darf personenbezogene Daten, die mit den Mitteln nach § 8 Absatz 2 erhoben worden sind, an die Staatsanwaltschaften, die Finanzbehörden nach § 386 Absatz 1 der Abgabenordnung, die Polizeien, die mit der Steuerfahndung betrauten Dienststellen der Landesfinanzbehörden, die Behörden des Zollfahndungsdienstes sowie andere Zolldienststellen, soweit diese Aufgaben nach dem Bundespolizeigesetz wahrnehmen, übermitteln, soweit dies erforderlich ist zur

1. Erfüllung eigener Aufgaben der Informationsgewinnung (§ 8 Absatz 1 Satz 2 und 3),

2. Abwehr einer im Einzelfall bestehenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben, Gesundheit oder Freiheit einer Person oder für Sachen von erheblichem Wert, deren Erhaltung im öffentlichen Interesse geboten ist,

3. Verhinderung oder sonstigen Verhütung von Straftaten von erheblicher Bedeutung oder

4. Verfolgung von Straftaten von erheblicher Bedeutung;

§ 20 bleibt unberührt. [2]Im Übrigen darf es an inländische öffentliche Stellen personenbezogene Daten übermitteln, wenn dies zur Erfüllung seiner Aufgaben erforderlich ist oder der Empfänger die Daten zum Schutz der freiheitlichen demokratischen Grundordnung oder sonst für erhebliche Zwecke der öffentlichen Sicherheit benötigt. [3]Der

Empfänger darf die übermittelten Daten, soweit gesetzlich nichts anderes bestimmt ist, nur zu dem Zweck verwenden, zu dem sie ihm übermittelt wurden.

[…]

Der in Bezug genommene § 8 Abs. 2 BVerfSchG lautet: 15

§ 8 Abs. 2 BVerfSchG in der Fassung vom 19. Juni 2020 (BGBl I S. 1328) – Befugnisse des Bundesamtes für Verfassungsschutz

(1) […]

(2) [1]Das Bundesamt für Verfassungsschutz darf Methoden, Gegenstände und Instrumente zur heimlichen Informationsbeschaffung, wie den Einsatz von Vertrauensleuten und Gewährspersonen, Observationen, Bild- und Tonaufzeichnungen, Tarnpapiere und Tarnkennzeichen anwenden. […]

§ 20 BVerfSchG in der Fassung vom 20. Dezember 1990 (BGBl I S. 2954) – Übermittlung von Informationen durch das Bundesamt für Verfassungsschutz an Strafverfolgungs- und Sicherheitsbehörden in Angelegenheiten des Staats- und Verfassungsschutzes

(1) [1]Das Bundesamt für Verfassungsschutz übermittelt den Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, den Polizeien von sich aus die ihm bekanntgewordenen Informationen einschließlich personenbezogener Daten, wenn tatsächliche Anhaltspunkte dafür bestehen, daß die Übermittlung zur Verhinderung oder Verfolgung von Staatsschutzdelikten erforderlich ist. [2]Delikte nach Satz 1 sind die in §§ 74a und 120 des Gerichtsverfassungsgesetzes genannten Straftaten sowie sonstige 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. [3]Das Bundesamt für Verfassungsschutz übermittelt dem Bundesnachrichtendienst von sich aus die ihm bekanntgewordenen Informationen einschließlich personenbezogener Daten, wenn tatsächliche Anhaltspunkte dafür bestehen, daß die Übermittlung für die Erfüllung der gesetzlichen Aufgaben des Empfängers erforderlich ist.

(2) [1]Die Polizeien dürfen zur Verhinderung von Staatsschutzdelikten nach Absatz 1 Satz 2 das Bundesamt für Verfassungsschutz um Übermittlung der erforderlichen Informationen einschließlich personenbezogener Daten ersuchen. [2]Der Bundesnachrichtendienst darf zur Erfüllung seiner Aufgaben das Bundesamt für Verfassungsschutz

um die Übermittlung der erforderlichen Informationen einschließlich personenbezogener Daten ersuchen.

§ 21 BVerfSchG in der Fassung vom 20. Dezember 1990 (BGBl I S. 2954) – Übermittlung von Informationen durch die Verfassungsschutzbehörden der Länder an Strafverfolgungs- und Sicherheitsbehörden in Angelegenheiten des Staats- und Verfassungsschutzes

(1) [1]Die Verfassungsschutzbehörden der Länder übermitteln den Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, den Polizeien Informationen einschließlich personenbezogener Daten unter den Voraussetzungen des § 20 Abs. 1 Satz 1 und 2 sowie Abs. 2 Satz 1. [2]Auf die Übermittlung von Informationen zwischen Behörden desselben Bundeslandes findet Satz 1 keine Anwendung.

[…]

§ 23 BVerfSchG vom 20. Dezember 1990 (BGBl I S. 2954) – Übermittlungsverbote

Die Übermittlung nach den Vorschriften dieses Abschnitts unterbleibt, wenn

1. für die übermittelnde Stelle erkennbar ist, daß unter Berücksichtigung der Art der Informationen und ihrer Erhebung die schutzwürdigen Interessen des Betroffenen das Allgemeininteresse an der Übermittlung überwiegen,

2. überwiegende Sicherheitsinteressen dies erfordern oder

3. besondere gesetzliche Übermittlungsregelungen entgegenstehen; die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

Die relevanten Vorschriften des Rechtsextremismus-Datei-Gesetzes lauten wie folgt: 16

§ 2 RED-G in der Fassung vom 18. Dezember 2014 (BGBl I S. 2318) – Inhalt der Datei und Speicherungspflicht

[1]Die beteiligten Behörden sind verpflichtet, bereits erhobene Daten nach § 3 Absatz 1 in der Datei nach § 1 zu speichern, wenn sie gemäß den für sie geltenden Rechtsvorschriften über polizeiliche oder

nachrichtendienstliche Erkenntnisse (Erkenntnisse) verfügen, dass die Daten sich beziehen auf

1. Personen

   a) bei denen Tatsachen die Annahme rechtfertigen, dass sie einer terroristischen Vereinigung nach § 129a des Strafgesetzbuchs mit rechtsextremistischem Hintergrund angehören oder diese unterstützen,

   b) die als Täter oder Teilnehmer einer rechtsextremistischen Gewalttat Beschuldigte oder rechtskräftig Verurteilte sind;

2. Personen, bei denen Tatsachen die Annahme rechtfertigen, dass sie rechtsextremistische Bestrebungen verfolgen und in Verbindung damit zur Gewalt aufrufen, die Anwendung von rechtsextremistisch begründeter Gewalt als Mittel zur Durchsetzung politischer Belange unterstützen, vorbereiten oder durch ihre Tätigkeiten vorsätzlich hervorrufen oder bei denen Schusswaffen ohne die erforderlichen waffenrechtlichen Berechtigungen, Kriegswaffen oder Explosivstoffe aufgefunden wurden, oder

3. a) rechtsextremistische Vereinigungen und Gruppierungen,

   b) Sachen, Bankverbindungen, Anschriften, Telekommunikationsanschlüsse, Telekommunikationsendgeräte, Internetseiten oder Adressen für elektronische Post,

   bei denen Tatsachen die Annahme rechtfertigen, dass sie im Zusammenhang mit einer Person nach Nummer 1 oder Nummer 2 stehen und durch sie Hinweise für die Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus gewonnen werden können,

und die Kenntnis der Daten für die Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus erforderlich ist. [2]Satz 1 gilt nur für Daten, die die beteiligten Behörden nach den für sie geltenden Rechtsvorschriften automatisiert verarbeiten dürfen.

§ 6 RED-G in der Fassung vom 18. Dezember 2014 (BGBl I S. 2318)
– Weitere Verwendung der Daten

(1) [1]Die abfragende Behörde darf die Daten, auf die sie Zugriff erhalten hat, zur Prüfung, ob der Treffer der gesuchten Person oder der

gesuchten Angabe nach § 2 Satz 1 Nummer 3 zuzuordnen ist, für ein Ersuchen um Übermittlung von Erkenntnissen zur Wahrnehmung ihrer jeweiligen Aufgabe zur Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus und zu den Zwecken nach § 7 nutzen. [2]Eine Nutzung zu einem anderen Zweck als zur Wahrnehmung ihrer jeweiligen Aufgabe zur Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus ist nur zulässig, soweit

1. dies zur Verfolgung einer besonders schweren Straftat oder zur Abwehr einer Gefahr für Leib, Leben, Gesundheit oder Freiheit einer Person erforderlich ist und

2. die Behörde, die die Daten eingegeben hat, der Verwendung zustimmt.

(2) - (3) […]

(4) [1]Soweit das Bundeskriminalamt, die Landeskriminalämter oder weitere beteiligte Polizeivollzugsbehörden nach § 1 Absatz 2 auf Ersuchen oder im Auftrag der das strafrechtliche Ermittlungsverfahren führenden Staatsanwaltschaft die Datei nach § 1 nutzen, übermitteln sie dieser die Daten, auf die sie Zugriff erhalten haben, für die Zwecke der Strafverfolgung. [2]Sie darf die Daten für Ersuchen nach Absatz 1 Satz 1 verwenden. [3]§ 487 Absatz 3 der Strafprozessordnung gilt entsprechend.

§ 8 RED-G in der Fassung vom 20. August 2012 (BGBl I S. 1798) – Übermittlung von Erkenntnissen

Die Übermittlung von Erkenntnissen aufgrund eines Ersuchens nach § 6 Absatz 1 Satz 1 oder von erweitert genutzten Daten nach § 7 zwischen den beteiligten Behörden richtet sich nach den jeweils geltenden Übermittlungsvorschriften.

II.

Der Beschwerdeführer wurde im Prozess um den sogenannten „Nationalsozialistischen Untergrund“ „NSU“ im Jahr 2018 wegen Beihilfe zu neun Fällen des Mordes zu einer Jugendstrafe von drei Jahren verurteilt. Bereits im Jahre 2012 wurde er aus der Untersuchungshaft entlassen, nachdem zur Überzeugung der Behörden feststand, dass er sich glaubhaft von der rechtsextremistischen Szene distanziert habe. Der Beschwerdeführer befindet sich derzeit im Zeugenschutzprogramm des Bundeskriminalamts. Mit seiner Verfassungsbeschwerde rügt er eine Verletzung des Grundrechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG. 17

1. Zur Zulässigkeit seiner Verfassungsbeschwerde trägt der Beschwerdeführer vor, er sei durch die angegriffenen Vorschriften unmittelbar, selbst und gegenwärtig betroffen. 18

a) Er könne sich ausnahmsweise unmittelbar gegen die grundsätzlich vollziehungsbedürftigen Regelungen wenden, weil er mangels Kenntnis der Vollzugsmaßnahmen den Rechtsweg nicht beschreiten könne. Über Datenübermittlungen nach den angegriffenen Vorschriften würden betroffene Personen nicht unterrichtet. Auch wenn sie nachträglich Kenntnis erlangten, sei eine Beeinträchtigung persönlicher Belange nicht rückgängig zu machen. In seinem Falle sei zu unterstellen, dass inländische Geheimdienste jedenfalls mit Bekanntwerden der Aktivitäten des „Nationalsozialistischen Untergrunds“ eine Vielzahl von Informationen über ihn übermittelt hätten. Es bestehe auch aktuell jederzeit die Möglichkeit, dass solche Daten an die in den angegriffenen Vorschriften genannten Stellen übermittelt würden. 19

b) Er sei selbst und gegenwärtig betroffen. Es sei zu unterstellen, dass die rechtsextremistische Szene Gegenstand von vielfältigen geheimdienstlichen Datenerhebungen gewesen sei. Der Beschwerdeführer habe sich in dieser Szene engagiert. Vor allem aber folge aus dem sogenannten NSU-Verfahren die hochgradige Wahrscheinlichkeit einer Übermittlung und Speicherung personenbezogener Daten aufgrund der angegriffenen Vorschriften. 20

c) Die Verfassungsbeschwerde sei fristgerecht erhoben. Zwar seien die angegriffenen Regelungen des Bundesverfassungsschutzgesetzes bereits am 30. Dezember 1990 in Kraft getreten. Das Rechtsextremismus-Datei-Gesetz vom 20. August 2012 habe aber die angegriffenen Vorschriften inhaltlich verändert und diesbezüglich die Jahresfrist des § 93 Abs. 3 BVerfGG neu in Gang gesetzt. Hier seien die Erwägungen des Bundesverfassungsgerichts im ersten Urteil zur Antiterrordatei (vgl. BVerfGE 133, 277 <311 ff. Rn. 82 ff.>) zu übertragen. 21

d) Zudem erfülle der Beschwerdeführer die gesetzlichen Voraussetzungen für eine Speicherung in der Rechtsextremismus-Datei. Es komme nicht darauf an, ob er sich um eine entsprechende Auskunft bereits bemüht und gegebenenfalls den Rechtsweg beschritten habe. Diese Rechtsschutzmöglichkeit sei schon deswegen nicht effektiv oder nachhaltig, weil selbst eine Mitteilung, nicht in die Rechtsextremismus-Datei aufgenommen zu sein, bereits am folgenden Tage überholt sein könne. 22

2. Die Verfassungsbeschwerde sei auch begründet. Die Vorschriften griffen ohne verfassungsrechtliche Rechtfertigung in das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) ein. Sie verstießen gegen den Verhältnismäßigkeitsgrundsatz und teilweise auch gegen das Gebot der Bestimmtheit und Normenklarheit. 23

a) Eine Zweckumwandlung in Gestalt einer Datenübermittlung von Geheimdiensten an mit operativen Aufgaben betraute Behörden sei von erheblicher Eingriffsintensität, weshalb gesteigerte verfassungsrechtliche Anforderungen gelten würden. Das Bundesverfassungsschutzgesetz enthalte keine Bestimmungen zum Kernbereichsschutz. Auch unterliege das Bundesamt für Verfassungsschutz keiner Kontrolle, die etwa mit derjenigen der Polizei in Strafverfahren vergleichbar sei. 24

b) Die Vorschrift des § 19 Abs. 1 Satz 1 BVerfSchG a.F. erlaube Datenübermittlungen an zu viele Empfänger („alle inländischen öffentlichen Stellen“) für einen zu weit gefassten Übermittlungszweck („sonst für Zwecke der öffentlichen Sicherheit“). Damit verstoße sie gegen das Übermaßverbot und gegen das Bestimmtheitsgebot. 25

c) Ebenso sei die Übermittlungsverpflichtung des § 20 Abs. 1 Satz 1 BVerfSchG nicht zu rechtfertigen. Sie ermögliche Durchbrechungen des informationellen Trennungsprinzips und verletze angesichts der Weite der anlassgebenden Delikte den Grundsatz der Verhältnismäßigkeit. Gegen die Anforderungen des Rechtsgüterschutzes werde schon dadurch verstoßen, dass die Vorschrift auch Staatsschutzdelikte aus dem Bereich der einfachen oder allenfalls mittleren Kriminalität einbeziehe. Die offene Formulierung der „sonstigen Straftaten“ sei zu unbestimmt. Ferner lege die Norm die erforderlichen Übermittlungsschwellen nicht hinreichend bestimmt und normenklar fest. Der Grundsatz der Verhältnismäßigkeit sei insbesondere dadurch verletzt, dass die Übermittlung keine gesicherte Tatsachenbasis als Übermittlungsanlass voraussetze. So könne bereits eine vage Prognose für einen extremistischen, sicherheitsgefährdenden oder geheimdienstlichen Hintergrund einer Straftat die Übermittlungspflicht auslösen. Schließlich fehle es an einer ausdrücklichen Verankerung des Kriteriums der hypothetischen Datenneuerhebung. 26

d) Aus denselben Gründen seien die in § 21 Abs. 1 Satz 1 in Verbindung mit § 20 Abs. 1 Satz 1 und 2 BVerfSchG geregelten Übermittlungsbefugnisse der 27

Landesverfassungsschutzbehörden verfassungsrechtlich nicht zu rechtfertigen.

e) Die in § 23 BVerfSchG vorgesehenen Übermittlungsverbote könnten die Verhältnismäßigkeit nicht sichern. Denn letztlich entscheide der jeweilige Geheimdienst selbst über das Vorliegen von Übermittlungsverboten, ohne dass eine externe Kontrolle stattfinde. Die Regelung biete auch keinen Schutz in Fällen, in denen die Unzulässigkeit der Übermittlung bei deren Vornahme noch nicht erkennbar gewesen sei. 28

3. Mit Schriftsatz vom 9. Januar 2021 führte der Beschwerdeführer zur geänderten Rechtslage aus, dass der ursprünglich angegriffene § 19 Abs. 1 Satz 1 BVerfSchG a.F. geändert und sein Anwendungsbereich maßgeblich eingeschränkt worden sei. Rückblickend sei dieser jedoch bereits deshalb mit dem Verhältnismäßigkeitsgrundsatz unvereinbar gewesen, weil der Gesetzgeber das Prinzip der hypothetischen Datenneuerhebung fehlerhaft umgesetzt und nicht ausdrücklich verankert habe. Die neue Fassung teile die Verfassungswidrigkeit der Altfassung, da die Bedenken an der fehlenden Bestimmtheit, Normenklarheit und Verhältnismäßigkeit nicht ausgeräumt seien. Insbesondere der in Bezug genommene § 8 Abs. 2 BVerfSchG sei nicht hinreichend bestimmt und umfasse eine Vielzahl unterschiedlich intensiver Eingriffsmaßnahmen. Zudem gebiete der Grundsatz der hypothetischen Datenneuerhebung, Informationen, die durch eine Infiltration krimineller oder terroristischer Vereinigungen gewonnen worden seien, grundsätzlich von einer Weiterleitung an Polizei- oder Strafverfolgungsbehörden auszunehmen. Diese Behörden hätten die Daten nach eigenen Erhebungsbefugnissen selbst nie rechtmäßig erlangen können. 29

III.

Zur Verfassungsbeschwerde haben die Bundesregierung, der Generalbundesanwalt beim Bundesgerichtshof, die Bayerische Staatsregierung, die jeweils amtierenden Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, der Bayerische Landesbeauftragte für den Datenschutz, der Berliner Beauftragte für Datenschutz und Informationsfreiheit, die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen, das Bundesverwaltungsgericht und die Humanistische Union e.V. Stellung genommen. 30

Der Deutsche Bundestag, der Bundesrat, die Landesregierungen von Hessen, Niedersachsen, Mecklenburg-Vorpommern und Thüringen, der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg, der Lan- 31

desbeauftragte für den Datenschutz Sachsen-Anhalt und der Landesdatenschutzbeauftragte des Landes Schleswig-Holstein, der Bundesgerichtshof, das Deutsche Institut für Menschenrechte e.V. sowie die Deutsche Vereinigung für Datenschutz e.V. haben auf eine eigene Stellungnahme verzichtet.

1. Die Bundesregierung betont die außerordentliche Bedeutung des Informationsaustausches zwischen den Verfassungsschutzbehörden und den Sicherheits- und Strafverfolgungsbehörden von Bund und Ländern. Sie hält die Verfassungsbeschwerde für unzulässig, jedenfalls aber unbegründet. 32

a) Es bestünden erhebliche Zweifel an der Zulässigkeit. Die Verfassungsbeschwerde sei verfristet. Das Rechtsextremismus-Datei-Gesetz habe die angegriffenen Vorschriften nicht inhaltlich verändert, weil das materielle Gewicht der durch die sie ermöglichten Grundrechtseingriffe nicht gesteigert worden sei. Eine größere praktische Wirksamkeit oder Anwendungshäufigkeit sei hierfür unerheblich. Die Ausführungen im ersten Urteil zur Antiterrordatei zum geänderten materiellen Gewicht der Übermittlungsvorschriften ließen sich nicht auf Erwägungen des Fristlaufs übertragen, sondern hätten allein im Kontext der materiellen Prüfung des Antiterrordateigesetzes gestanden. Die Frist des § 93 Abs. 3 BVerfGG sei auch nicht dadurch neu in Gang gesetzt worden, dass an die unveränderten Übermittlungsvorschriften Folgeeingriffe anknüpften, deren Anwendungsbereich erweitert worden sei. Denn die Verwendung der übermittelten Daten durch die Empfänger bestimme sich unverändert nach dem jeweiligen Fachrecht. 33

Selbst wenn man unterstelle, die angegriffenen Vorschriften seien durch das Rechtsextremismus-Datei-Gesetz fristauslösend geändert worden, führe dies nicht zur Zulässigkeit der Verfassungsbeschwerde. Eine erst nach Ablauf der Beschwerdefrist lediglich intensivierte Beschwer setze die Frist nicht neu in Gang, wenn nach der Begründung der Verfassungsbeschwerde schon die anfänglich geringere Beschwer verfassungswidrig gewesen sein solle. Hier hätten die Argumente der Beschwerdeschrift zur Verfassungswidrigkeit der angegriffenen Normen losgelöst vom Rechtsextremismus-Datei-Gesetz schon vor dessen Inkrafttreten vorgebracht werden können. 34

Im Übrigen könne sich eine fristauslösende zusätzliche Beschwer durch die angegriffenen Vorschriften allenfalls aus einem individuellen Zusatzrisiko polizeilicher Erkenntnisanfragen bei den Verfassungsschutzbehörden und hiervon veranlasster Übermittlungen ergeben. Entgegen der Unterstellung des Beschwerdefüh- 35

rers seien in der Rechtsextremismus-Datei keine auf ihn bezogenen Daten durch das Bundesamt für Verfassungsschutz oder die Landesverfassungsschutzbehörden gespeichert worden, da er bereits vor Einrichtung der Rechtsextremismus-Datei aus der rechtsextremistischen Szene ausgestiegen sei. Dass der Datei im konkreten Fall eine Anbahnungswirkung für eine Übermittlung durch das Bundesamt für Verfassungsschutz zugekommen sei, liege fern.

Höchst hilfsweise sei jedenfalls der Prüfungsumfang in zweifacher Hinsicht begrenzt: Er könne sich nur auf den Zeitraum seit Inkrafttreten des Rechtsextremismus-Datei-Gesetzes erstrecken und gegenständlich nur auf das Zusammenspiel der angegriffenen Normenkomplexe. 36

Der Beschwerdeführer sei ferner nicht unmittelbar von den angegriffenen Übermittlungsvorschriften betroffen. Zwar gebe es hier keine Benachrichtigungspflicht. Dem Beschwerdeführer sei jedoch bewusst gewesen, dass das Bundesamt für Verfassungsschutz und das Thüringer Landesamt für Verfassungsschutz Informationen über ihn erhoben und gespeichert hätten. Mit dieser Kenntnis hätte er fachgerichtlichen Rechtsschutz gegen die einzelnen Vollzugsakte erlangen können und müssen, wobei eine Überprüfung der Verfassungsmäßigkeit der jeweiligen Übermittlungsnormen inzident erfolgt wäre. Es komme daher nicht darauf an, ob und inwieweit er auf Antrag Auskunft erhalten und Rechtsschutz erlangen könne. 37

b) Jedenfalls sei die Verfassungsbeschwerde unbegründet. Die angegriffenen Übermittlungsvorschriften seien verhältnismäßig, hinreichend bestimmt und normenklar und somit mit dem Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) vereinbar. Das informationelle Trennungsprinzip fordere nicht, dass Nachrichtendienste ihre Erkenntnisse den für die Umsetzung von Maßnahmen zuständigen Stellen vorenthalten müssten. Als Institution zum Schutz der freiheitlichen demokratischen Grundordnung und des Bestandes und der Sicherheit des Bundes und der Länder müsse der Verfassungsschutz grundsätzlich befugt sein, Informationen an die zuständigen Stellen weiterzugeben. Insoweit sei seine Aufgabenwahrnehmung von vornherein auf die Informationsdienstleistung an die operativ tätigen Stellen gerichtet, ohne dass es darauf ankomme, ob die empfangende Stelle die übermittelten Informationen – hypothetisch – auch selbst hätte erheben können. 38

Der Gesetzgeber normiere verschiedentlich spezielle Übermittlungsregelungen und -voraussetzungen für besonders eingriffsintensiv erhobene Daten, neben denen ein Rückgriff auf die angegriffenen Übermittlungsvorschriften ausscheide. Ferner stelle die Erhebung personenbezogener Daten mit nachrichtendienstlichen Mitteln und deren Übermittlung nicht die Regel, sondern die Ausnahme dar. Schließlich beschränke die fachrechtliche Verhältnismäßigkeitsschranke des § 8 Abs. 5 BVerfSchG und deren übermittlungsbezogene Konkretisierung unter spezieller Hervorhebung der Art der Informationen und ihrer Erhebung (§ 23 Nr. 1 BVerfSchG) die Übermittlungsbefugnisse und garantiere die Verhältnismäßigkeit im Einzelfall. Bei besonders sensiblen oder mittels nachrichtendienstlicher Mittel gewonnenen Daten sei eine Übermittlung in der Regel unverhältnismäßig und damit unzulässig, wenn lediglich die Bekämpfung geringfügiger Gefahren in Rede stehe. Entgegen der Befürchtungen des Beschwerdeführers fehle es daher auch nicht am Kernbereichsschutz. Dieser sei durch die jeweiligen speziellen Eingriffsbefugnisse sowie § 8 Abs. 5 BVerfSchG sichergestellt. Im Übrigen sei eine Übermittlung von Kernbereichsdaten einem Übermittlungsverbot nach § 23 Nr. 1 BVerfSchG unterworfen. Die Beachtung der Übermittlungsvoraussetzungen werde durch eine Prüfungspflicht des übermittelnden Bundesamtes für Verfassungsschutz und eine eigenverantwortliche Prüfungspflicht der empfangenden Stelle doppelt abgesichert. 39

aa) Vor diesem Hintergrund stelle § 19 Abs. 1 Satz 1 BVerfSchG a.F. in allen Übermittlungsvarianten hinreichend normenklar und bestimmt sicher, dass personenbezogene Daten nur übermittelt würden, wenn dies zur Verfolgung verfassungsrechtlich legitimer Zwecke notwendig und die Verhältnismäßigkeit auch im Einzelfall gewahrt sei. Insbesondere sei § 19 Abs. 1 Satz 1 Variante 3 BVerfSchG a.F. weder im Hinblick auf den Begriff der „inländischen öffentlichen Stelle“ noch auf den der Übermittlung für „Zwecke der öffentlichen Sicherheit“ zu unbestimmt. Zudem wahre die Vorschrift die im ersten Urteil zum Antiterrordateigesetz formulierten Anforderungen an den Rechtsgüterschutz und die Übermittlungsschwellen bei Datenübermittlungen von Nachrichtendiensten an Polizeibehörden. Jedenfalls werde diesen durch Auslegung sowie bei der Rechtsanwendung im Einzelfall ausreichend Rechnung getragen. 40

bb) § 20 Abs. 1 Satz 1 BVerfSchG sei ebenfalls hinreichend bestimmt. Die Vorschrift unterliege jedenfalls keinen strengeren Bestimmtheitsanforderungen als die in Bezug genommenen Strafnormen selbst. Die Staatsschutzdelikte seien in § 20 Abs. 1 Satz 2 BVerfSchG definiert. Neben den Katalogstraftaten erfasse die 41

Norm durch den Auffangtatbestand der „sonstigen Straftaten“ alle nicht in §§ 74a und 120 GVG aufgeführten Straftaten, bei denen die weiteren in § 20 Abs. 1 Satz 2 BVerfSchG genannten Merkmale erfüllt seien. Die Tatbestandsmerkmale des § 20 Abs. 1 Satz 2 BVerfSchG seien auslegungsfähig und in diesem Sinne hinreichend bestimmt. Der Gesetzgeber sei nicht verpflichtet, sämtliche in Betracht kommenden Straftatbestände einzeln aufzuzählen.

Die Übermittlungsvorschrift des § 20 Abs. 1 Satz 1 und 2 BVerfSchG sei nicht unverhältnismäßig. Sie ermögliche insbesondere keinen freien Austausch der Datenbestände des Bundesamtes für Verfassungsschutz und der Staatsanwaltschaften und Polizeien. Ferner bestehe ein herausragendes öffentliches Interesse an der Verfolgung oder Verhinderung der genannten Staatsschutzdelikte. Trotz des teilweise geringeren Strafrahmens einzelner in §§ 74a und 120 GVG genannter Straftaten sowie verschiedener sonstiger Straftaten handele es sich nicht um Bagatellkriminalität. Vielmehr schützten die betreffenden Delikte hochrangige Verfassungs- und Gemeinwohlgüter und könnten somit die Datenübermittlung rechtfertigen. § 20 Abs. 1 Satz 1 und 2 BVerfSchG sehe hinreichende Übermittlungsschwellen vor und erlaube diese nicht allein aufgrund vager Prognosen. Das Abstellen auf tatsächliche Anhaltspunkte als Übermittlungsanlass genüge verfassungsrechtlichen Anforderungen. 42

cc) Da der Beschwerdeführer keine eigenständigen Gründe für die Verfassungswidrigkeit des § 21 Abs. 1 Satz 1 BVerfSchG geltend mache, sei auch dieser verfassungsrechtlich nicht zu beanstanden. 43

2. Der Generalbundesanwalt beim Bundesgerichtshof teilt weitgehend die Ansicht der Bundesregierung, die Verfassungsbeschwerde sei unzulässig; jedenfalls sei sie unbegründet. 44

a) Die Jahresfrist sei allenfalls gewahrt, soweit der Beschwerdeführer belastende Wirkungen aus dem Zusammenspiel der Rechtsextremismus-Datei mit den angegriffenen Übermittlungsregelungen des Bundesverfassungsschutzgesetzes und damit insbesondere die erhöhte Wahrscheinlichkeit von Übermittlungen rüge. Eine neue Beschwer könne bezogen auf die nachfolgenden Datenübermittlungen allein aus den praktischen Wirkungen der vorherigen Speicherung von Daten in der Verbunddatei resultieren. Die wesentlichen Belastungen ergäben sich damit aber letztlich unmittelbar aus dem Rechtsextremismus-Datei-Gesetz, das der Beschwerdeführer nicht angegriffen habe. 45

Die Verfassungsbeschwerde sei jedenfalls unzulässig, weil der Beschwerdeführer sich für die Darlegung seiner Betroffenheit auf die erste Entscheidung zur Antiterrordatei stütze, dabei aber nicht gegen die Schaffung der Verbunddatei selbst vorgehe. Zweifel an seiner Betroffenheit resultierten daraus, dass zwischen der Abfrage von Grunddaten in der Rechtsextremismus-Datei zur Vorbereitung eines Übermittlungsersuchens und der späteren, auf einer eigenständigen Prüfung beruhenden tatsächlichen Datenübermittlung zu trennen sei. Der Beschwerdeführer hätte sich unmittelbar gegen das Rechtsextremismus-Datei-Gesetz wenden und insbesondere die Speicherung seiner Daten beanstanden können. 46

Im Übrigen sei angesichts seines schon vor Jahren erfolgten Ausstiegs aus dem rechtsextremistischen Umfeld eine tatsächliche Übermittlung von ihn betreffenden Daten nicht mehr wahrscheinlich. Etwaige Übermittlungsvorgänge – im Zusammenhang mit der Einleitung und Durchführung des Strafverfahrens im NSU-Prozess – lägen in der Vergangenheit. 47

b) Die Verfassungsbeschwerde sei darüber hinaus unbegründet. Die Übermittlungsbefugnisse seien jedenfalls im Kontext des Rechtsextremismus-Datei-Gesetzes verhältnismäßig. 48

aa) Am legitimen Ziel der Aufklärung und Bekämpfung des gewaltbezogenen Rechtsextremismus bestehe ein herausragendes öffentliches Interesse. Dieses Ziel würde ohne effektive Zusammenarbeit der Sicherheitsbehörden verfehlt, wie die im Zuge der Aufarbeitung der vom NSU über Jahre hinweg verübten Mordserie zu Tage getretenen Versäumnisse unterstrichen hätten. Ein wirksames Sicherheitskonzept müsse die Ergebnisse der Ermittlungen der Nachrichtendienste zwingend berücksichtigen, da gefahrenabwehrrechtliche, strafprozessuale und nachrichtendienstliche Probleme in ihrem Gesamtzusammenhang gesehen werden müssten. Der durch die Übermittlung begründete Grundrechtseingriff sei auch im Übrigen angemessen. 49

bb) Danach begegne § 19 Abs. 1 Satz 1 BVerfSchG a.F. keinen verfassungsrechtlichen Bedenken. Die am erleichterten Datenaustausch der Rechtsextremismus-Datei beteiligten Behörden seien abschließend benannt; der erforderliche Bezug zum gewaltbezogenen Rechtsextremismus grenze den betroffenen Personenkreis ein. Effektive Beschränkungen folgten insbesondere aus dem Zusammenspiel des Erfordernisses einer rechtsextremistischen Motivation mit der Vo- 50

raussetzung des Gewaltbezugs, die eine objektivierbare Förderung von Gewaltanwendung verlange.

Die Übermittlungsvorschriften selbst statuierten ebenfalls hinreichend konkrete und qualifizierte Eingriffsschwellen. Ob der Begriff der „Erforderlichkeit“ als solcher ausreichend bestimmt sei, könne offenbleiben, da insoweit wiederum auf die Voraussetzungen für eine vorherige Datenspeicherung zu verweisen sei. Hierfür seien die tatsachengestützte Annahme eines rechtsextremistisch motivierten Gewaltbezugs (vgl. § 2 RED-G) und die Erforderlichkeit zur Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus (vgl. § 6 Abs. 1 RED-G) vorausgesetzt. 51

Dem informationellen Trennungsgebot werde ferner durch die weitere Behandlung der übermittelten Informationen Rechnung getragen. Vor einer Übernahme nachrichtendienstlicher Daten in das Strafverfahren sei zu prüfen, ob Anhaltspunkte vorlägen, die der Rechtmäßigkeit der Datenerhebung im Ausgangsverfahren entgegenstehen könnten. Der Generalbundesanwalt achte insbesondere darauf, dass die Nachrichtendienste sich mit der Datenübermittlung an Polizei und Strafverfolgungsbehörden keinen faktischen „Vollzugsarm“ schüfen. Dabei werde für die strafprozessuale Verwendung von Daten darauf abgestellt, ob die Daten durch eine vergleichbare strafprozessuale Maßnahme in vergleichbarer Weise rechtmäßig hätten erlangt werden können. Eine Umgehung grundrechtsbezogener Beschränkungen des Einsatzes bestimmter Erhebungsmethoden werde somit verhindert. 52

cc) Aus denselben Gründen genügten auch die Übermittlungsvorschriften der § 20 Abs. 1 Satz 1 und 2 sowie § 21 Abs. 1 Satz 1 in Verbindung mit § 20 Abs. 1 Satz 1 und 2 BVerfSchG den aus dem informationellen Trennungsgebot folgenden Anforderungen. Soweit der Beschwerdeführer die Einbeziehung von Staatsschutzdelikten aus dem Bereich der einfachen und mittleren Kriminalität beanstande, sei darauf hinzuweisen, dass derartige Delikte in der Praxis als Anlass von Übermittlungen nachrichtendienstlicher Erkenntnisse nach § 20 Abs. 1 Satz 1 und 2 BVerfSchG keine Rolle spielten und die Bezugnahme des Rechtsextremismus-Datei-Gesetzes auf einen rechtsextremistisch motivierten Gewaltbezug einschränkend wirke. Die Übermittlungsschwelle tatsächlicher Anhaltspunkte entspreche den Voraussetzungen für die Einleitung eines Strafverfahrens, wofür entgegen der Ansicht des Beschwerdeführers bloße Spekulationen oder Vermutungen nicht genügten. 53

3. Nach Auffassung der Bayerischen Staatsregierung ist bereits im Ausgangspunkt nicht frei von Zweifeln, ob durch eine Übermittlung erneut in das Grundrecht eingegriffen wird, das durch die Datenerhebung beeinträchtigt worden ist. 54

Jedenfalls seien die angegriffenen Übermittlungsvorschriften verhältnismäßig. Die Informationsweitergabe sei die „funktionelle Kehrseite“ des organisatorischen und befugnisrechtlichen Trennungsprinzips. Nachrichtendienstliche Gefahrerforschung und polizeiliche Gefahrenintervention bildeten arbeitsteilig ineinandergreifende Funktionselemente eines einheitlichen Prozesses der Gefahrenabwehr. Hinsichtlich des Grundsatzes der hypothetischen Datenneuerhebung gälten für Nachrichtendienste Besonderheiten. Diese erhöben Daten nicht zu eigenen operativen Zwecken, sondern mit dem Ziel, sie nach Aufbereitung weiterzugeben. Das Grundgesetz ordne den Verfassungsschutz in Art. 73 Abs. 1 Nr. 10 GG zwischen der Kriminalpolizei und der internationalen Verbrechensbekämpfung ein und bringe eine „verfassungsrechtlich begründete Funktionsidentität der Sicherheitsbehörden“ zum Ausdruck. Durch ein strenges informationelles Trennungsprinzip würden die Verfassungsschutzbehörden entgegen der grundgesetzlichen Konzeption ihre Funktion als Frühwarnsystem weitgehend einbüßen. In jedem Fall müssten sich die Anforderungen des informationellen Trennungsprinzips nach den konkreten Belastungswirkungen richten. Bei der Übermittlung an Polizeien oder andere Sicherheitsbehörden sei zu berücksichtigen, dass die Ausübung exekutiver Befugnisse an eigene Voraussetzungen geknüpft sei. Überdies könne die Belastungswirkung einer nachrichtendienstlichen Übermittlung nicht mit derjenigen der vorangegangenen Erhebung gleichgesetzt werden, da in aller Regel keine Rohdaten übermittelt würden, sondern in ihrer Wirkung für den Betroffenen beschränkte Auswertungsprodukte. 55

§ 20 Abs. 1 Satz 1 und 2 sowie § 21 Abs. 1 BVerfSchG bildeten den essenziellen Kern der informationellen Dienstleistung der Verfassungsschutzbehörden und seien in der bisherigen Praxis nicht ausufernd, sondern zu restriktiv gehandhabt worden. 56

4. Die im Verfahren beteiligten Bundesbeauftragten für den Datenschutz und die Informationsfreiheit äußerten verfassungsrechtliche Bedenken, da die Tatbestandsvoraussetzungen der angegriffenen Vorschriften in Ansehung der Intensität des Grundrechtseingriffs zu unbestimmt und weit gefasst seien. Verletzt seien sowohl das Gebot der Normenklarheit als auch der Verhältnismäßigkeitsgrundsatz. 57

§ 20 Abs. 1 Satz 1 und 2 BVerfSchG enthalte eine zu extensive Definition der Staatsschutzdelikte. Insbesondere die Erstreckung auf sonstige, gegen die in den Art. 73 Abs. 1 Nr. 10 GG genannten Schutzgüter gerichteten Straftaten erfasse mitunter niederschwellige Sachverhalte. So genüge bereits eine „Gefährdung“ der „auswärtigen Belange“ durch eine Vorbereitungshandlung, die auf eine zukünftige Gewaltanwendung gerichtet sei. Die Auslegung der weit gefassten Rechtsbegriffe werde den Nachrichtendiensten weitgehend selbst überlassen und finde wegen der Heimlichkeit der Übermittlungen nicht mit Kenntnis der Betroffenen im Wechselspiel von Verwaltungsakt und gerichtlicher Kontrolle statt. 58

Die ermöglichten Grundrechtseingriffe seien mitunter schwerwiegend, so dass gravierende Zweifel an der Verhältnismäßigkeit der Normen bestünden. Insgesamt werde eine Übermittlung nicht auf den Schutz besonders gewichtiger Rechtsgüter beschränkt und an keine ausreichenden tatbestandlichen Erkenntnisschwellen gebunden. Das Kriterium der Erforderlichkeit genüge nicht; es bestehe das Risiko einer Fehlprognose, so dass selbst unbescholtene Bürgerinnen und Bürger in den Fokus der Nachrichtendienste geraten könnten. 59

Für die Eingriffsintensität der Datenübermittlungen sei maßgeblich, dass diese in aller Regel ohne Kenntnis oder nachträgliche Benachrichtigung der Betroffenen erfolgten. Die in derartigen Fällen zum Schutz der subjektiven Rechte der Betroffenen vorgegebene Kompensationsfunktion der Datenschutzaufsicht sei in der Praxis nicht adäquat zu gewährleisten. Es fehle an einer notwendigen Pflicht zur Kennzeichnung und Dokumentation hinsichtlich der Übermittlung von Erkenntnissen, die mit nachrichtendienstlichen Mitteln erhoben seien. Für die Betroffenen bestehe oftmals auch im Nachhinein keine Möglichkeit, effektiven Rechtsschutz gegen heimliche Maßnahmen zu erlangen, weil die Auskunft nach dem Bundesverfassungsschutzgesetz nur unter besonderen Voraussetzungen zu erlangen sei und weitgehende Ausnahmetatbestände vorsehe. Auch insoweit bestünden gravierende Zweifel an der Angemessenheit der angegriffenen Vorschriften. 60

Das Eingriffsgewicht der Datenübermittlung werde durch die im Gesetz restriktiv und relativ unbestimmt ausgestalteten Übermittlungsverbote der §§ 23 und 24 BVerfSchG nicht aufgefangen. Insbesondere enthielten auch behördeninterne Vorschriften keine ausreichenden Vorgaben und Hinweise zur Auslegung des § 23 BVerfSchG. 61

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ergänzt in der Stellungnahme vom 25. Mai 2021, dass durch die bisherigen Gesetzesreformen das informationelle Trennungsprinzip unzureichend umgesetzt worden sei. 62

5. Der Bayerische Landesbeauftragte für den Datenschutz folgt inhaltlich im Wesentlichen der Bewertung durch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, die entsprechend für § 21 Abs. 1 BVerfSchG gelte. 63

6. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit trägt insbesondere zur Anwendungspraxis der genannten Vorschriften vor, die teilweise nicht dem intendierten Regelungskonzept entspreche. 64

7. Die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen trägt vor, dass es vereinzelte Datenübermittlungen des Bundesamtes für Verfassungsschutz an die Bremer Landespolizei zu Strafverfolgungszwecken und zum Zweck der Gefahrenabwehr gegeben habe, während § 21 Abs. 1 Satz 1 BVerfSchG keine praktische Anwendung gefunden habe. 65

8. Der 6. Senat des Bundesverwaltungsgerichts teilt im Wesentlichen mit, dass der – damals noch zuständige – 1. Senat des Bundesverwaltungsgerichts im Jahr 1995 eine Nichtzulassungsbeschwerde gegen eine auf § 19 BVerfSchG gestützte Entscheidung verworfen habe (BVerwG, Beschluss vom 6. März 1995 - 1 B 226.94 -). Hier habe der Senat festgehalten, dass der Bundesverfassungsschutz zu einer sorgfältigen Prüfung der Tatbestandsvoraussetzungen verpflichtet sei und dem Datenempfänger gegebenenfalls nähere Informationen mitteilen müsse, um diesem die Einhaltung des Grundsatzes der Zweckbindung zu ermöglichen. Der mittlerweile zuständige 6. Senat sei mit den angegriffenen Vorschriften nicht befasst gewesen. 66

9. Die Humanistische Union hält die Verfassungsbeschwerde für zulässig, da das Rechtsextremismus-Datei-Gesetz die Voraussetzungen für die Eingabe und Verwendung der Daten nicht selbstständig regele, sondern auf die in den Fachgesetzen enthaltenen allgemeinen Übermittlungsregelungen verweise und die Beschwerdefrist neu in Lauf setze. 67

Die Verfassungsbeschwerde sei auch begründet. § 19 Abs. 1 Satz 1 BVerfSchG fasse den Kreis der informationszugangsberechtigten Behörden zu 68

weit; er setze zudem keine Mindestgefahrenschwellen und verletze den Zweckbindungsgrundsatz. Zudem umfasse die öffentliche Sicherheit praktisch sämtliche in der Rechtsordnung geschützten Rechtsgüter, weshalb mit der Übermittlung beliebige Zwecke bei beliebigen Behörden verfolgt werden dürften. § 19 Abs. 1 BVerfSchG unterlaufe damit zudem die grundgesetzliche Kompetenzordnung.

§ 20 Abs. 1 BVerfSchG sei zwar durch die Verweise auf die in den § 74a Abs. 1 und § 120 Abs. 1 und 2 GVG geregelten Straftatenkataloge hinreichend normenklar. Die Kataloge beschränkten sich jedoch nicht – wie verfassungsrechtlich geboten – auf besonders schwere Straftaten. Problematisch sei die Übermittlungspflicht mit Blick auf Straftaten, die Vorbereitungshandlungen pönalisierten, zumal die übermittelten Informationen durch den Beobachtungsauftrag der Nachrichtendienste noch weit vor jedem strafprozessualen Anfangsverdacht liegen könnten. Die Einbeziehung sonstiger Straftaten verstoße gegen das Bestimmtheitsgebot, weil sie die Datenübermittlung anlässlich von Delikten der allgemeinen Kriminalität ermögliche, soweit diese auch nur in einem weiteren Zusammenhang mit Staatsschutzdelikten stünden. 69

IV.

Auf einen Fragenkatalog des Bundesverfassungsgerichts zur praktischen Bedeutung und Anwendung der angegriffenen Vorschriften haben eine schriftliche Stellungnahme abgegeben: der Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages samt einer Stellungnahme des Parlamentarischen Kontrollgremiums, die Bundesregierung, der Generalbundesanwalt beim Bundesgerichtshof, die Staatsregierungen Bayern und Sachsen, die Landesregierungen von Brandenburg, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Sachsen-Anhalt, Schleswig-Holstein, Thüringen und die Senate von Berlin, der Freien Hansestadt Bremen sowie der Freien und Hansestadt Hamburg; weiter der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, der Bayerische Landesbeauftragte für den Datenschutz, die Berliner Beauftragte für Datenschutz und Informationsfreiheit, die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen, der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, der Hessische Beauftragte für Datenschutz und Informationsfreiheit, die Landesbeauftragte für den Datenschutz Niedersachsen, die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, die Landesbeauftragte für Datenschutz und Informa- 70

tionsfreiheit Saarland, der Landesbeauftragte für den Datenschutz Sachsen-Anhalt sowie die Landesbeauftragte für Datenschutz Schleswig-Holstein.

B.

Die Verfassungsbeschwerde ist teilweise zulässig. 71

I.

Allerdings sind weder § 19 Abs. 1 Satz 1 BVerfSchG in der Fassung vom 5. Januar 2007 noch § 19 Abs. 1 Satz 2 BVerfSchG in der Fassung vom 17. November 2015 zulässig zum Gegenstand der Verfassungsbeschwerde gemacht worden. Der Beschwerdeführer hat seine Verfassungsbeschwerde nach der Gesetzesänderung auch nicht fristgerecht auf die Neufassung der Vorschrift umgestellt. Seiner gegen die Altfassung gerichteten Verfassungsbeschwerde fehlt nach deren Außerkrafttreten das Rechtsschutzbedürfnis. 72

1. Soweit der Beschwerdeführer § 19 Abs. 1 Satz 1 BVerfSchG in der Fassung vom 5. Januar 2007 angegriffen hat, ist seine Verfassungsbeschwerde jedenfalls verfristet und daher unzulässig. 73

Durch das Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 17. November 2015 ist der damalige § 19 Abs. 1 Satz 1 BVerfSchG a.F. mit Wirkung zum 21. November 2015 erheblich umgestaltet worden und geht nunmehr in dem Regelungskonzept der Sätze 1 und 2 des § 19 Abs. 1 BVerfSchG n.F. auf. Nach der Neufassung unterscheiden sich die Anforderungen an die Übermittlung von mit nachrichtendienstlichen Mitteln nach § 8 Abs. 2 BVerfSchG erhobenen personenbezogenen Daten und Informationen in Abhängigkeit von den jeweiligen Übermittlungsempfängern deutlich. Dass sich der Wortlaut von § 19 Abs. 1 Satz 1 BVerfSchG a.F. weitgehend in § 19 Abs. 1 Satz 2 BVerfSchG n.F. wiederfindet, ist nicht maßgeblich, da sich der Anwendungsbereich der Norm erheblich verändert hat. In einem solchen Fall erstreckt sich die Verfassungsbeschwerde gegen die aufgehobene Vorschrift nicht automatisch auf die an ihre Stelle getretene Norm; dies gilt selbst dann, wenn die Neuregelung – anders als vorliegend – inhaltsgleich zu der Vorgängerregelung ist (vgl. BVerfGE 87, 181 <194>; 155, 119 <158 Rn. 66> – Bestandsdatenauskunft II). 74

Beschwerdeführende haben zwar die Möglichkeit, ihre bereits gegen die vorherige Gesetzesfassung erhobene Verfassungsbeschwerde auf die Neufassung umzustellen. Dann muss aber die Umstellung ihrerseits die Jahresfrist wahren 75

(vgl. BVerfGE 87, 181 <194>; 155, 119 <158 Rn. 67>; 158, 170 <183 Rn. 24> – IT-Sicherheitslücken). Somit hätte der Beschwerdeführer bis zum Ablauf des 20. November 2016 seine Verfassungsbeschwerde auf die neue Gesetzesfassung umstellen können. Von dieser Möglichkeit hat er fristgerecht keinen Gebrauch gemacht. Erst mit Schriftsatz vom 9. Januar 2021 – und damit weit nach Ablauf der Jahresfrist des § 93 Abs. 3 BVerfGG – ließ er sich zu der geänderten Rechtslage ein.

2. Der somit allein gegen § 19 Abs. 1 Satz 1 BVerfSchG in der Fassung vom 5. Januar 2007 gerichteten Verfassungsbeschwerde fehlt das Rechtsschutzinteresse, da dieser am 20. November 2015 außer Kraft getreten ist. Das Rechtsschutzinteresse entfällt, wenn die von dem angegriffenen Gesetz ausgehende Beschwer deshalb wegfällt, weil die Vorschriften durch Neuregelungen ersetzt worden sind (vgl. BVerfGE 87, 181 <194>; 100, 271 <281 f.>; 155, 119 <158 Rn. 68>). Gegen eine von der Nachfolgeregelung ausgehende neue Beschwer ist grundsätzlich mit einer neuen Verfassungsbeschwerde vorzugehen (vgl. BVerfGE 106, 210 <214>; dazu auch BVerfG, Beschluss der 3. Kammer des Ersten Senats vom 4. Juni 2014 - 1 BvR 1443/08 -, Rn. 2). 76

Ein ausnahmsweise fortbestehendes Rechtsschutzbedürfnis an einer Entscheidung des Bundesverfassungsgerichts über die Altfassung von § 19 Abs. 1 Satz 1 BVerfSchG hat der Beschwerdeführer weder dargelegt noch ist dies sonst ersichtlich. Insbesondere unterbleibt auf diese Weise nicht etwa die Klärung verfassungsrechtlicher Fragen von grundsätzlicher Bedeutung (vgl. BVerfGE 81, 138 <140>; 100, 271 <281 f.>; 155, 119 <158 f. Rn. 68>; stRspr). Denn die im Hinblick auf die Altregelung auftretenden Fragen der verfassungsrechtlichen Anforderungen an die Übermittlung von mit nachrichtendienstlichen Mitteln erhobenen personenbezogenen Daten und Informationen sind mittlerweile geklärt (vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 229 ff. – Bayerisches Verfassungsschutzgesetz). 77

II.

Soweit sich die Verfassungsbeschwerde gegen die § 20 Abs. 1 Satz 1 und 2, § 21 Abs. 1 Satz 1 in Verbindung mit § 20 Abs. 1 Satz 1 und 2 BVerfSchG richtet – jeweils in der Fassung vom 20. Dezember 1990 –, ist sie zulässig. 78

1. Die unverändert gebliebenen Vorschriften sind bei verständiger Auslegung allerdings nur teilweise als Beschwerdegegenstand anzusehen. Zwar nennt die 79

Beschwerdeschrift sie ohne weitere Einschränkung als Beschwerdegegenstand. Aus der Beschwerdebegründung ergibt sich jedoch, dass der Beschwerdeführer die jeweilige Übermittlungspflicht nur beanstandet, soweit sie sich auf personenbezogene Daten und Informationen bezieht, die unter Einsatz nachrichtendienstlicher Mittel im Sinne des § 8 Abs. 2 BVerfSchG erhoben wurden. Diese Methoden, Gegenstände und Instrumente umfassen eine Bandbreite von Mitteln zur heimlichen Informationsbeschaffung, die – ungeachtet ihres unterschiedlichen Eingriffsgewichts im Einzelnen – auch sehr schwerwiegende Grundrechtseingriffe ermöglichen. Darunter fallen etwa langfristig angelegte Ton- und Bildaufzeichnungen privater Gespräche und Situationen oder das Ausnutzen von Vertrauen durch Verdeckte Ermittler oder Vertrauenspersonen (vgl. BVerfGE 141, 220 <290 Rn. 160>). Für die Argumentation des Beschwerdeführers zu den hohen Anforderungen an die Übermittlung personenbezogener Daten durch die Verfassungsschutzbehörden ist durchgängig das Eingriffsgewicht der Ersterhebung maßgeblich, das er nur mit Blick auf die nachrichtendienstlichen Mittel darlegt. Nicht als Beschwerdegegenstand anzusehen sind bei verständiger Auslegung der Verfassungsbeschwerde deshalb die obigen Vorschriften, soweit sie die Übermittlung anderweitig erhobener Daten ermöglichen. Im Übrigen wäre eine entsprechende Rüge nicht substantiiert, da der Beschwerdeführer das besondere Eingriffsgewicht derartiger Datenübermittlungen nicht darlegt.

Die Übermittlungsbefugnisse nach § 20 Abs. 1 Satz 1 und 2 sowie § 21 Abs. 1 Satz 1 in Verbindung mit § 20 Abs. 1 Satz 1 und 2 BVerfSchG beanstandet der Beschwerdeführer ferner allein, soweit sie von § 8 RED-G in Bezug genommen werden. 80

2. Die so verstandene Verfassungsbeschwerde ist zulässig. Der Beschwerdeführer ist beschwerdebefugt. Das Subsidiaritätserfordernis ist ebenso gewahrt wie die Beschwerdefrist. Schließlich ist die Materie nicht vom Unionsrecht volldeterminiert und damit einer Entscheidung des Bundesverfassungsgerichts zugänglich. 81

a) Der Beschwerdeführer ist beschwerdebefugt (vgl. Art. 93 Abs. 1 Nr. 4a GG, § 90 Abs. 1 BVerfGG). 82

aa) Insbesondere hat er eine mögliche Verletzung des Grundrechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG durch die Übermittlung seiner Daten den Begründungsanforderungen nach § 23 Abs. 1 Satz 2, § 92 BVerfGG entsprechend dargelegt (vgl. BVerfGE 125, 39 <73>; 83

BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 93 f.). Er trägt vor, die angegriffenen Übermittlungsvorschriften seien unbestimmt, nicht normenklar und unverhältnismäßig ausgestaltet. Eine Grundrechtsverletzung erscheint danach möglich, weil die Übermittlung personenbezogener Daten, mit der eine Behörde die von ihr erhobenen Daten einer anderen Stelle zugänglich macht, einen eigenen Grundrechtseingriff begründet (vgl. BVerfGE 154, 152 <266 Rn. 212>; BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 230; stRspr).

bb) Der Beschwerdeführer hat dargetan, durch die angegriffenen Übermittlungsbefugnisse, soweit sie von § 8 RED-G in Bezug genommen werden, selbst, gegenwärtig und unmittelbar betroffen zu sein. Seine Verfassungsbeschwerde erfüllt die spezifischen Anforderungen, die für unmittelbar gegen Gesetze gerichtete Verfassungsbeschwerden gelten. 84

(a) Die angegriffenen Vorschriften betreffen den Beschwerdeführer unmittelbar. Zwar verpflichten diese nur zur Datenübermittlung und bedürfen daher eines konkreten Vollzugsakts. Von einer unmittelbaren Betroffenheit durch ein vollziehungsbedürftiges Gesetz ist jedoch auch dann auszugehen, wenn Beschwerdeführende den Rechtsweg nicht beschreiten können, weil sie keine Kenntnis von der Maßnahme erlangen oder wenn eine nachträgliche Bekanntgabe zwar vorgesehen ist, von ihr aber aufgrund weitreichender Ausnahmetatbestände auch langfristig abgesehen werden kann (vgl. BVerfGE 155, 119 <159 Rn. 73>). 85

So liegt es hier. Die Datenübermittlung nach den angegriffenen Vorschriften erfolgt regelmäßig ohne Kenntnis des Betroffenen. Eine spätere Kenntniserlangung ist nicht durch aktive Benachrichtigungspflichten sichergestellt. Auch eine Auskunft ist aufgrund der weitreichenden Ausnahmevorschrift des § 15 Abs. 2 BVerfSchG jedenfalls nicht zuverlässig gewährleistet. Insbesondere erstreckt sich der Auskunftsanspruch des § 15 Abs. 1 BVerfSchG nach dessen Abs. 3 ausdrücklich nicht darauf, an wen erhobene Daten übermittelt wurden. 86

(b) Der Beschwerdeführer ist durch die angegriffenen Regelungen auch selbst und gegenwärtig betroffen. Erfolgt die konkrete Beeinträchtigung erst durch die Vollziehung der angegriffenen Vorschriften und erlangen die Betroffenen – wie vorliegend – in der Regel keine Kenntnis von den Vollzugsakten, reicht es aus, wenn sie darlegen, mit einiger Wahrscheinlichkeit durch die auf den angegriffenen Rechtsnormen beruhenden Maßnahmen in eigenen Grundrechten berührt zu wer- 87

den (vgl. BVerfGE 155, 119 <160 Rn. 75>). Insoweit sind Darlegungen, durch die sich Beschwerdeführende selbst einer Straftat bezichtigen müssten, zum Beleg der Selbstbetroffenheit ebenso wenig erforderlich wie der Vortrag, für sicherheitsgefährdende oder nachrichtendienstlich relevante Aktivitäten verantwortlich zu sein (vgl. BVerfGE 130, 151 <176 f.>; stRspr). Obwohl der Beschwerdeführer bereits im Jahr 2001 aus der rechtsextremistischen Szene ausgestiegen ist, ist aufgrund seines Werdegangs und seiner vergangenen vielfältigen Verstrickung in der rechtsextremistischen Szene mit einiger Wahrscheinlichkeit zu erwarten, dass beim Bundesamt für Verfassungsschutz oder den Verfassungsschutzbehörden eines oder mehrerer Bundesländer personenbezogene Informationen über den Beschwerdeführer gespeichert sind. Besteht aber die begründete Annahme, dass auf ihn bezogene Daten erhoben und gesammelt werden könnten, ist auch eine Übermittlung jener Daten und daraus gewonnener Informationen hinreichend wahrscheinlich.

(c) Der Beschwerdeführer wendet sich vorliegend allerdings nur insoweit gegen die angegriffenen Übermittlungsvorschriften, als diese durch die Bezugnahme in § 8 RED-G einen neuen materiellen Gehalt bekommen haben. Dieser verweist für die Übermittlung von Erkenntnissen aufgrund eines Ersuchens nach § 6 Abs. 1 Satz 1 RED-G zwischen den beteiligten Behörden unter anderem auf die vorliegend angegriffenen Übermittlungsvorschriften. Grundvoraussetzung eines solchen übermittlungsanbahnenden Ersuchens ist eine Speicherung in der Rechtsextremismus-Datei durch die Verfassungsschutzbehörden. Aus dem Vortrag des Beschwerdeführers ergibt sich, dass er aber auch insoweit selbst, gegenwärtig und unmittelbar betroffen ist. 88

Obwohl § 2 RED-G lediglich die Speicherungsverpflichtung der Behörden regelt und es insoweit eines konkreten Vollzugsakts bedarf, fehlt es dem Beschwerdeführer nicht an einer unmittelbaren Betroffenheit. So legt er nachvollziehbar dar, er könne grundsätzlich weder von der Speicherung noch von der Verwendung seiner Daten verlässlich Kenntnis erhalten. Daran ändert nichts, dass er gemäß § 11 Abs. 3 RED-G auf Antrag die Möglichkeit hat, teilweise Auskunft über die Speicherung der Daten zu erlangen und anschließend gegen die Speicherung die Gerichte anzurufen. Denn die Auskunftspflicht unterliegt gemäß § 57 in Verbindung mit § 56 Abs. 2 des Bundesdatenschutzgesetzes zahlreichen Ausnahmen und ist überdies vom Einvernehmen der speichernden Behörde abhängig. Ferner kann er auf diesem Weg lediglich dagegen vorgehen, dass zu einem bestimmten Zeitpunkt Daten über ihn tatsächlich gespeichert sind, nicht aber dagegen, dass 89

eine solche Speicherung, ohne dass er hierauf Einfluss hat oder hiervon Kenntnis erlangt, jederzeit möglich ist. Eine aktive Informationspflicht des Staates, welche die spätere Kenntniserlangung des Betroffenen rechtlich sichert (vgl. BVerfGE 155, 119 <159 Rn. 73>), sieht das Rechtsextremismus-Datei-Gesetz nicht vor. Dementsprechend lässt auch die Einlassung der Bundesregierung, in der Rechtsextremismus-Datei seien zum Beschwerdeführer keine personenbezogenen Daten durch das Bundesamt für Verfassungsschutz oder die Landesverfassungsschutzbehörden gespeichert worden, seine unmittelbare Betroffenheit nicht entfallen.

Der Beschwerdeführer hat noch hinreichend dargelegt, durch eine Speicherung von auf ihn bezogenen, durch die Verfassungsschutzbehörden mutmaßlich erhobenen Daten mit einiger Wahrscheinlichkeit auch selbst betroffen zu sein. § 2 Satz 1 RED-G sieht grundsätzlich eine Pflicht zur Speicherung bereits erhobener Daten für bestimmte Personen vor. Nachdem der Beschwerdeführer im NSU-Prozess wegen Beihilfe zu neun Fällen des Mordes rechtskräftig verurteilt worden ist, gehört er grundsätzlich zum relevanten Personenkreis im Sinne des § 2 Satz 1 Nr. 1 Buchstabe b RED-G. Zwar ermöglicht die die Speicherpflichten allgemein begrenzende Klausel in § 2 Satz 1 RED-G, nach der die Kenntnis der Daten für die Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus erforderlich sein muss, Korrekturen, wenn im Einzelfall Zweifel an der Verhältnismäßigkeit der Speicherung bestehen (vgl. zur Antiterrordatei BVerfGE 133, 277 <339 f. Rn. 146>). Dennoch bedurfte es angesichts der Selbstbelastungsfreiheit und der begrenzten Darlegungsmöglichkeiten des Beschwerdeführers vorliegend keines weiteren diesbezüglichen Vortrags. Insbesondere drängt sich nicht auf, dass seine Situation einen atypischen Einzelfall darstellt, der die Speicherungspflicht entfallen lässt. Letztlich beurteilt die speichernde Behörde die Erforderlichkeit und die einzelnen Gründe dafür bleiben dem Beschwerdeführer regelmäßig verborgen. 90

b) Der Zulässigkeit der Verfassungsbeschwerde steht der Grundsatz der Subsidiarität nicht entgegen (vgl. zu den Maßstäben BVerfGE 143, 246 <321 f. Rn. 210>; 158, 170 <199 ff. Rn. 68 ff.>; stRspr). Der Beschwerdeführer musste vor Erhebung der Verfassungsbeschwerde keinen fachgerichtlichen Rechtsschutz gegen die angegriffenen Vorschriften suchen. Die ausschließlich gegen Gesetze gerichtete Verfassungsbeschwerde wirft im Kern allein spezifisch verfassungsrechtliche Fragen auf, die das Bundesverfassungsgericht zu beantworten hat, ohne dass von einer vorausgegangenen fachgerichtlichen Prüfung substantiell verbesserte Entscheidungsgrundlagen zu erwarten wären. Die verfassungsrechtliche Beurtei- 91

lung hängt nicht von der Klärung von Tatsachen oder der fachrechtlichen Auslegung der einzelnen Tatbestandsmerkmale der angegriffenen Befugnisse ab, sondern maßgeblich von deren hinreichender gesetzlicher Begrenzung und Bestimmtheit.

c) Die am 22. August 2013 erhobene Verfassungsbeschwerde wahrt die Beschwerdefrist des § 93 Abs. 3 BVerfGG. Zwar sind sowohl der angegriffene § 20 Abs. 1 Satz 1 und 2 BVerfSchG als auch § 21 Abs. 1 Satz 1 in Verbindung mit § 20 Abs. 1 Satz 1 und 2 BVerfSchG bereits am 21. Dezember 1990 in Kraft getreten (vgl. BGBl I S. 2954, 2970) und seither unverändert geblieben. Durch das Inkrafttreten des Rechtsextremismus-Datei-Gesetzes am 31. August 2012 haben die angegriffenen Übermittlungsvorschriften jedoch einen neuen Gehalt bekommen. § 8 RED-G verweist für die Übermittlung von Erkenntnissen aufgrund eines Ersuchens nach § 6 Abs. 1 Satz 1 RED-G zwischen den beteiligten Behörden auf die jeweils geltenden – und damit auch die vorliegend angegriffenen – Übermittlungsvorschriften. Als Instrument der Informationsanbahnung erleichtert die Rechtsextremismus-Datei damit den fachrechtlichen Austausch und verleiht so den bestehenden Einzelübermittlungsvorschriften materiell ein verändertes Gewicht. Es stellt diese in ein anderes, nun vorinformiertes Umfeld und bewirkt den Austausch von Erkenntnissen für Fälle, in denen er andernfalls unpraktikabel oder unmöglich wäre (zur strukturähnlichen Antiterrordatei BVerfGE 133, 277 <331 f. Rn. 127 f.>). Hierin liegt eine neue grundrechtliche Beschwer, für welche die Beschwerdefrist neu in Gang gesetzt wird (vgl. BVerfGE 45, 104 <119>; 100, 313 <356>; 141, 220 <262 f. Rn. 85>; 154, 152 <214 Rn. 83>; stRspr). 92

d) Die angegriffenen Übermittlungsvorschriften haben zum Teil Bezüge zu datenschutzrechtlichen Bestimmungen in Rechtsakten der Europäischen Union wie insbesondere in der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl EU, L 119 vom 4. Mai 2016, S. 89 – JI-Richtlinie). Ungeachtet der Frage der Anwendbarkeit von Rechtsvorschriften der Europäischen Union auf die Übermittlungsbefugnisse der Verfassungsschutzbehörden (vgl. Art. 4 Abs. 2 Satz 3 EUV) ist die Zuständigkeit des Bundesverfassungsgerichts für die Prüfung der Vereinbarkeit dieser Normen mit den Grundrechten des Grundgesetzes eröffnet und ist die Verfassungsbeschwerde zulässig, 93

da es sich jedenfalls nicht um die Umsetzung zwingenden Unionsrechts handelt (vgl. dazu BVerfGE 155, 119 <162 ff. Rn. 83 ff.> m.w.N. – Bestandsdatenauskunft II; 156, 11 <35 ff. Rn. 63 ff.> – Antiterrordateigesetz II; s. auch BVerfGE 152, 152 <168 f. Rn. 39, 42> – Recht auf Vergessen I; 158, 1 <27 Rn. 45> – Ökotox; 158, 170 <183 Rn. 23> – IT-Sicherheitslücken; BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 142 f. – Bayerisches Verfassungsschutzgesetz). Rechtsvorschriften der Europäischen Union enthalten keine Bestimmungen, welche die hier angegriffenen Übermittlungsbefugnisse einer Verfassungsschutzbehörde erforderten oder gar abschließend regelten.

C.

Soweit die Verfassungsbeschwerde zulässig ist, ist sie auch begründet. Die durch die angegriffenen Vorschriften ermöglichte Übermittlung personenbezogener Daten greift in das Grundrecht des Beschwerdeführers auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG ein (I.). Die angegriffenen Vorschriften sind zwar formell verfassungsgemäß (II.), genügen aber in ihrer Ausgestaltung nicht durchgehend den Anforderungen an die Normenklarheit und die Verhältnismäßigkeit (III.). 94

I.

Durch Übermittlungen personenbezogener Daten und Informationen nach den angegriffenen Regelungen ist das – vom Beschwerdeführer allein gerügte – Grundrecht auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG betroffen. 95

Die Übermittlung personenbezogener Daten, mit der eine Behörde die von ihr erhobenen Daten einer anderen Stelle zugänglich macht, begründet einen eigenen Grundrechtseingriff. Dieser ist an dem Grundrecht zu messen, in das bei der ursprünglichen Datenerhebung eingegriffen wurde (vgl. BVerfGE 154, 152 <266 Rn. 212>; BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 230; stRspr). Die gerügten Vorschriften umfassen die Übermittlung von Informationen einschließlich personenbezogener Daten, die die Verfassungsschutzbehörden mit verschiedenen Maßnahmen unterschiedlichen Eingriffsgewichts erhoben haben oder die ihnen anderweitig bekannt geworden sind. Der Beschwerdeführer beanstandet die Übermittlungstatbestände allerdings nur hinsichtlich der Übermittlung mit nachrichtendienstlichen Mitteln heimlich erhobener personenbe- 96

zogener Daten, die unter Eingriff in sein Grundrecht auf informationelle Selbstbestimmung erlangt wurden. Bei der verfassungsrechtlichen Würdigung ist zudem in Rechnung zu stellen, dass für die Übermittlung von Daten und Informationen, die unter Eingriff in das Brief- und Fernmeldegeheimnis (Art. 10 Abs. 1 GG) und das Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG) erhoben wurden, strengere Anforderungen geregelt sind. Hier ist jede weitere Nutzung der Daten in einem neuen Verfahren nur dann zweckentsprechend, wenn sie auch aufgrund einer den Erhebungsvoraussetzungen entsprechend dringenden beziehungsweise zumindest konkretisierten Gefahr erforderlich ist. Zusätzlich ist sicherzustellen, dass Daten, die aus einer optischen Wohnraumüberwachung erlangt worden sind, dabei allein im Fall einer dringenden Gefahr zu deren Abwehr übermittelt werden dürfen (vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 228, 388). Grundsätzlich unzulässig ist ihre Übermittlung an die Strafverfolgungsbehörden. Art. 13 Abs. 3 GG erlaubt für die Strafverfolgung nur den Einsatz der akustischen Wohnraumüberwachung. Dies darf durch eine Übermittlung von Daten aus einer präventiv angeordneten optischen Wohnraumüberwachung nicht unterlaufen werden (BVerfGE 141, 220 <338 f. Rn. 317>).

II.

Die angegriffenen Vorschriften sind in formeller Hinsicht mit der Verfassung vereinbar. Insbesondere steht dem Bund sowohl für § 20 Abs. 1 Satz 1 und 2 als auch für § 21 Abs. 1 Satz 1 in Verbindung mit § 20 Abs. 1 Satz 1 und 2 BVerfSchG die Gesetzgebungskompetenz zu. 97

1. Die Zuständigkeit für die Regelung der Übermittlungsbefugnisse des Bundesamtes für Verfassungsschutz nach § 20 Abs. 1 Satz 1 und 2 BVerfSchG ergibt sich aus Art. 73 Abs. 1 Nr. 10 Buchstabe b GG. Danach hat der Bund die ausschließliche Kompetenz für die Zusammenarbeit des Bundes und der Länder im Bereich des Verfassungsschutzes. Diese umfasst zwar nicht die allgemeine Zuständigkeit für den Verfassungsschutz. Jedoch ermöglicht der Kompetenztitel dem Bund, auch in gewissem Umfang selbst im Bereich des Verfassungsschutzes gesetzgeberisch tätig zu werden und dem Bundesamt für Verfassungsschutz die für seine Aufgaben erforderlichen Befugnisse einzuräumen (vgl. BVerfGE 155, 119 <174 Rn. 116> m.w.N.). Dazu gehören auch die hier in Frage stehenden Übermittlungsbefugnisse. 98

2. Soweit § 21 Abs. 1 Satz 1 in Verbindung mit § 20 Abs. 1 Satz 1 und 2 BVerfSchG die Übermittlung von personenbezogenen Daten durch die Verfas- 99

sungsschutzbehörden der Länder an die Staatsanwaltschaften und Polizeien von Bund und Ländern vorsieht, folgt die Kompetenz zur Regelung der behördlichen Zusammenarbeit grundsätzlich aus Art. 73 Abs. 1 Nr. 10 Buchstabe a bis c GG. Diese Zusammenarbeit umfasst insbesondere die laufende gegenseitige Unterrichtung und Auskunftserteilung (vgl. BVerfGE 133, 277 <317 f. Rn. 96 ff.>; 156, 11 <41 Rn. 76>). Hierunter fällt auch die für Staatsschutzdelikte vorgesehene Übermittlungspflicht der Verfassungsschutzbehörden der Länder.

Dem Rückgriff auf Art. 73 Abs. 1 Nr. 10 GG steht dabei nicht entgegen, dass 100
eine Zusammenarbeit der Polizei- und Verfassungsschutzbehörden nicht nur fachlich, sondern zugleich fachübergreifend geregelt wird. So bezweckt die Vorschrift gerade nicht die Übermittlung zwischen den jeweiligen Fachbehörden auf Landes- und Bundesebene untereinander, die sich für die Verfassungsschutzbehörden nach § 6 Abs. 1 BVerfSchG richtet. Vielmehr ist § 21 Abs. 1 Satz 1 BVerfSchG auf eine übergreifende Zusammenarbeit zwischen den Verfassungsschutzbehörden einerseits und den Staatsanwaltschaften und Polizeien andererseits gerichtet. Art. 73 Abs. 1 Nr. 10 GG erlaubt derartige fachübergreifende Regelungen (vgl. BVerfGE 133, 277 <318 Rn. 99>; 156, 11 <41 Rn. 77>). Dies entspricht nicht nur einem funktionalen Verständnis der Norm, die allgemein eine Effektivierung der Zusammenarbeit der verschiedenen Sicherheitsbehörden über föderale Kompetenzgrenzen hinweg ermöglichen will, sondern wird auch durch ihre ursprüngliche Fassung nahegelegt, die noch nicht in einzelne Buchstaben aufgegliedert war. Den Materialien lässt sich ebenfalls nichts für ein engeres Verständnis entnehmen. Die Änderung der Vorschrift im Jahr 1972 hatte nicht das Ziel, der Norm in dieser Hinsicht einen anderen Sinn zu geben (vgl. BTDrucks VI/1479; BVerfGE 133, 277 <318 Rn. 99>).

Die Gesetzgebungskompetenz des Bundes aus Art. 73 Abs. 1 Nr. 10 GG er- 101
streckt sich ferner nicht nur auf die Zusammenarbeit des Bundes und der Länder, sondern ebenfalls auf die der Länder untereinander. Dieses Verständnis wird nicht nur durch den Wortlaut nahegelegt, sondern entspricht auch ihrer Zielsetzung (vgl. auch BbgVerfG, Urteil vom 9. Dezember 2004 - VfGBbg 6/04 - m.w.N.). Hingegen besteht keine Bundeskompetenz für die Regelung der Übermittlung von Informationen zwischen Behörden desselben Landes. Dies hat der Gesetzgeber auch in § 21 Abs. 1 Satz 2 BVerfSchG zugrunde gelegt.

Schließlich umfasst die Bundeskompetenz aus Art. 73 Abs. 1 Nr. 10 GG grund- 102
sätzlich die Regelung der Übermittlungspflichten im Bereich der Staatsschutzdelik-

te mit Blick sowohl auf eine präventive als auch auf eine repressive Zwecksetzung.

Danach steht dem Bund die Gesetzgebungskompetenz zu, soweit § 21 Abs. 1 Satz 1 in Verbindung mit § 20 Abs. 1 Satz 2 Variante 2 BVerfSchG eine Übermittlung zur präventiven Verhinderung von sonstigen Straftaten zulässt, 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 Art. 73 Abs. 1 Nr. 10 Buchstabe b oder c GG genannten Schutzgüter gerichtet sind. 103

Die Zuständigkeit für die Regelung der Übermittlungsverpflichtung zur präventiven Verhinderung der in den Katalogen der §§ 74a und 120 GVG normierten Staatsschutzdelikte nach § 21 Abs. 1 Satz 1 in Verbindung mit § 20 Abs. 1 Satz 2 Variante 1 BVerfSchG folgt ebenfalls aus Art. 73 Abs. 1 Nr. 10 GG. Soweit die Katalogstraftaten – wie ganz überwiegend – einen hinreichenden Staatsschutzbezug aufweisen, ergibt sich die Bundeskompetenz bereits aus Art. 73 Abs. 1 Nr. 10 Buchstabe b und c GG. Hinsichtlich der übrigen Katalogdelikte kann der Bund ergänzend auf Art. 73 Abs. 1 Nr. 10 Buchstabe a GG zurückgreifen. Denn der Begriff „Kriminalpolizei“ in Art. 73 Abs. 1 Nr. 10 Buchstabe a GG schließt nicht aus, dass der Bund eine Zusammenarbeit auch zur Verhinderung von Straftaten regeln kann, sondern dient lediglich der Beschränkung auf Regelungen, die sich auf bedeutsame Straftaten von Gewicht beziehen (vgl. BVerfGE 133, 277 <318 Rn. 98>; 156, 11 <41 f. Rn. 77>). Dabei muss es sich allerdings um Straftatbestände handeln, bei denen es der durch Art. 73 Abs. 1 Nr. 10 GG erlaubten Zusammenarbeit bedarf oder eine solche naheliegt. Ausgeschlossen sind von vornherein die allgemeine Gefahrenabwehr oder die Bekämpfung von Kleinkriminalität, erst recht die Bekämpfung von Ordnungswidrigkeiten (BVerfGE 156, 11 <41 f. Rn. 77>). 104

Die Katalogstraftaten der §§ 74a und 120 GVG sind auf bedeutsame Straftaten von Gewicht im vorgenannten Sinne beschränkt. Dementsprechend findet auch die Regelung der Übermittlungspflicht zur repressiven Strafverfolgung dieser Katalogstraftaten ihre Grundlage in Art. 73 Abs. 1 Nr. 10 GG. Nichts anderes gilt im Grundsatz für die sonstigen Straftaten im Sinne des § 20 Abs. 1 Satz 2 Variante 2 BVerfSchG, an deren Verfolgung der Gesetzgeber jedenfalls wegen ihrer Ausrichtung gegen die Schutzgüter des Art. 73 Abs. 1 Nr. 10 Buchstabe b oder c GG ein „herausragendes öffentliches Interesse“ (vgl. BTDrucks 18/4654, S. 34) anerkennt. Soweit einzelnen Straftaten das notwendige Gewicht fehlt, könnte sich der Bund 105

auf die konkurrierende Gesetzgebungskompetenz des Art. 74 Abs. 1 Nr. 1 Variante 4 GG für das gerichtliche Verfahren stützen. Die Kompetenzmaterie „gerichtliches Verfahren“ ist weit zu verstehen. Sie erstreckt sich auf das Strafverfahrensrecht als das Recht der Aufklärung und Aburteilung von Straftaten; hierzu gehören die Ermittlung und Verfolgung von Straftätern einschließlich der Fahndung nach ihnen (vgl. BVerfGE 150, 244 <273 Rn. 67> – Kfz-Kennzeichenkontrollen 2) und damit auch die angegriffenen Regelungen, soweit sie repressive Tätigkeiten der ermächtigten Behörden betreffen (vgl. BVerfGE 155, 119 <175 Rn. 119>).

III.

Die angegriffenen Übermittlungsbefugnisse genügen jedoch in materieller Hinsicht in ihrer konkreten Ausgestaltung nicht den verfassungsrechtlichen Anforderungen an die Normenklarheit und die Verhältnismäßigkeit. 106

1. Verfassungsschutzbehörden dürfen die mit nachrichtendienstlichen Mitteln erhobenen personenbezogenen Daten und Informationen nur dann an andere Behörden übermitteln, wenn die Rechtsgrundlage hierfür hinreichend bestimmt und normenklar ist (a) sowie den Grundsatz der Verhältnismäßigkeit wahrt (b). Die Übermittlung bedarf schließlich einer Protokollierung (c). 107

a) Als neuerliche Grundrechtseingriffe bedürfen Übermittlungen personenbezogener Daten einer eigenen hinreichend bestimmten und normenklaren Rechtsgrundlage (vgl. BVerfGE 113, 348 <375 ff.>; 154, 152 <237 f. Rn. 137, 266 Rn. 213>; 156, 11 <44 ff. Rn. 85 ff.>; BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 199, 272; stRspr). Der Grundsatz der Bestimmtheit und Normenklarheit dient dabei der Vorhersehbarkeit von Eingriffen für die Bürgerinnen und Bürger, einer wirksamen Begrenzung der Befugnisse gegenüber der Verwaltung sowie der Ermöglichung einer effektiven Kontrolle durch die Gerichte. 108

aa) Bei der Bestimmtheit geht es vornehmlich darum, dass Regierung und Verwaltung im Gesetz steuernde und begrenzende Handlungsmaßstäbe vorfinden und dass die Gerichte eine wirksame Rechtskontrolle vornehmen können. Der Gesetzgeber ist gehalten, seine Regelungen so bestimmt zu fassen, wie dies nach der Eigenart des zu ordnenden Lebenssachverhalts mit Rücksicht auf den Normzweck möglich ist (vgl. BVerfGE 145, 20 <69 f. Rn. 125> m.w.N.). Dabei reicht es aus, wenn sich im Wege der Auslegung der einschlägigen Bestimmung mit Hilfe der anerkannten Auslegungsregeln feststellen lässt, ob die tatsächlichen Voraus- 109

setzungen für die in der Rechtsnorm ausgesprochene Rechtsfolge vorliegen. Verbleibende Unsicherheiten dürfen nicht so weit gehen, dass die Vorhersehbarkeit und Justiziabilität des Handelns der durch die Norm ermächtigten staatlichen Stellen gefährdet sind (vgl. BVerfGE 134, 141 <184 Rn. 126>; 156, 11 <44 f. Rn. 85 ff.> m.w.N.).

bb) Bei der Normenklarheit steht die inhaltliche Verständlichkeit der Regelung im Vordergrund, insbesondere damit Bürgerinnen und Bürger sich auf mögliche belastende Maßnahmen einstellen können (vgl. BVerfGE 145, 20 <69 f. Rn. 125>). Bei der heimlichen Datenerhebung und -verarbeitung, die tief in die Privatsphäre einwirken können, stellt sie besonders strenge Anforderungen. Da deren Handhabung von den Betroffenen weitgehend nicht wahrgenommen und angegriffen werden kann, kann ihr Gehalt nur sehr eingeschränkt im Wechselspiel von Anwendungspraxis und gerichtlicher Kontrolle konkretisiert werden. Im Einzelnen unterscheiden sich hierbei die Anforderungen allerdings maßgeblich nach dem Gewicht des Eingriffs und sind insoweit mit den jeweiligen materiellen Anforderungen der Verhältnismäßigkeit eng verbunden (BVerfGE 141, 220 <265 Rn. 94>; 155, 119 <181 Rn. 133>; BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 273 jeweils m.w.N.; stRspr). 110

Weil die Grundrechte hier ohne Wissen der Bürgerinnen und Bürger und oft ohne die Erreichbarkeit gerichtlicher Kontrolle durch die Verwaltung, durch Polizei und Nachrichtendienste eingeschränkt werden, muss der Inhalt der einzelnen Norm verständlich und ohne größere Schwierigkeiten durch Auslegung zu konkretisieren sein. So mag eine Regelung durch Auslegung bestimmbar oder der verfassungskonformen Auslegung zugänglich und damit im Verfassungssinne bestimmt sein, jedoch geht damit nicht zwingend auch ihre Normenklarheit für die Adressaten einher (vgl. BVerfGE 156, 11 <45 f. Rn. 87 f.> m.w.N.). 111

(1) Die Normenklarheit setzt insbesondere der Verwendung gesetzlicher Verweisungsketten Grenzen. An einer normenklaren Rechtsgrundlage fehlt es zwar nicht schon deshalb, weil in einer Norm auf eine andere Norm verwiesen wird. Doch müssen Verweisungen begrenzt bleiben, dürfen nicht durch die Inbezugnahme von Normen, die andersartige Spannungslagen bewältigen, ihre Klarheit verlieren und in der Praxis nicht zu übermäßigen Schwierigkeiten bei der Anwendung führen. Unübersichtliche Verweisungskaskaden sind mit den grundrechtlichen Anforderungen daher nicht vereinbar (BVerfGE 154, 152 <266 Rn. 215> mit Verweis auf BVerfGE 110, 33 <57 f., 61 ff.>; BVerfG, Urteil des Ersten Senats vom 112

26. April 2022 - 1 BvR 1619/17 -, Rn. 391). Die inhaltliche Verständlichkeit der Regelung darf nicht verloren gehen. Die Verständlichkeit kann etwa durch eine hohe Anzahl von Gliedern in einer Verweisungskette verloren gehen. Problematisch kann es auch sein, wenn sich die Verweisungskette über eine Vielzahl verschiedener Fachgesetze erstreckt, indem die in Bezug genommenen Normen ihrerseits wieder auf andere Normen verweisen. Dies gilt umso mehr, wenn die in Bezug genommenen Normen aus ihrem inhaltlichen Kontext herausgelöst und in einen anderen Kontext gestellt werden, so dass der Bezug zum Gegenstand der Ausgangsnorm zunehmend unschärfer wird. Der Klarheit abträglich sind ferner pauschale Verweisungen auf ganze Fachgesetze mit verschiedenen Regelungskomplexen. Ein Mangel an Normenklarheit ist auch damit verbunden, dass auf Rechtsgrundlagen verwiesen wird, deren maßgebender Inhalt nur mit Schwierigkeiten erfasst werden kann (vgl. BVerfGE 110, 33 <63>). Verweist der Gesetzgeber auf andere Regelungen, hat er deshalb einzubeziehen, inwieweit sich diese selbst und für sich genommen bereits im Grenzbereich der Normenklarheit bewegen. Lange, über mehrere Ebenen gestaffelte, unterschiedlich variable Verweisungsketten, die bei gleichzeitiger Verzweigung in die Breite den Charakter von Kaskaden annehmen, sind daher problematisch (vgl. BVerfGE 110, 33 <63 f.>).

(2) Die Normenklarheit steht aber der Verwendung von Verweisungsketten nicht grundsätzlich entgegen. Verweisungen entlasten den Normtext und beugen unterschiedlichen Regelungen inhaltlich vergleichbarer Fragen vor. Verweisungsketten können auch als solche in komplexen Regelungszusammenhängen gegenüber der als Alternative in Betracht kommenden Umschreibung aller Eingriffsvoraussetzungen in einer Eingriffsnorm selbst durchaus vorzugswürdig sein. An Klarheit wird durch die Zusammenfassung in einer einzigen Norm nicht notwendig etwas gewonnen (vgl. insoweit BVerfGE 110, 33 <63>). Das Gebot der Normenklarheit des Gesetzes darf deshalb nicht übersteigert werden, da die Gesetze sonst zu lang und wiederum unverständlich würden. 113

Diese Gefahr läge nahe, wenn der Gesetzgeber stets jede Übermittlungsvorschrift bis ins Letzte ausführen müsste, ohne auf Verweisungen zurückgreifen zu können. Es kann im Bereich heimlicher Überwachung zweckdienlich und der Normenklarheit zuträglich sein, auf Fachgesetze zu verweisen. So werden die dort geregelten Sachverhalte häufig nicht in selber Weise der Heimlichkeit unterworfen sein wie sicherheitsrechtliche Datenverarbeitungen. Unbestimmte Rechtsbegriffe oder Auslegungsfragen können daher im dortigen Kontext – mit entsprechender Wirkung auch für die hieran anknüpfende heimliche Datenübermittlung – im 114

Wechselspiel von Anwendungspraxis und gerichtlicher Kontrolle konkretisiert werden (vgl. zu diesem Aspekt BVerfGE 156, 11 <45 Rn. 87>).

Auch die Verwendung mehrgliedriger Verweisungsketten ist nicht ausgeschlossen, wenn die Normadressaten aus diesen selbst heraus klar erfassen können, ob sie von einer heimlichen Datenübermittlung betroffen sein können. Das zu erfassen wird insbesondere durch Verweisungsketten erleichtert, die die in Bezug genommenen Vorschriften vollständig aufführen. Dabei gibt es keine starre Höchstgrenze der Glieder einer Verweisungskette. Vielmehr ist in einer wertenden Gesamtbetrachtung unter Berücksichtigung möglicher Regelungsalternativen zu entscheiden, ob eine Verweisung mit dem Gebot der Normenklarheit vereinbar ist. Zu gewichten sind die Besonderheiten des jeweiligen Übermittlungstatbestands einschließlich der Umstände, die zu der gesetzlichen Regelung führen (vgl. BVerfGE 28, 175 <183>; 86, 288 <311>; 126, 170 <196>; 149, 293 <324 Rn. 78>), wobei insbesondere auch der jeweilige Kreis der Normanwender und Normbetroffenen von Bedeutung sein kann (vgl. BVerfGE 110, 33 <64>; 123, 39 <81>; 128, 282 <318>; 149, 293 <324 Rn. 77>). 115

b) Die gesetzlichen Ermächtigungen zur Datenübermittlung als auch die Übermittlungsmaßnahmen im Einzelfall müssen den Anforderungen der Verhältnismäßigkeit genügen. Die Übermittlung muss zur Erreichung eines legitimen Zwecks geeignet, erforderlich und verhältnismäßig im engeren Sinne sein (vgl. BVerfGE 65, 1 <45 f.>; 141, 220 <327 Rn. 286>; 155, 119 <176 f. Rn. 123>; BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 149, 230; stRspr). Aus dem Grundsatz der Verhältnismäßigkeit im engeren Sinne ergeben sich an die Ausgestaltung der Übermittlungsbefugnisse von Verfassungsschutzbehörden differenzierte Anforderungen. Da Verfassungsschutzbehörden im Vergleich zu Behörden mit operativen Anschlussbefugnissen bei der Datenerhebung modifizierten Eingriffsschwellen unterworfen sind (aa), unterliegt die Übermittlung der mit nachrichtendienstlichen Mitteln erhobenen personenbezogenen Daten und Informationen gesteigerten Voraussetzungen (bb). 116

aa) Nachrichtendienstliche Behörden schöpfen ihre Erkenntnisse aus einer Fülle von Daten, die sie weit im Vorfeld konkreter Gefahren und operativer Tätigkeit erheben, miteinander und mit Erkenntnissen anderer Stellen verknüpfen und filtern, um daraus relevante Informationen zu gewinnen und auch weiterzugeben; dies ist eine Besonderheit ihrer Aufgabe (BVerfG, Urteil des Ersten Senats vom 117

26. April 2022 - 1 BvR 1619/17 -, Rn. 239 – Bayerisches Verfassungsschutzgesetz; vgl. auch BVerfGE 154, 152 <267 f. Rn. 218>).

Dass eine Verfassungsschutzbehörde nicht über eigene operative Anschlussbefugnisse verfügt, rechtfertigt es dabei im Grundsatz, die ihr zur Wahrnehmung ihrer Beobachtungsaufgaben eingeräumten Datenerhebungsbefugnisse im Vergleich zu den Befugnissen einer Behörde mit operativen Anschlussbefugnissen wegen des geringeren Eingriffsgewichts an modifizierte Eingriffsschwellen zu knüpfen, die zugleich dem speziellen Charakter der Aufgaben des Verfassungsschutzes entsprechen (vgl. mit ausführlicher Herleitung BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 157 bis 169). 118

Um dem Charakter der Tätigkeit der Verfassungsschutzbehörden und damit deren besonderer Aufgabenstellung Rechnung zu tragen, verfassungsfeindliche Bestrebungen im Vorfeld konkreter Gefahren aufzuklären (vgl. BVerfGE 120, 274 <330>; BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 162, 240), haben sie breite Befugnisse zur Datensammlung, die teilweise weder hinsichtlich der konkreten Tätigkeitsfelder spezifisch ausdefiniert noch hinsichtlich der jeweils einzusetzenden Mittel und der betroffenen Personen detailscharf ausgestaltet sind (vgl. BVerfGE 133, 277 <325 Rn. 117>). So sind wenig eingriffsintensive nachrichtendienstliche Maßnahmen durch Verfassungsschutzbehörden schon bei einem schlichten verfassungsschutzspezifischen Beobachtungsbedarf zulässig, ohne dass sich eine polizeiliche Gefahr in irgendeiner Weise abzeichnen müsste oder eine gesteigerte verfassungsschutzspezifische Beobachtungsbedürftigkeit gefordert wäre (vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 185 f.). Auch sind, sofern nachrichtendienstliche Grundrechtseingriffe für sich genommen gering wiegen, nicht unbedingt Anhaltspunkte für eine spezifische Verantwortlichkeit der Betroffenen erforderlich (vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 210 ff.). Von ihrer Verantwortlichkeit abzusehen wäre aber in anderen Bereichen des Sicherheitsrechts – jedenfalls bei noch kaum konkretisiertem Eingriffsanlass – mit verfassungsrechtlichen Anforderungen an staatliche Überwachung grundsätzlich nicht vereinbar (vgl. BVerfGE 150, 244 <297 Rn. 142> – Kfz-Kennzeichenkontrollen 2). Dass nachrichtendienstliche Beobachtung weit im Vorfeld konkreter Gefahren zulässig ist, begründet zugleich die inhaltliche Weite des Tätigkeitsfelds, das gerade nicht durch ein von konkreter Gefahr bedrohtes Schutzgut definiert wird, sondern durch eine möglicherweise noch wenig konkrete allgemeine Bedrohung vergleichsweise abstrakter Rechtsgüter nur grob abge- 119

steckt ist. Diese breite nachrichtendienstliche Beobachtungstätigkeit geschieht überdies weitgehend im Verborgenen. Die Nachrichtendienste sammeln Daten grundsätzlich geheim. Der Grundsatz der Offenheit der Datenerhebung gilt für sie nicht, und sie sind von Transparenz- und Berichtspflichten gegenüber den Betroffenen weithin freigestellt. Entsprechend gering sind die Möglichkeiten individuellen Rechtsschutzes (BVerfGE 133, 277 <325 f. Rn. 117>; BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 240).

Die weitreichenden Überwachungsbefugnisse der Verfassungsschutzbehörden können verfassungsrechtlich aber nur gerechtfertigt werden, wenn die aus der Überwachung gewonnenen Informationen nicht ohne Weiteres an andere Behörden mit operativen Anschlussbefugnissen übermittelt werden dürfen („informationelles Trennungsprinzip“; vgl. BVerfGE 133, 277 <329 Rn. 123>; 156, 11 <50 Rn. 101, 51 f. Rn. 105>). Ansonsten böte der Umstand, dass die Verfassungsschutzbehörde selbst nicht über operative Anschlussbefugnisse verfügt, den Überwachten am Ende doch kaum Schutz: Die der Verfassungsschutzbehörde verschlossenen eingriffsintensiven Folgemaßnahmen könnten dann von operativ ausgestatteten Behörden durchgeführt werden, die dabei die durch die Verfassungsschutzbehörde erlangten Informationen weiternutzten, ohne dass die für sie selbst als operative Behörden geltenden Datenerhebungsvoraussetzungen erfüllt sein müssten. Auf Seiten der empfangenden Behörde würden so die grundrechtsschützenden Eingriffsschwellen der Befugnisse operativer Behörden umgangen; zugleich verlöre auf Seiten der Verfassungsschutzbehörden der Umstand, dass diese ohne operative Anschlussbefugnisse sind, seinen schützenden Effekt. Um beides zu verhindern, sind hinreichende Übermittlungsvoraussetzungen verfassungsrechtlich unerlässlich (vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 171 f.). 120

bb) Der Grundsatz der Verhältnismäßigkeit im engeren Sinne stellt deshalb besondere Anforderungen an die gesetzliche Ausgestaltung der Übermittlungsbefugnisse von Verfassungsschutzbehörden. Die Anforderungen an die weitere Nutzung und Übermittlung staatlich erhobener Daten richten sich nach den Grundsätzen der Zweckbindung und Zweckänderung. Erlaubt der Gesetzgeber eine weitere Nutzung der Daten – wie eine Datenübermittlung – auch zu anderen Zwecken als denen der ursprünglichen Datenerhebung, liegt eine Zweckänderung vor. Dabei ist sicherzustellen, dass dem Eingriffsgewicht der Datenerhebung auch hinsichtlich der neuen Nutzung Rechnung getragen wird (vgl. BVerfGE 141, 220 <326 f. Rn. 284>; 154, 152 <267 Rn. 216>; BVerfG, Urteil des Ersten Senats vom 121

26. April 2022 - 1 BvR 1619/17 -, Rn. 225, 229). Dies richtet sich, jedenfalls, wenn die Daten mit nachrichtendienstlichen Mitteln erhoben wurden, nach dem Kriterium der hypothetischen Datenneuerhebung (1). Die Übermittlungsvoraussetzungen können sich danach unterscheiden, je nachdem, an welche Stelle übermittelt wird (2). So setzt die Übermittlung an eine Gefahrenabwehrbehörde voraus, dass sie dem Schutz eines besonders gewichtigen Rechtsguts dient, für das wenigstens eine hinreichend konkretisierte Gefahr besteht. Die Übermittlung an eine Strafverfolgungsbehörde kommt nur zur Verfolgung besonders schwerer Straftaten in Betracht und setzt voraus, dass ein durch bestimmte Tatsachen begründeter Verdacht vorliegt, für den konkrete und verdichtete Umstände als Tatsachenbasis vorhanden sind (vgl. BVerfGE 154, 152 <270 Rn. 222>; BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, 3. Leitsatz, Rn. 230 ff.).

(1) Das Kriterium der hypothetischen Datenneuerhebung dient dazu, sicherzustellen, dass dem Eingriffsgewicht der Datenerhebung auch hinsichtlich der neuen Nutzung Rechnung getragen wird (vgl. BVerfGE 141, 220 <326 f. Rn. 284> m.w.N.). Danach kommt es darauf an, ob die entsprechenden Daten nach verfassungsrechtlichen Maßstäben auch für den geänderten Zweck mit vergleichbar schwerwiegenden Mitteln neu erhoben werden dürften (vgl. BVerfGE 141, 220 <327 f. Rn. 287>; 154, 152 <266 f. Rn. 216> m.w.N.; 156, 11 <49 f. Rn. 99>; BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 231; stRspr). Das bemisst sich danach, ob der empfangenden Stelle unter den gegebenen Bedingungen eine eigene Befugnis eingeräumt werden dürfte, die Daten mit vergleichbar schwerwiegenden Mitteln wie dem ersten Eingriff erneut zu erheben. Danach sind Anforderungen sowohl an den Rechtsgüterschutz als auch an die Eingriffsschwellen, hier in Form von Übermittlungsschwellen, zu stellen (BVerfGE 154, 152 <268 Rn. 220>; stRspr). Die neue Nutzung der Daten muss also zum einen dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten solchen Gewichts dienen, dass dies eine Neuerhebung durch die empfangende Stelle mit vergleichbar schwerwiegenden Mitteln wie die vorangegangene nachrichtendienstliche Überwachung rechtfertigen könnte (vgl. BVerfGE 141, 220 <328 Rn. 288>; 154, 152 <269 Rn. 221>; 156, 11 <55 Rn. 116>). Zum anderen setzt die Übermittlung grundsätzlich einen Anlass voraus, der eine ebenso eingriffsintensive Ersterhebung durch die empfangende Stelle verfassungsrechtlich rechtfertigen würde (vgl. BVerfGE 133, 277 <329 Rn. 123>; 154, 152 <269 f. Rn. 222>; 156, 11 <55 Rn. 117 f.>). Dabei gilt der Grundsatz der hypothetischen Datenneuerhebung nicht schematisch abschließend und schließt die Berücksichtigung weiterer Gesichtspunkte nicht aus (vgl. BVerfGE 156, 11 <50 Rn. 100> m.w.N.). Das Kriterium 122

der hypothetischen Neuerhebung gilt grundsätzlich auch für die Übermittlung von Daten durch nachrichtendienstliche Behörden, also auch durch eine Verfassungsschutzbehörde (vgl. BVerfGE 141, 220 <327 f. Rn. 287>; 154, 152 <266 f. Rn. 216>; 156, 11 <1. Leitsatz>; BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 232).

(2) (a) Nach dem Kriterium der hypothetischen Datenneuerhebung können sich die Übermittlungsanforderungen unterscheiden, je nachdem, an welche Behörde übermittelt wird. Denn für die Rechtfertigung einer Übermittlung kommt es danach darauf an, ob der empfangenden Behörde zu dem jeweiligen Übermittlungszweck eine eigene Datenerhebung mit vergleichbar schwerwiegenden Mitteln wie der vorangegangenen Überwachung durch die Verfassungsschutzbehörde erlaubt werden dürfte. Das hängt aber auch davon ab, mit welchen Befugnissen die empfangende Behörde ausgestattet ist. Verfügt die empfangende Behörde über operative Anschlussbefugnisse, wären an eine Datenneuerhebung wegen der unmittelbar möglichen Folgemaßnahmen – und sind entsprechend an eine Übermittlung – grundsätzlich strengere Anforderungen zu stellen, als wenn die empfangende Behörde keine weiteren operativen Befugnisse hat. Dabei ist hier nur über die Übermittlung von Informationen zu entscheiden, die mit nachrichtendienstlichen Mitteln erlangt wurden (vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 234). 123

(b) Bei der Übermittlung nachrichtendienstlich ersterhobener personenbezogener Daten und daraus gewonnener Informationen an Gefahrenabwehrbehörden gelten besonders strenge Anforderungen, wenn diese über operative Zwangsbefugnisse verfügen. Im Ergebnis setzt dies voraus, dass für ein besonders gewichtiges Rechtsgut (aa) wenigstens eine konkretisierte Gefahr (bb) besteht (BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 235). 124

(aa) Die Übermittlung nachrichtendienstlich ersterhobener personenbezogener Daten und daraus gewonnener Informationen an eine Gefahrenabwehrbehörde muss einem besonders gewichtigen Rechtsgut dienen. An der Übermittlung muss mithin ein herausragendes öffentliches Interesse bestehen (BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 236; siehe auch BVerfGE 133, 277 <329 Rn. 123>; 154, 152 <268 Rn. 219>; 156, 11 <51 f. Rn. 105, 55 Rn. 116>). 125

Für die Übermittlung von Daten, die mittels der hier überwiegend in Rede stehenden besonders eingriffsintensiven Überwachungsbefugnisse erlangt wurden, folgt das schon daraus, dass solche Befugnisse generell nur zum Schutz besonders hochwertiger Rechtsgüter eingeräumt werden dürfen. Wenn eine operativ handelnde Gefahrenabwehrbehörde mittels solcher Überwachungsbefugnisse selbst Daten erheben würde, wäre zu verlangen, dass dies dem Schutz eines besonders gewichtigen Rechtsguts dient (vgl. BVerfGE 141, 220 <270 f. Rn. 108>). Für die Übermittlung an eine Gefahrenabwehrbehörde gilt nichts anderes (BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 237). 126

Aber auch nachrichtendienstliche Erkenntnisse, die aus für sich genommen jeweils weniger eingriffsintensiven Überwachungsmaßnahmen stammen, dürfen nur zum Schutz besonders hochwertiger Rechtsgüter übermittelt werden. Eine Differenzierung nach dem Eingriffsgewicht der jeweiligen Einzelmaßnahme kommt insoweit nach dem Kriterium der hypothetischen Datenneuerhebung wegen der Besonderheiten nachrichtendienstlicher Aufgabenwahrnehmung nicht in Betracht (vgl. auch BVerfGE 133, 277 <329 Rn. 123>; 154, 152 <268 Rn. 219>; 156, 11 <51 f. Rn. 105>). Denn durch die Betrachtung eines einzelnen, für sich genommen weniger eingriffsintensiven Datenerhebungsvorgangs würde die Grundrechtsbelastung, die von der breit angelegten, teils niederschwelligen Beobachtungstätigkeit nachrichtendienstlicher Behörden ausgeht, nicht in Gänze erfasst (BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 238). 127

Auch wenn eine einzelne Datenerhebung für sich genommen weniger schwer wiegt, unterliegt diese von jeder konkreten Rechtsgutgefährdung und teilweise auch von spezifischer Verantwortlichkeit der Betroffenen losgelöste Befugnis zur weitgehend verborgenen, breit angelegten Datensammlung, -auswertung und -aufbereitung daher hohen verfassungsrechtlichen Rechtfertigungsbedingungen. Dass nachrichtendienstliche Behörden unter erleichterten Bedingungen im Vorfeld konkreter Gefahren weitgehend im Dunkeln in großer Zahl Zugriff auf personenbezogene Daten erhalten und daraus Informationen über die Bürgerinnen und Bürger gewinnen können, ist nur wegen der besonderen Aufgabe der Verfassungsschutzbehörden und hinsichtlich der besonders hohen Rechtsgüter zu rechtfertigen, denen ihre Tätigkeit dient (vgl. auch BVerfGE 133, 277 <329 Rn. 123>). Einer Polizeibehörde dürften eigene Befugnisse diesen Zuschnitts aufgrund ihres Aufgaben- und Befugnisspektrums in keiner Konstellation eingeräumt werden (vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 241). 128

Das schließt eine Übermittlung zwar nicht von vornherein aus, denn das Kriterium der hypothetischen Neuerhebung gilt nicht schematisch abschließend. Dass die Zielbehörde bestimmte Datenerhebungen, zu denen die Ausgangsbehörde berechtigt ist, ihrerseits wegen ihres Aufgabenspektrums nicht vornehmen darf, steht einem Datenaustausch nicht prinzipiell entgegen (vgl. BVerfGE 141, 220 <328 Rn. 287>; 154, 152 <268 Rn. 219>; 156, 11 <50 Rn. 100>). Was den Übermittlungszweck angeht, ist das Kriterium der hypothetischen Neuerhebung jedoch streng. Voraussetzung für eine Zweckänderung ist danach jedenfalls, dass die neue Nutzung der Daten dem Schutz von Rechtsgütern solchen Gewichts dient, dass dies ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln verfassungsrechtlich rechtfertigen könnte (vgl. BVerfGE 141, 220 <328 Rn. 288>). Danach darf die Übermittlung – auch von aus weniger eingriffsintensiven Maßnahmen erlangten Informationen – nur zum Schutz eines Rechtsguts von herausragendem öffentlichem Interesse erfolgen (vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 242). 129

Besonders gewichtige Rechtsgüter sind Leib, Leben und Freiheit der Person sowie der Bestand oder die Sicherheit des Bundes oder eines Landes (vgl. BVerfGE 156, 11 <55 Rn. 116>). Darüber hinaus kann auch der Schutz von Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, die Übermittlung rechtfertigen (vgl. BVerfGE 141, 220 <296 Rn. 183>). Allerdings ist dabei ein enges Verständnis geboten. Gemeint sind etwa wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen (vgl. BVerfGE 133, 277 <365 Rn. 203>). Die Übermittlung muss dabei nicht auf den Schutz desselben Rechtsguts gerichtet sein wie die nachrichtendienstliche Überwachungsmaßnahme (vgl. BVerfGE 154, 152 <269 Rn. 221>) (BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 243). 130

Bei der Regelung der Übermittlung nachrichtendienstlich erhobener Daten zur Gefahrenabwehr muss der Gesetzgeber das erforderliche Rechtsgut auch nicht zwingend unmittelbar benennen, sondern kann an entsprechende Straftaten anknüpfen (vgl. dazu BVerfGE 154, 152 <269 Rn. 221>). Bezieht er sich nicht unmittelbar auf Rechtsgüter, sondern auf die Art der zur verhindernden Straftaten, sind die Gewichtungen, die für die strafprozessuale Datenerhebung gelten, entsprechend heranzuziehen. Zwischen der präventiven und der repressiven Anknüpfung von Übermittlungsvoraussetzungen an Straftaten besteht ein Gleichlauf (vgl. BVerfGE 141, 220 <348 Rn. 347>). Allerdings ist für die bei der Übermittlung poli- 131

zeilich ersterhobener Daten geltende Abstufung nach erheblichen, schweren und besonders schweren Straftaten bei der Übermittlung nachrichtendienstlich erhobener Daten an Gefahrenabwehrbehörden kein Raum. Das Rechtsgut muss insoweit vielmehr immer von herausragendem öffentlichem Interesse sein. Dem entspricht eine Begrenzung auf besonders schwere Straftaten (vgl. BVerfGE 154, 152 <269 Rn. 221 a.E.>) (BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 244).

(bb) Als Übermittlungsschwelle für Übermittlungen durch den Verfassungsschutz an Gefahrenabwehrbehörden muss wenigstens eine konkretisierte Gefahr (vgl. BVerfGE 141, 220 <272 f. Rn. 112>) bestehen. 132

Zwar gilt wiederum, dass die Verfassungsschutzbehörde regelmäßig Informationen übermitteln wird, die sie nicht aus einem einzelnen Datenerhebungsvorgang, sondern aus ihrer breit angelegten Beobachtungstätigkeit im Verborgenen gewonnen hat, und dass Befugnisse solchen Zuschnitts Polizeibehörden aufgrund ihres Aufgaben- und Befugnisspektrums in keiner Konstellation eingeräumt werden dürften. Jedoch steht auch insoweit die Tatsache, dass die Zielbehörde bestimmte Datenerhebungen, zu denen die Ausgangsbehörde berechtigt ist, ihrerseits wegen ihres Aufgabenspektrums nicht vornehmen darf, einem Datenaustausch nicht prinzipiell entgegen (vgl. BVerfGE 141, 220 <328 Rn. 287>; 154, 152 <268 Rn. 219>). Weil den Gefahrenabwehrbehörden so weite Befugnisse wie dem Verfassungsschutz von vornherein nicht zur Verfügung gestellt werden dürften, gelten für die Übermittlungsschwelle (auch Übermittlungsanlass genannt) die verfassungsrechtlichen Anforderungen, die sonst im Bereich der Gefahrenabwehr für heimliche Überwachungsmaßnahmen mit hoher Eingriffsintensität gelten (vgl. auch BVerfGE 154, 152 <268 Rn. 219>), mithin das Erfordernis einer wenigstens konkretisierten Gefahr (dazu BVerfGE 141, 220 <271 ff. Rn. 109 ff.>) (vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 246). 133

Der Begriff der hinreichend konkretisierten Gefahr ist dabei weiter als der der konkreten Gefahr, die eine Sachlage voraussetzt, bei der im konkreten Fall die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zeit ein Schaden für die jeweiligen Rechtsgüter eintreten wird (vgl. BVerfGE 115, 320 <362>). Die konkretisierte Gefahr verlangt, dass zumindest tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr für die Schutzgüter bestehen. Dies kann schon dann der Fall sein, wenn sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, sofern bereits bestimmte 134

Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen (vgl. BVerfGE 141, 220 <272 f. Rn. 112>). Danach kann bei der Übermittlung zur Gefahrenabwehr auch an Straftaten angeknüpft werden, in denen die Strafbarkeitsschwelle durch die Pönalisierung von Vorbereitungshandlungen oder bloßen Rechtsgutgefährdungen in das Vorfeld von Gefahren verlagert wird (vgl. BVerfGE 125, 260 <329 f.>; 154, 152 <269 Rn. 221>). Der Gesetzgeber muss aber sicherstellen, dass in jedem Einzelfall eine konkrete oder konkretisierte Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegt. Knüpft der Gesetzgeber die Übermittlungsregelungen an die Begehung solcher Straftaten an, muss er also zusätzlich fordern, dass damit bereits eine konkretisierte Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegt. Diese mag sich in vielen Fällen aus der drohenden Verwirklichung der Delikte ergeben. Zwingend ist dies jedoch nicht.

(c) Die verfassungsrechtlichen Anforderungen an die Regelung von Übermittlungen zur Strafverfolgung richten sich ebenfalls nach dem Kriterium der hypothetischen Datenneuerhebung. 135

Für Maßnahmen, die der Strafverfolgung dienen und damit repressiven Charakter haben, kommt es auf das Gewicht der Straftaten an, die der Gesetzgeber in – jeweils näher bestimmte – erhebliche, schwere und besonders schwere Straftaten eingeteilt hat (vgl. BVerfGE 141, 220 <270 Rn. 107>). Eine Übermittlung von Daten, die eine Verfassungsschutzbehörde mit nachrichtendienstlichen Mitteln erhoben hat, kommt nur zum Schutz eines herausragenden öffentlichen Interesses und daher nur zur Verfolgung besonders schwerer Straftaten in Betracht (vgl. BVerfGE 154, 152 <269 Rn. 221>) (BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 251). 136

Als Schwelle für die Übermittlung mit nachrichtendienstlichen Mitteln ersterhobener Daten zur Strafverfolgung muss der Gesetzgeber verlangen, dass bestimmte, den Verdacht begründende Tatsachen vorliegen, was bedeutet, dass insoweit konkrete und in gewissem Umfang verdichtete Umstände als Tatsachenbasis für den Verdacht vorhanden sein müssen (vgl. BVerfGE 154, 152 <269 f. Rn. 222>; 156, 11 <51 f. Rn. 105, 56 Rn. 120>; siehe bereits BVerfGE 100, 313 <392>). Zwar dürften auch zur Strafverfolgung keine Befugnisse solchen Zuschnitts begründet werden, wie sie dem Verfassungsschutz zustehen und aufgrund derer dieser die zur Strafverfolgung übermittelten Informationen erlangt; auch insoweit steht das dem Datenaustausch jedoch nicht prinzipiell entgegen (vgl. BVerfGE 137

141, 220 <328 Rn. 287>) (BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 252).

c) Da die Übermittlung von Daten an andere Stellen einen eigenen Grundrechtseingriff begründet, setzt sie schließlich in jedem Fall eine förmliche Entscheidung voraus, bei der die jeweiligen gesetzlichen Übermittlungsvoraussetzungen geprüft werden müssen. Dafür tragen die Verfassungsschutzbehörden angesichts ihrer weiten Befugnisse eine besondere Verantwortung. So wie ihnen einerseits besonders weite Befugnisse zukommen, müssen sie andererseits die gewonnenen Informationen vor ihrer Übermittlung sorgfältig sichten und diese in Anwendung der jeweils einschlägigen Übermittlungsvorschriften auf das notwendige Maß beschränken. Die Übermittlung ist zu protokollieren, um die Beachtung der Übermittlungsvoraussetzungen einer unabhängigen Kontrolle zugänglich zu machen (vgl. BVerfGE 141, 220 <284 Rn. 141, 340 f. Rn. 322>; 154, 152 <296 Rn. 291>). Dabei ist auch die der Übermittlung zugrunde gelegte Rechtsvorschrift zu nennen (BVerfGE 154, 152 <272 Rn. 229>). 138

2. Danach genügen die angegriffenen Übermittlungsvorschriften nicht durchgehend den verfassungsrechtlichen Anforderungen. Zum Teil wahren sie nicht den Grundsatz der Normenklarheit (a). Im Übrigen verstoßen sie gegen den Grundsatz der Verhältnismäßigkeit im engeren Sinne, da sie nicht durchgehend hinreichende Voraussetzungen für die Übermittlung vorsehen (b). Schließlich enthalten sie keine ausreichenden Vorgaben für eine Protokollierung der Datenübermittlung (c). 139

a) Zwar sind die Empfangsbehörden hinreichend bestimmt (so bereits BVerfGE 154, 152 <305 Rn. 312>). Offenbleiben kann dabei, ob die Bezugnahme in § 20 Abs. 1 Satz 2 Variante 2 BVerfSchG auf sonstige 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 Art. 73 Abs. 1 Nr. 10 Buchstabe b oder c GG genannten Schutzgüter gerichtet sind, noch den Anforderungen an die Bestimmtheit genügt. Jedenfalls entsprechen die angegriffenen Regelungen nicht durchgehend dem Gebot der Normenklarheit. 140

aa) Dies folgt hier indes nicht ohne weiteres bereits daraus, dass sich der Gesetzgeber mitunter mehrgliedriger Verweisungsketten bedient hat (vgl. BVerfGE 154, 152 <304 f. Rn. 312>; zu den Maßstäben oben Rn. 112 ff.). Der Grundsatz 141

der Normenklarheit steht der Verwendung – auch längerer – Verweisungsketten nicht kategorisch entgegen, soweit diese hinreichend verständlich gehalten sind.

So ist unter dem Aspekt der Normenklarheit etwa die Verweisungskette nach § 20 Abs. 1 Satz 1 und 2 Variante 1 BVerfSchG in Verbindung mit § 120 Abs. 1 Nr. 3 am Ende GVG in Verbindung mit § 4 Abs. 4 des Halbleiterschutzgesetzes in Verbindung mit § 9 Abs. 2 des Gebrauchsmustergesetzes und in Verbindung mit § 52 Abs. 2 des Patentgesetzes nicht zu beanstanden. Während sie zwar mehrgliedrig ist und sich über insgesamt fünf Gesetze erstreckt, führt bereits § 120 Abs. 1 Nr. 3 am Ende GVG selbst alle weiter in Bezug genommenen Vorschriften vollständig und damit für Normadressaten aus sich selbst heraus klar erfassbar auf. Zudem verweist der Gesetzgeber hier nicht pauschal auf ganze Fachgesetze, sondern spezifisch allein auf die für die Strafbarkeit relevanten Normbestandteile. 142

Mit dem Gebot der Normenklarheit ist bei einer wertenden Gesamtbetrachtung unter Berücksichtigung möglicher Regelungsalternativen beispielsweise ebenfalls vereinbar, dass § 20 Abs. 1 Satz 1 und 2 Variante 1 BVerfSchG Bezug auf § 120 Abs. 1 Nr. 6 GVG nimmt, der wiederum unter anderem auf § 129a Abs. 2 Nr. 4 StGB verweist, in dem die Strafbarkeit der Bildung einer terroristischen Vereinigung normiert wird, deren Zwecke oder deren Tätigkeit darauf gerichtet sind, bestimmte Straftaten im Sinne des Gesetzes über die Kontrolle von Kriegswaffen (KrWaffKontrG) zu begehen. § 129a Abs. 2 Nr. 4 StGB bezieht sich unter anderem auf § 20a Abs. 1 Nr. 1 KrWaffKontrG, der Verstöße gegen das in § 18a KrWaffKontrG normierte Verbot von Antipersonenminen und Streumunition sanktioniert. § 18a Abs. 2 Satz 1 KrWaffKontrG verweist für die Begriffsbestimmung von Antipersonenminen auf Artikel 2 des Übereinkommens über das Verbot des Einsatzes, der Lagerung, der Herstellung und der Weitergabe von Antipersonenminen und über deren Vernichtung vom 3. Dezember 1997. Für Streumunition gilt nach §18a Abs. 2 Satz 2 KrWaffKontrG die Begriffsbestimmung des Artikels 2 Nummer 2 des Übereinkommens über Streumunition vom 3. Dezember 2008. Eine solche Verweisungskette ist aus sich selbst heraus klar genug erfassbar. Die Mehrgliedrigkeit der Verweisungskette ist hier allein durch die Regelung einer komplexen Materie bedingt. Auch kann von dem in diesem sicherheitsrelevanten Bereich tätigen Normbetroffenen verlangt werden, dass sie sich über die einschlägigen Vorschriften unterrichten. Es entsteht keine unübersichtliche Verweisungskaskade. Der Gesetzgeber verweist zwar auf einen Straftatbestand, der seinerseits weitere Verweisungen enthält. Der Inhalt dieser Verweisungen bezieht sich aber stets auf einzelne Teilelemente des zu prüfenden Tatbestands, die in ihrer 143

abgegrenzten Form auch im Rahmen einer über mehrere Stufen gehenden Verweisungstechnik verständlich sind.

bb) Jedoch sind die angegriffenen Regelungen nicht normenklar, weil § 20 Abs. 1 Satz 2 BVerfSchG zur Bestimmung der Straftaten, die eine Übermittlungspflicht auslösen, ohne weitere Einschränkung auf § 120 GVG verweist. Diese Vorschrift normiert die Zuständigkeit des Oberlandesgerichts für die Verhandlung und Entscheidung im ersten Rechtszug in bestimmten Strafsachen. § 120 Abs. 1 GVG knüpft die Zuständigkeit allein an dort aufgezählte Straftaten an. § 120 Abs. 2 Satz 1 Nr. 1 bis 4 GVG enthält zwar ebenfalls einen Katalog von Delikten, macht die erstinstanzliche Zuständigkeit des Oberlandesgerichts aber von zusätzlichen Tatbestandsvoraussetzungen abhängig. Insbesondere wird diese Zuständigkeit nur begründet, „wenn der Generalbundesanwalt wegen der besonderen Bedeutung des Falles die Verfolgung übernimmt“. 144

Ob und inwieweit dieses Tatbestandmerkmal im Rahmen der Übermittlungspflicht zu berücksichtigen ist, lässt § 20 Abs. 1 Satz 2 Variante 1 BVerfSchG in Verbindung mit § 120 Abs. 2 GVG dabei nicht mit hinreichender Klarheit erkennen. Denkbar erscheint, auf den formalen Akt einer Verfolgungsübernahme durch den Generalbundesanwalt abzustellen. Alternativ könnte die Prüfung des unbestimmten Rechtsbegriffs der besonderen Bedeutung des Falles den Verfassungsschutzbehörden überantwortet sein. Schließlich kommt eine Auslegung der Verweisungsnorm dahin in Betracht, dass sie die Ermittlungsübernahme generell nicht umfassen sollte. Der Wortlaut des § 20 Abs. 1 Satz 2 BVerfSchG spricht zwar dafür, dass eine Übermittlung wegen der in § 120 Abs. 2 Satz 1 Nr. 1 bis 4 GVG genannten Straftaten lediglich im Fall der tatsächlichen Übernahme der Verfolgung durch den Generalbundesanwalt zulässig sein soll. Jedenfalls im Bereich der Verhütung von Straftaten kann es aber in aller Regel nicht darauf ankommen, dass der Generalbundesanwalt die Ermittlungen tatsächlich übernommen hat. Dies wäre allenfalls bei Dauerdelikten denkbar. Dann liefe die – spezialgesetzlich geregelte – Übermittlungspflicht der Verfassungsschutzbehörden im gefahrenabwehrrechtlichen Bereich weitestgehend leer. 145

Ausgehend hiervon könnte eine Auslegung von § 20 Abs. 1 Satz 2 BVerfSchG zweckmäßig erscheinen, nach der die Verfassungsschutzbehörde im Vorfeld der Übermittlung eigenständig prüfen muss, ob die zu verhindernde Straftat im Falle ihrer Begehung eine besondere Bedeutung hätte, so dass der Generalbundesanwalt die Ermittlungen an sich ziehen müsste. Das gesetzliche Zuständigkeits- 146

merkmal der besonderen Bedeutung des Falles ist dabei als unbestimmter Rechtsbegriff zu verstehen. Deshalb würde eine Prüfung durch die Verfassungsschutzbehörden auch nicht mit dem sogenannten Evokationsrecht des Generalbundesanwalts kollidieren. Dieser hat bei der Prüfung der Übernahme des Verfahrens den Begriff der besonderen Bedeutung auszulegen und die Umstände des konkreten Falles darunter zu subsumieren. Ist danach die besondere Bedeutung zu bejahen, hat er die Sache an sich zu ziehen. Ein Beurteilungsspielraum steht ihm bei der Ausübung des sogenannten Evokationsrechts nicht zu. Die Übernahme ist zwingend und unterliegt der Nachprüfung durch die Gerichte (vgl. BVerfGE 9, 223 <229> zu § 24 Abs. 1 Nr. 2 GVG a.F. = § 24 Abs. 1 Nr. 3 GVG n.F.; dazu auch BGH, Urteil vom 22. Dezember 2000 - 3 StR 378/00 -, BGHSt 46, 238 <254 f. Rn. 46>).

Obgleich kein Beurteilungsspielraum besteht, erfordert die Prüfung der besonderen Bedeutung mitunter eine komplexe Würdigung tatsächlicher und rechtlicher Umstände. Daher könnte es als nicht sachgerecht erscheinen, diese komplexe Frage der besonderen Bedeutung durch einen Nachrichtendienst (vor-)entscheiden und die Übermittlungspflicht möglicherweise hieran scheitern zu lassen. Zu bedenken ist dabei auch, dass die Ermittlungsübernahme zwar für die Zuständigkeit des Gerichts relevant ist, jedoch nichts an dem materiell-rechtlichen Charakter einer Straftat ändert, auf den es für die Übermittlung ankommt (vgl. Gazeas, Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, 2014, S. 325 f. m.w.N.). 147

Einer Entscheidung, welcher dieser Auslegungsvarianten der Vorzug zu geben ist, bedarf es jedoch an dieser Stelle nicht. Es steht vielmehr dem Gesetzgeber zu, diese eindeutig zu normieren. Bestimmt er die Übermittlungsvoraussetzung durch Verweisungen, müssen diese begrenzt bleiben und dürfen nicht – wie vorliegend – durch die Inbezugnahme von Normen, die andersartige Spannungslagen bewältigen, ihre Klarheit verlieren und in der Praxis zu übermäßigen Schwierigkeiten bei der Anwendung führen (vgl. BVerfGE 154, 152 <266 Rn. 215> mit Verweis auf BVerfGE 110, 33 <57 f.; 61 ff.>; BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 272). Die gewählte Verweisungstechnik lässt im Ergebnis nicht normenklar erkennen, ob die Straftaten des § 120 Abs. 2 GVG eine Übermittlungspflicht bereits für sich genommen oder erst durch das Hinzutreten ihrer besonderen Bedeutung oder gar der Ermittlungsübernahme durch den Generalbundesanwalt auslösen sollen. Gleiches gilt wegen des umfas- 148

senden Verweises für § 21 Abs. 1 Satz 1 in Verbindung mit § 20 Abs. 1 Satz 1 und 2 BVerfSchG.

b) Die angegriffenen Übermittlungsregelungen verstoßen zudem gegen den Grundsatz der Verhältnismäßigkeit. Sie verfolgen zwar ein legitimes Ziel und sind hierfür geeignet und erforderlich, genügen jedoch im Hinblick auf ihre Angemessenheit den verfassungsrechtlichen Anforderungen nicht durchgehend. 149

aa) Die angegriffenen Normen dienen legitimen Zwecken. Sie zielen darauf ab, Staatsschutzdelikte effektiv zu bekämpfen und damit einhergehend den Bestand und die Sicherheit des Staates sowie Leib, Leben und Freiheit der Bevölkerung zu schützen (vgl. zur Terrorismusbekämpfung BVerfGE 133, 277 <321 Rn. 106, 333 f. Rn. 133>; 141, 220 <266 Rn. 96>; 156, 11 <47 Rn. 91>). Staatsschutzdelikte richten sich gegen die in Art. 73 Abs. 1 Nr. 10 Buchstabe b oder c GG genannten Rechtsgüter von hohem verfassungsrechtlichem Gewicht (vgl. BVerfGE 141, 220 <267 f. Rn. 100>), an deren Schutz ein herausragendes öffentliches Interesse besteht (vgl. BTDrucks 18/4654, S. 34). Sie wenden sich gegen die Grundpfeiler der verfassungsrechtlichen Ordnung und das Gemeinwesen als Ganzes. Die Bereitstellung wirksamer Aufklärungsmittel – auch in Form eines effektiven Informationsaustausches – zu ihrer Abwehr und Verfolgung ist ein legitimes Ziel und für die demokratische und freiheitliche Ordnung von großem Gewicht (vgl. BVerfGE 133, 277 <333 f. Rn. 133>; 141, 220 <266 Rn. 96> m.w.N.; 156, 11 <47 Rn. 91>; BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 239). Hierzu gehört, dass Verfassungsschutzbehörden, denen das Grundgesetz die Sammlung von Unterlagen zum Zwecke des Verfassungsschutzes auch mit verdeckt genutzten nachrichtendienstlichen Mitteln gestattet (BVerfGE 146, 1 <50 Rn. 110>; 156, 11 <51 f. Rn. 104 f.>; 156, 270 <304 Rn. 104>; BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 150), diese im Einzelfall weitergeben (vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 232, 239 m.w.N.). 150

bb) Dass die angegriffenen Übermittlungsbefugnisse zur Erreichung dieser Zwecke grundsätzlich im verfassungsrechtlichen Sinne geeignet und erforderlich sind, steht nicht in Zweifel. Es liegt auf der Hand, dass die Weitergabe der Daten an Behörden, zu deren Aufgaben die Verhinderung, Aufklärung oder Verfolgung von Straftaten gehört, der Erfüllung dieser Aufgaben zugute kommt. In den Kreis der Empfänger sind auch keine Behörden einbezogen worden, die zur Erreichung des Gesetzeszwecks nichts beitragen können (vgl. BVerfGE 100, 313 <390>). 151

cc) Die in § 20 Abs. 1 Satz 1 und 2 BVerfSchG geregelten Übermittlungsbefugnisse genügen jedoch im Hinblick auf ihre Angemessenheit den verfassungsrechtlichen Anforderungen nicht. Denn sie begrenzen die Übermittlung nicht durchgehend auf den Schutz besonders gewichtiger Rechtsgüter oder die Verfolgung besonders schwerer Straftaten und binden sie nicht an eine hinreichend konkretisierte Gefahrenlage oder an einen durch bestimmte Tatsachen erhärteten Verdacht solcher Straftaten. 152

(1) § 20 Abs. 1 Satz 1 BVerfSchG benennt bei der Regelung der Übermittlung nachrichtendienstlich erhobener Daten zur Gefahrenabwehr nicht unmittelbar das zu schützende Rechtsgut, sondern knüpft ebenso wie bei der Übermittlung zur Strafverfolgung an die in § 20 Abs. 1 Satz 2 BVerfSchG aufgeführten Straftaten an. 153

Grundsätzlich steht es dem Gesetzgeber frei, bei der Regelung der Übermittlung nachrichtendienstlich erhobener Daten zur Gefahrenabwehr das erforderliche Rechtsgut nicht unmittelbar zu benennen, sondern an entsprechende Straftaten anzuknüpfen (vgl. dazu BVerfGE 154, 152 <269 Rn. 221>; BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 244). Zwischen der präventiven und der repressiven Anknüpfung von Übermittlungsvoraussetzungen an Straftaten besteht dann ein Gleichlauf (vgl. BVerfGE 141, 220 <348 Rn. 347>; BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 244). 154

Unabhängig davon sind aber die Anforderungen an den Rechtsgüterschutz nicht durchgehend gewahrt. Denn nicht alle in den §§ 74a und 120 GVG genannten und durch die Vorschrift pauschal in Bezug genommenen Straftaten können als besonders schwere Straftaten qualifiziert werden. Gleiches gilt für den offenen Übermittlungstatbestand, der beliebige sonstige Straftaten alleine aufgrund ihrer Zielsetzung oder des Motivs des Täters mit einbezieht (so bereits BVerfGE 154, 152 <305 Rn. 312>). Insbesondere die vom Beschwerdeführer gerügte Einbeziehung von Delikten, die einen Strafrahmen von bis zu einem und drei Jahren Freiheitsstrafe oder Geldstrafe vorsehen (vgl. § 20 Abs. 1 Nr. 1 bis 4 VereinsG, § 89b StGB <von § 74a Abs. 1 Nr. 2 und 4 GVG erfasst> und § 97 Abs. 2 StGB <von § 120 Abs. 1 Nr. 3 GVG erfasst>), verfehlt die verfassungsrechtlichen Anforderungen. Soweit sich hier der für die Bestimmung der Schwere der Straftat maßgebliche Strafrahmen nicht mit dem Rang der strafrechtlich geschützten Rechtsgüter decken sollte, hätte dem Gesetzgeber die Möglichkeit offen gestanden, für die präventiv ausgerichtete Übermittlung einen Rechtsgüterkatalog zu normieren. 155

Insoweit hilft es auch nicht, dass § 23 Nr. 1 BVerfSchG ein allgemeines Verbot unverhältnismäßiger Übermittlungen enthält. Danach muss die Übermittlung von Informationen unterbleiben, wenn erkennbar ist, dass unter Berücksichtigung der Art der Informationen und ihrer Erhebung die schutzwürdigen Interessen des Betroffenen das Interesse der Allgemeinheit oder des Empfängers an der Übermittlung überwiegen. Dieser Pauschalvorbehalt strukturiert den Abwägungsprozess trotz der inzwischen erfolgten verfassungsgerichtlichen Konkretisierung der Anforderungen jedenfalls wegen der in § 20 Abs. 1 Satz 1 BVerfSchG normierten Pflicht zur Übermittlung nicht in einer Weise, dass eine Beschränkung der Übermittlung auf Fälle gesichert wäre, in denen die notwendigen Voraussetzungen vorliegen, die Übermittlung also insbesondere dem Schutz eines Rechtsguts von herausragendem öffentlichem Interesse dient (vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 367). 156

(2) Darüber hinaus fehlt es an der verfassungsrechtlich gebotenen Übermittlungsschwelle. Der Gesetzgeber hat insoweit Voraussetzungen zu formulieren, die den Anforderungen an eine konkretisierte Gefahrenlage (vgl. BVerfGE 141, 220 <271 ff. Rn. 111 ff.>) oder hinreichend verdachtsbegründende Tatsachen entsprechen müssen (BVerfGE 154, 152 <305 Rn. 312>). 157

Die angegriffenen Vorschriften erlauben eine Übermittlung bereits dann, wenn tatsächliche Anhaltspunkte dafür bestehen, dass diese zur Verhinderung oder Verfolgung von Staatsschutzdelikten erforderlich ist. Diese Anhaltspunkte beziehen sich hier allein auf den offenen Begriff der „Erforderlichkeit für die Verhinderung oder Verfolgung“ und ermöglichen damit die Übermittlung von Informationen, die unabhängig von einer konkretisierten Gefahrenlage oder von bestimmten, den Verdacht begründenden Tatsachen als erforderlich angesehen werden können. Die Bindung an die „Erforderlichkeit“ der Übermittlung genügt den verfassungsrechtlichen Anforderungen nicht (vgl. BVerfGE 154, 152 <306 Rn. 314>). 158

Bei einer Neuregelung der Übermittlung mit nachrichtendienstlichen Mitteln erhobener personenbezogener Daten und Informationen zur Gefahrenabwehr hat der Gesetzgeber aber auch darauf zu achten, eine Übermittlung nicht zu weit im Vorfeld einer in ihren Konturen noch nicht absehbaren Gefahr für die Schutzgüter zu erlauben. Eine präventiv ausgerichtete Anknüpfung der Übertragungsschwelle an Straftaten im Vorfeldstadium ist verfassungsrechtlich angesichts der Schwere des Eingriffs nicht hinnehmbar, wenn nur diffuse Anhaltspunkte für mögliche Gefahren bestehen (vgl. BVerfGE 100, 313 <395>; 141, 220 <273 Rn. 113>; BVerfG, 159

Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 376). Dies schließt nicht etwa aus, die Übermittlung zur präventiven Verhinderung von abstrakten Gefährdungsdelikten wie § 89a oder § 129a StGB zu ermöglichen (oben Rn. 134). Sicherzustellen ist dabei aber bereits auf Ebene der Übermittlungsvorschrift selbst, dass eine Übermittlung nur bei einer konkretisierten Gefahr für das durch die jeweiligen Straftatbestände geschützte Rechtsgut erfolgen darf.

c) Schließlich genügen die Übermittlungsvorschriften den verfassungsrechtlichen Anforderungen an eine spezifisch normierte Pflicht zur Protokollierung der Übermittlung sowie zur Nennung der für die Übermittlung in Anspruch genommenen Rechtsgrundlage nicht (vgl. BVerfGE 154, 152 <307 Rn. 319>). 160

D.

I.

Im Ergebnis genügen die § 20 Abs. 1 Satz 1 und 2, § 21 Abs. 1 Satz 1 in Verbindung mit § 20 Abs. 1 Satz 1 und 2 BVerfSchG, soweit sie zur Übermittlung personenbezogener Daten verpflichten, die unter Einsatz nachrichtendienstlicher Mittel im Sinne des § 8 Abs. 2 BVerfSchG erhoben wurden, nicht den verfassungsrechtlichen Anforderungen. Die Verfassungsbeschwerde ist insoweit begründet. § 20 Abs. 1 Satz 1 und 2 BVerfSchG ist nicht hinreichend normenklar gefasst. Er begrenzt die Übermittlung nicht durchgehend auf den Schutz besonders gewichtiger Rechtsgüter oder die Verfolgung besonders schwerer Straftaten und bindet sie nicht an eine hinreichend konkretisierte Gefahrenlage oder an einen durch bestimmte Tatsachen erhärteten Verdacht solcher Straftaten. Überdies fehlt es an einer spezifisch normierten Protokollierungspflicht. 161

II.

1. Die Feststellung der Verfassungswidrigkeit gesetzlicher Vorschriften führt grundsätzlich zu deren Nichtigkeit. Allerdings kann sich das Bundesverfassungsgericht, wie sich aus § 31 Abs. 2 Satz 2 und 3 BVerfGG ergibt, auch darauf beschränken, eine verfassungswidrige Norm nur für mit der Verfassung unvereinbar zu erklären. Es verbleibt dann bei einer bloßen Beanstandung der Verfassungswidrigkeit ohne den Ausspruch der Nichtigkeit. 162

Die Unvereinbarkeitserklärung kann das Bundesverfassungsgericht dabei zugleich mit der Anordnung einer befristeten Fortgeltung der verfassungswidrigen Regelung verbinden. Dies kommt in Betracht, wenn die sofortige Ungültigkeit der 163

zu beanstandenden Norm dem Schutz überragender Güter des Gemeinwohls die Grundlage entziehen würde und eine Abwägung mit den betroffenen Grundrechten ergibt, dass der Eingriff für eine Übergangszeit hinzunehmen ist. Für die Übergangszeit kann das Bundesverfassungsgericht vorläufige Anordnungen treffen, um die Befugnisse der Behörden bis zur Herstellung eines verfassungsmäßigen Zustandes durch den Gesetzgeber auf das zu reduzieren, was nach Maßgabe dieser Abwägung geboten ist (BVerfGE 141, 220 <351 Rn. 355> m.w.N.; stRspr).

2. a) Danach sind § 20 Abs. 1 Satz 1 und 2 und § 21 Abs. 1 Satz 1 in Verbindung mit § 20 Abs. 1 Satz 1 und 2 BVerfSchG lediglich für mit der Verfassung unvereinbar zu erklären. Auf Grundlage der hier erhobenen Verfassungsbeschwerde kann zwar nur ein Verfassungsverstoß der Übermittlungspflichten nach § 20 Abs. 1 Satz 1 und 2 sowie § 21 Abs. 1 Satz 1 in Verbindung mit § 20 Abs. 1 Satz 1 und 2 BVerfSchG festgestellt werden, soweit sie von § 8 RED-G in Bezug genommen werden (vgl. oben Rn. 80). Die Unvereinbarkeitserklärung ist aber entsprechend § 78 Satz 2 BVerfGG auf den übrigen Anwendungsbereich der Übermittlungspflichten zu erstrecken (vgl. BVerfGE 150, 244 <306 f. Rn. 169, 308 Rn. 171>), da die Vorschriften insoweit aus denselben Gründen verfassungswidrig sind. 164

Die Unvereinbarkeitserklärung ist mit der Anordnung ihrer vorübergehenden Fortgeltung bis zum Ablauf des 31. Dezember 2023 zu verbinden. Die Gründe für die Verfassungswidrigkeit dieser Vorschriften betreffen nicht den Kern der Übermittlungspflicht, sondern einzelne Aspekte ihrer rechtsstaatlichen Ausgestaltung. Der Gesetzgeber kann in diesen Fällen die verfassungsrechtlichen Beanstandungen nachbessern und damit den Kern der mit den Vorschriften verfolgten Ziele auf verfassungsmäßige Weise verwirklichen. Ein effektiver Informationsaustausch, der der Verhinderung und Verfolgung von Staatsschutzdelikten dient, ist von großer Bedeutung. Unter diesen Umständen ist die vorübergehende Fortgeltung der Übermittlungsvorschriften eher hinzunehmen als ihre Nichtigkeitserklärung, die eine Datenübermittlung von Verfassungsschutzbehörden an Strafverfolgungs- und Sicherheitsbehörden in Angelegenheiten des Staats- und Verfassungsschutzes erheblich beeinträchtigen würde (vgl. auch BVerfGE 141, 220 <352 Rn. 357>). 165

b) Die Anordnung der Fortgeltung bedarf mit Blick auf das betroffene Grundrecht jedoch einschränkender Maßgaben. So ist eine Übermittlung von mit nachrichtendienstlichen Mitteln erlangten personenbezogenen Daten und Informationen gemäß § 20 Abs. 1 Satz 1 und 2 und § 21 Abs. 1 Satz 1 in Verbindung mit 166

§ 20 Abs. 1 Satz 1 und 2 BVerfSchG nur zum Schutz eines Rechtsguts von herausragendem öffentlichem Interesse zulässig, was einer Begrenzung auf besonders schwere Straftaten entspricht. Außerdem müssen die nach Maßgabe der Gründe an die jeweilige Übermittlungsschwelle zu stellenden Anforderungen erfüllt sein, die sich danach unterscheiden, an welche Stelle übermittelt wird (vgl. oben Rn. 132 ff.; BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, 3. Leitsatz, Rn. 230 ff.).

III.

Die Auslagenentscheidung beruht auf § 34a Abs. 2 BVerfGG. 167

Harbarth Baer Britz

Ott Christ Radtke

Härtel Wolff